Prerequisites for Windows Client Deployment in Configuration Manager

Updated: November 18, 2016

Applies To: System Center 2012 Configuration Manager, System Center 2012 Configuration Manager SP1, System Center 2012 Configuration Manager SP2, System Center 2012 R2 Configuration Manager, System Center 2012 R2 Configuration Manager SP1

Deploying System Center 2012 Configuration Manager clients in your environment has the following external dependencies and dependencies within the product. Additionally, each client deployment method has its own dependencies that must be met for client installations to be successful.

Use the following sections to determine the prerequisites to install the Configuration Manager client on computers and mobile devices:

- Prerequisites for Computer Clients
- Prerequisites for Mobile Device Clients

Make sure that you also review Supported Configurations for Configuration Manager to confirm that devices meet the minimum hardware and operating system requirements for the System Center 2012 Configuration Manager client.

For information about the prerequisites for the Configuration Manager client for Linux and UNIX, see the Prerequisites for Client Deployment to Linux and UNIX Servers section in the Planning for Client Deployment for Linux and UNIX Servers topic.

Prerequisites for Computer Clients

Use the following information to determine the prerequisites for when you install the Configuration Manager client on computers.

Dependencies External to Configuration Manager

Dependencies external to Configuration Manager	More information
For Configuration Manager client computers with no service pack that will connect to the Application Catalog:	If you run Configuration Manager with no service pack, the Application Catalog website uses an ActiveX control for Internet Explorer, which coordinates application installation and approval requests with the Configuration Manager client. The ActiveX control file is named
Configure Internet Explorer to exclude the ActiveX control Microsoft.ConfigurationManager	Microsoft.ConfigurationManager.SoftwareCatalog.Website.ClientBridgeCont rol.dll and is automatically installed on the client when the Configuration Manager client is installed.
.SoftwareCatalog.Website.Client BridgeControl.dll from ActiveX	You must configure Internet Explorer to exclude this ActiveX control from ActiveX filtering and allow it to run in the browser. You can manually configure Internet

)17 Pre	requisites for Windows Client Deployment in Configuration Manager
filtering and allow it to run in the browser.	Explorer or use Group Policy settings. For more information, see your Windows documentation. Note This configuration is not required for Configuration Manager SP1, because Configuration Manager SP1 does not use an ActiveX control.
Windows Installer version 3.1.4000.2435	Required to support the use of Windows Installer update (.msp) files for packages and software updates.
Install the hotfix described in KB2552033 on site servers that run Windows Server 2008 R2.	The hotfix described in KB2552033 must be installed on site servers that run Windows Server 2008 R2 when client push installation is enabled.
Microsoft Background Intelligent Transfer Service (BITS) version 2.5	Microsoft Background Intelligent Transfer Service (BITS) is required to allow throttled data transfers between the client computer and System Center 2012 Configuration Manager site systems. BITS is not automatically downloaded during client installation.
	✓ Note
	When BITS is installed on computers, a restart is typically required to complete the installation.
	♦ Important
	Most operating systems include BITS, but if they do not (for example, Windows Server 2003 R2 SP2), you must install BITS before you install the System Center 2012 Configuration Manager client.
Microsoft Task Scheduler service	The Microsoft Task Scheduler service must be enabled on the client for the client installation to complete.

Mote

The software version numbers only list the minimum version numbers.

Dependencies External to Configuration Manager and Automatically Downloaded During Installation

The System Center 2012 Configuration Manager client has some potential external dependencies. These dependencies depend on the operating system and the installed software on the client computer.

If these dependencies are required to complete the installation of the client, they are automatically installed with the client software.

Dependencies automatically supplied during installation	More information
Windows Update Agent version 7.0.6000.363	Required by Windows to support update detection and deployment.
Microsoft Core XML Services (MSXML) version 6.20.5002 or later	Required to support the processing of XML documents in Windows.
Microsoft Remote Differential Compression (RDC)	Required to optimize data transmission over the network.
Microsoft Visual C++ 2005 Redistributable version 8.0.50727.42	Required to support Microsoft SQL Server Compact operations.
	✓ Note
	Not required for Microsoft System Center 2012 Configuration Manager SP2 or System Center 2012 R2 Configuration Manager SP1 (both with Cumulative Update 4).
Microsoft Visual C++ 2008 Redistributable version 9.0.30729.4148.	For Microsoft System Center 2012 Configuration Manager SP1 or earlier. Required to support client operations.
	✓ Note
	When this update is installed on client computers, a restart might be required to complete the installation.
Microsoft Visual C++	For System Center 2012 R2 Configuration Manager.
2010 Redistributable version 10.0.40219.1	Required to support client operations.
	✓ Note

017	Prerequisites for Windows Client Deployment in Configuration Manager
	When this update is installed on client computers, a restart might be required to complete the installation.
Microsoft Visual C++ 2013 Redistributable version 12.0.21005.1	For Microsoft System Center 2012 Configuration Manager SP2 and System Center 2012 R2 Configuration Manager SP1. Required to support client operations.
	✓ Note
	When this update is installed on client computers, a restart might be required to complete the installation.
Windows Imaging APIs 6.0.6001.18000	Required to allow Configuration Manager to manage Windows image (.wim) files.
Microsoft Policy Platform 1.2.3514.0	Required to allow clients to evaluate compliance settings.
Microsoft Silverlight 4.0.50524.0	For Configuration Manager with no service pack only.
4.0.30324.0	Required to support the Application Catalog website user experience.
Microsoft Silverlight 5.1.10411.0	For Microsoft System Center 2012 Configuration Manager SP1.
3.1.10411.0	Required to support the Application Catalog website user experience.
Microsoft Silverlight 5.1.20513.0	For System Center 2012 R2 Configuration Manager.
3.1.20313.0	Required to support the Application Catalog website user experience.
Microsoft Silverlight 5.1.30514.0	For Microsoft System Center 2012 Configuration Manager SP2 and System Center 2012 R2 Configuration Manager SP1.
	Required to support the Application Catalog website user experience.
Microsoft .NET Framework 4 Client Profile	Client computers require the .NET Framework to support client operations. If a client computer does not have one of the following installed versions, the Microsoft .NET Framework 4 Client Profile is installed automatically:
	 Microsoft .NET Framework version 3.0. Microsoft .NET Framework version 3.5. Microsoft .NET Framework version 4.0.
	✓ Note
	When the .NET Framework 4 is installed on computers, a restart might be required to

017	referedusites for windows client Deployment in Configuration Manager
	complete the installation.
Microsoft SQL Server Compact 3.5 SP2 components	Required to store information related to client operations.
Microsoft Windows Imaging Components	Required by Microsoft .NET Framework 4.0 for Windows Server 2003 or Windows XP SP2 for 64-bit computers.

Mote

The software version numbers only list the minimum version numbers.

Configuration Manager Dependencies

For more information about the following site system roles, see Determine the Site System Roles for Client Deployment in Configuration Manager.

Configuratio n Manager site system	More information
Management point	Although a management point is not required to deploy the System Center 2012 Configuration Manager client, you must have a management point to transfer information between client computers and System Center 2012 Configuration Manager servers. Without a management point, you cannot manage client computers.
Distribution point	The distribution point is an optional, but recommended site system role for client deployment. All distribution points host the client source files, which lets computers find the nearest distribution point from which to download the client source files during client deployment. If the site does not have a distribution point, computers download the client source files from their management point.
Fallback status point	The fallback status point is an optional, but recommended site system role for client deployment. The fallback status point tracks client deployment and enables computers in the System Center 2012 Configuration Manager site to send state messages when they cannot communicate with a management point.
Reporting services point	The reporting services point is an optional, but recommended site system role that can display reports related to client deployment and management.
	For more information, see Reporting in Configuration Manager.

Installation Method Dependencies

The following prerequisites are specific to the various methods of client installation.

Client installation method	More information
Client push installation	 Client push installation accounts are used to connect to computers to install the client and are specified on the Accounts tab of the Client Push Installation Properties dialog box. The account must be a member of the local administrators group on the destination computer. If you do not specify a client push installation account, the site server computer account will be used. The computer on which you are installing the client must have been discovered by at least one System Center 2012 Configuration Manager discovery method. The computer has an ADMIN\$ share. Enable client push installation to assigned resources must be selected in the Client Push Installation Properties dialog box if you want to automatically push the System Center 2012 Configuration Manager client to discovered resources. The client computer must be able to contact a distribution point or a management point to download the supporting files. You must have the following security permissions to install the Configuration Manager client by using client push: To configure the Client Push Installation account: Modify and Read permission for the Site object. To use client push to install the client to collections, devices and queries: Modify Resource and Read permission for the Collection object. The Infrastructure Administrator security role includes the required permissions to manage client push installation. For more information about how to configure the requirements in the Client Push Installation Properties dialog box, see the How to Install Configuration Manager Clients by Using Client Push section in the How to Install Clients on Windows-Based Computers in Configuration Manager.
Software update point- based installation	 If the Active Directory schema has not been extended, or you are installing clients from another forest, installation properties for CCMSetup.exe must be provisioned in the registry of the computer by using Group Policy. For more information, see the How to Provision Client Installation Properties (Group Policy and Software Update-Based Client Installation) section in the How to Install Clients on Windows-Based Computers in Configuration Manager topic. The System Center 2012 Configuration Manager client must be published to the software update point. The client computer must be able to contact a distribution point or a management point in order to download supporting files. For the security permissions required to manage Configuration Manager software updates, see Prerequisites for Software Updates in Configuration Manager.

Group Policy- based installation	 If the Active Directory schema has not been extended, or you are installing clients from another forest, installation properties for CCMSetup.exe must be provisioned in the registry of the computer by using Group Policy. For more information, see the How to Provision Client Installation Properties (Group Policy and Software Update-Based Client Installation) section in the How to Install Clients on Windows-Based Computers in Configuration Manager topic. The client computer must be able to contact a management point in order to download supporting files.
Logon script- based installation	 The client computer must be able to contact a distribution point or a management point in order to download supporting files unless, at the command prompt, you specified CCMSetup.exe with the command-line property ccmsetup /source.
Manual installation	 The client computer must be able to contact a distribution point or a management point in order to download supporting files unless, at the command prompt, you specified CCMSetup.exe with the command-line property ccmsetup /source.
Workgroup computer installation	 In order to access resources in the System Center 2012 Configuration Manager site server domain, the Network Access Account must be configured for the site. For more information about how to configure the Network Access Account, see the Configure the Network Access Account section in the Configuring Content Management in Configuration Manager topic.
Software distribution- based installation (for upgrades only)	 If the Active Directory schema has not been extended, or you are installing clients from another forest, installation properties for CCMSetup.exe must be provisioned in the registry of the computer by using Group Policy. For more information, see the How to Provision Client Installation Properties (Group Policy and Software Update-Based Client Installation) section in the How to Install Clients on Windows-Based Computers in Configuration Manager topic. The client computer must be able to contact a distribution point or a management point to download the supporting files. For the security permissions required to upgrade the Configuration Manager client using application
	management, see Prerequisites for Application Management in Configuration Manager.
Automatic client upgrades	You must be a member of the Full Administrator security role to configure automatic client upgrades.

Firewall Requirements

If there is a firewall between the site system servers and the computers onto which you want to install the Configuration Manager client, see Windows Firewall and Port Settings for Client Computers in Configuration Manager.

Prerequisites for Mobile Device Clients

Use the following information to determine the prerequisites for when you install the Configuration Manager client on mobile devices and use Configuration Manager to enroll them.

Dependencies External to Configuration Manager

Dependencies external to Configuration Manager	More information
A Microsoft enterprise certification authority (CA) with certificate templates to deploy and manage the certificates required for mobile devices. The issuing CA must automatically approve certificate requests from the mobile device users during the enrollment process.	For more information about the certificate requirements, see PKI Certificate Requirements for Configuration Manager.
A security group that contains the users that can enroll their mobile devices.	This security group is used to configure the certificate template that is used during mobile device enrollment. For more information, see the Deploying the Enrollment Certificate for Mobile Devices section in the Step-by-Step Example Deployment of the PKI Certificates for Configuration Manager: Windows Server 2008 Certification Authority topic.
Optional but recommended: a DNS alias (CNAME record) named ConfigMgrEnroll that is configured for the site system server name on which you will install the enrollment proxy point.	This DNS alias is required to support automatic discovery for the enrollment service: If you do not configure this DNS record, users must manually specify the site system server name of the enrollment proxy point as part of the enrollment process.
Site system role dependencies for the computers that will run the enrollment point and the enrollment proxy point site system roles.	See the Prerequisites for Site System Roles section in the Supported Configurations for Configuration Manager topic.

Configuration Manager Dependencies

For more information about the following site system roles, see Determine the Site System Roles for Client Deployment in Configuration Manager.

Configuration Manager site system	More information
Management point that is configured for HTTPS client connections and enabled	A management point is always required to install the System Center 2012 Configuration Manager client on mobile devices. In addition to the

17 Prerequisit	es for Windows Client Deployment in Configuration Manager
for mobile devices	configuration requirements of HTTPS and enabled for mobile devices, the management point must be configured with an Internet FQDN and accept client connections from the Internet.
Enrollment point and enrollment proxy point	An enrollment proxy point manages enrollment requests from mobile devices and the enrollment point completes the enrollment process. The enrollment point must be in the same Active Directory forest as the site server, but the enrollment proxy point can be in another forest.
Client settings for mobile device enrollment	Configure client settings to allow users to enroll mobile devices and configure at least one enrollment profile.
Reporting services point	The reporting services point is an optional, but recommended site system role that can display reports related to mobile device enrollment and client management.
	For more information, see Reporting in Configuration Manager.
To configure enrollment for mobile devices, you must have the following security permissions:	For more information about how to configure security permissions, see the Configure Role-Based Administration section in the Configuring Security for Configuration Manager topic.
 To add, modify, and delete the enrollment site system roles: Modify permission for the Site object. To configure client settings for enrollment; Default client settings. 	
enrollment: Default client settings require Modify permission for the Site object, and custom client settings require Client agent permissions.	
The Full Administrator security role includes the required permissions to configure the enrollment site system roles.	
To manage enrolled mobile devices, you must have the following security permissions:	
 To wipe or retire a mobile device: Delete resource for the Collection object. To cancel a wipe or retire command: Delete resource for the Collection object. To allow and block mobile devices: Modify resource for the 	

 To remote lock, or reset the passcode on a mobile device: Modify resource for the Collection object.

The **Operations Administrator** security role includes the required permissions to manage mobile devices.

Firewall Requirements

Intervening network devices such as routers and firewalls, and Windows Firewall if applicable, must allow the traffic associated with mobile device enrollment:

- Between mobile devices and the enrollment proxy point: HTTPS (by default, TCP 443)
- Between the enrollment proxy point and the enrollment point: HTTPS (by default, TCP 443)

If you use a proxy web server, it must be configured for SSL tunneling; SSL bridging is not supported for mobile devices.

See Also

Planning for Client Deployment in Configuration Manager

© 2017 Microsoft