ARIZONA WESTERN COLLEGE – ITSS

**SCCM Endpoint Protection**

**Version 1.001**

# **Disclaimers**

The information contained in this document is the proprietary and exclusive property of Arizona Western College except as otherwise indicated. No part of this document, in whole or in part, may be reproduced, stored, transmitted, or used for design purposes without the prior written permission of Arizona Western College.

The information contained in this document is subject to change without notice.

The information in this document is provided for informational purposes only. Arizona Western College specifically disclaims all warranties, express or limited, including, but not limited, to the implied warranties of merchantability and fitness for a particular purpose, except as provided for in a separate software license agreement.

# **Privacy Information**

This document may contain information of a sensitive nature. This information should not be given to persons other than those who are involved in the SCCM Endpoint Protection project or who will become involved during the lifecycle.

# **Version History**

|  |  |  |  |
| --- | --- | --- | --- |
| REVISION CHART | | | |
| Version | Author(s) | Description of Version | Date Completed |
| 1.0 | Robert Schroeder | Created document | 10-5-2018 |
| 1.001 | Robert Schroeder | Removed component design from document | 10-17-2018 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# **Document Owner**

The primary contact for questions regarding this document is:

Author: Tier 2, Endpoint Systems Management

SCCM Endpoint Protection

# **Document Approval**

Document Name: SCCM Endpoint Protection

Publication Date:

Prepared by:

Approval: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

***Name and Organization***

Concurrence: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

***Name and Organization***

Table of Contents

1. **Introduction**
   1. Purpose of this document
   2. Scope
   3. Overview
   4. References
2. **System Overview**
   1. **System Overview**
3. **System Architecture**
   1. **Product Components**
   2. **Decomposition Description**
   3. **Design Rationale**
4. **Human Interface Design**
   1. **Overview of the User Interface**
   2. **Screen Images**
   3. **Screen Objects and Actions**
5. **Requirements Matrix**
   1. **Site Systems**
   2. **Clients**
   3. **Configuration Manager Console**

1 Introduction

* 1. **Purpose of this document**

**The purpose of this document is to describe the implementation of the SCCM Endpoint Protection and serve as an overall guidance to the architecture of System Center Endpoint Protection.**

* 1. **Scope**

**System Center Endpoint Protection (SCEP) offers powerful and efficient protection against emerging malware threats. SCEP application is a server/client combination that will provide Arizona Western College with antivirus protection against malicious system attacks. SCEP will also provide real-time file system protection, and on-demand computers scans.**

* 1. **Overview**

**This document is divided into 5 sections with various subsections. The sections of the document are:**

* **Introduction**
* **System Overview**
* **System Architecture**
* **Human Interface Design**
* **Requirements Matrix**
  1. **References**
* Aczechowski. “Endpoint Protection - Configuration Manager.” *Microsoft Docs: Endpoint Protection*, 2 Aug. 2018, docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-protection.

2 System Overview

**2.1 System Overview**

Microsoft System Center Endpoint Protection provides an antimalware and security solution for the Microsoft platform.

When System Center Endpoint Protection is used with System Center Configuration Manager, it provides a comprehensive enterprise management solution that lets you do the following:

* Centrally deploy and configure the Windows Defender and Endpoint Protection clients.
* Configure default and custom antimalware policies that apply to groups of computers.
* Create and deploy Windows Firewall settings to groups of computers.
* Use Configuration Manager software updates to automatically download the latest antimalware definition files to keep client computers up-to-date.
* Control who manages the antimalware policies and Windows Firewall settings by using the **Endpoint Protection Manager** security role.
* Use email notifications to alert you when computers report that malware is installed.
* View summary and detailed information from the Configuration Manager console and reports.
  1. System Architecture

**3.1 Product Components**

**Table – Main components**

|  |  |
| --- | --- |
| **Component** | **Description** |
| **System Center Configuration Manager** | **System Center Configuration Manager is a management server that manages events, policies, and client registration for the client computers that connect to Arizona Western College’s network. System Center Configuration Manager includes the following subcomponents:**   * **The management server software provides secure communication to and from the client computers and the console.** * **The console is the interface to the management server. The console software coordinates and manages security policies, client computers, reports, logs, roles and access, administrative functions, and security. A remote console can be installed and use it to connect to the management server from any computer within Arizona Western College’s network.** * **A SQL Server database stores security policies and events for System Center Configuration Manager.** |
| **System Center  Endpoint Protection client** | **The System Center Endpoint Protection client provides the security protection part of the solution. The client downloads policies and content from the System Center Configuration Manager and runs on Windows and Mac.** |

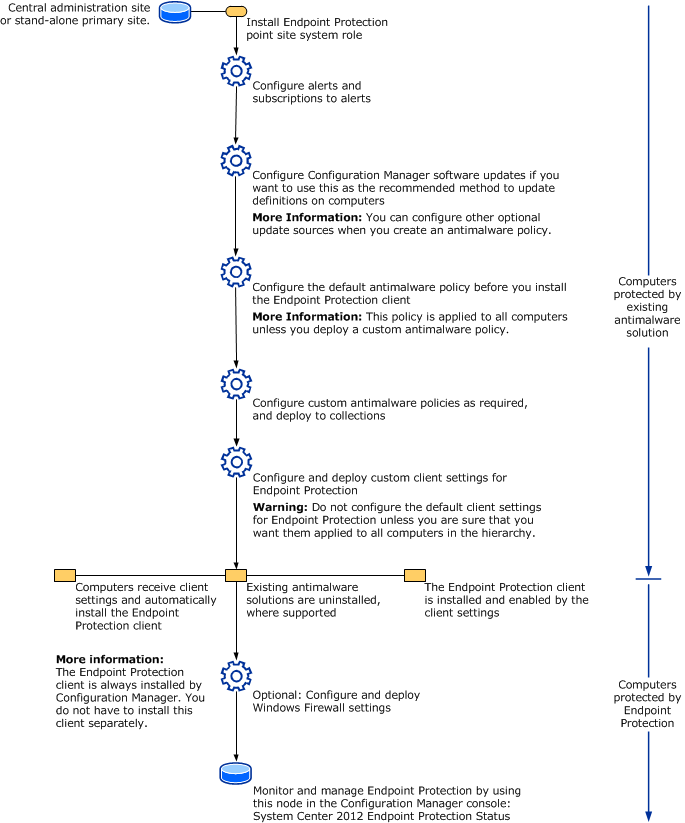
**3.2 Decomposition Description**

**The System Center Endpoint Protection architecture uses three functional groups of components. Some of the components belong in multiple groups because they are multi-functional.**

**Figure: System Center Endpoint Protection components**



**Figure: System Center Endpoint Protection workflow**



**3.3 Design Rationale**

* **Cost – Microsoft System Center Configuration Manager is available through Arizona Western College’s current license agreement with Microsoft. System Center Endpoint Protection is part of the Microsoft System Center Configuration system. Previous to Microsoft’s System Center Endpoint Protection, Arizona Western College was using Sophos Endpoint Protection as its primary source of antivirus and malware threat protection. Sophos was an added cost to Arizona Western College and it was decided to implement System Center Endpoint Protection to retain the funds that were being paid to Sophos.**
* **Usability – Microsoft System Endpoint Protection and its tight integration with System Center Configuration Manager allows for a centralized management point for Arizona Western College owned devices. All administration is performed through the System Center Management Console. An industry AV test completed by The Independent IT-Security Institute in March-April showed a usability score of 5.5/6.0. Microsoft provides best practices and templates for creating antimalware policies and provides support through Microsoft TechNet Library, System Center forums, and wiki articles.**
* **Efficiency – System Center Endpoint Protection offers protection across different platforms including Windows and Mac, which is currently the largest collection of devices owned by Arizona Western College. The March-April AV test revealed that System Center Endpoint Protection received a score of 5.5/6.0 for Protection (missing only 2 out of 5,680 malware samples) and a 5.5/6.0 for Performance (System Center Endpoint Protection continues to outperform the industry in most areas).**
  1. Human Interface Design

**4.1 Overview of the User Interface**

**Windows**

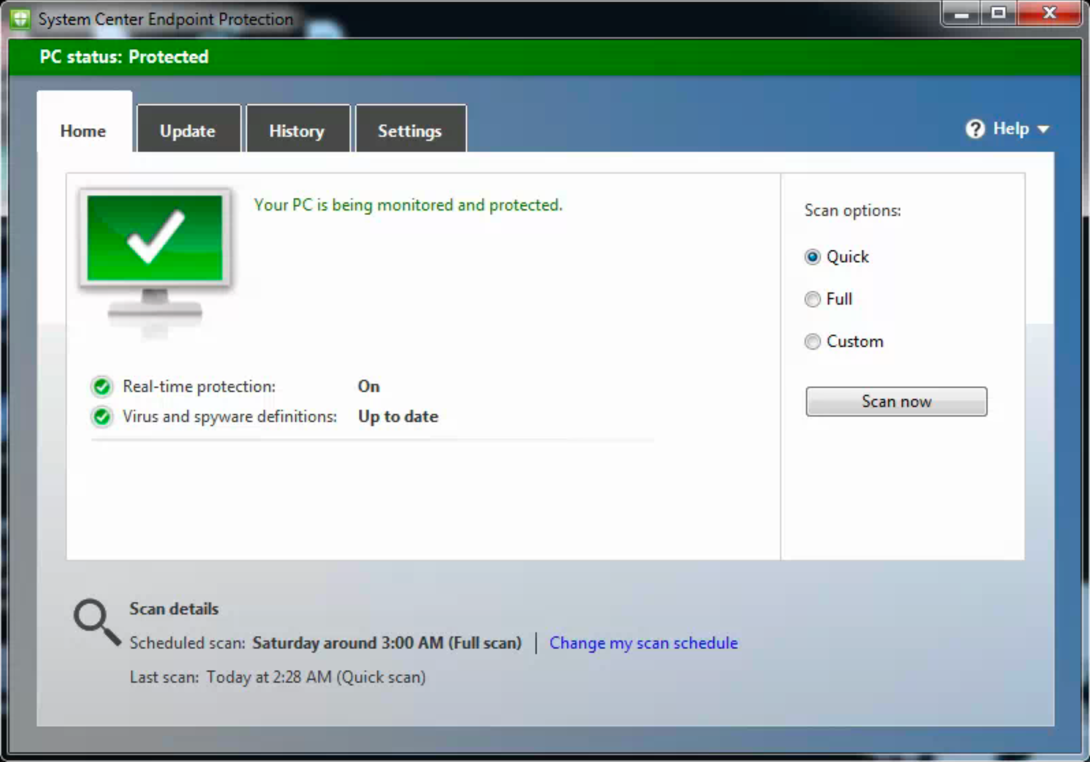
**The System Center Endpoint Protection user interface provides users with protection, update, and history status of their computer. Users can perform on-demand scans from the interface and can also perform updates to the virus signature database within the user interface.**

**Mac**

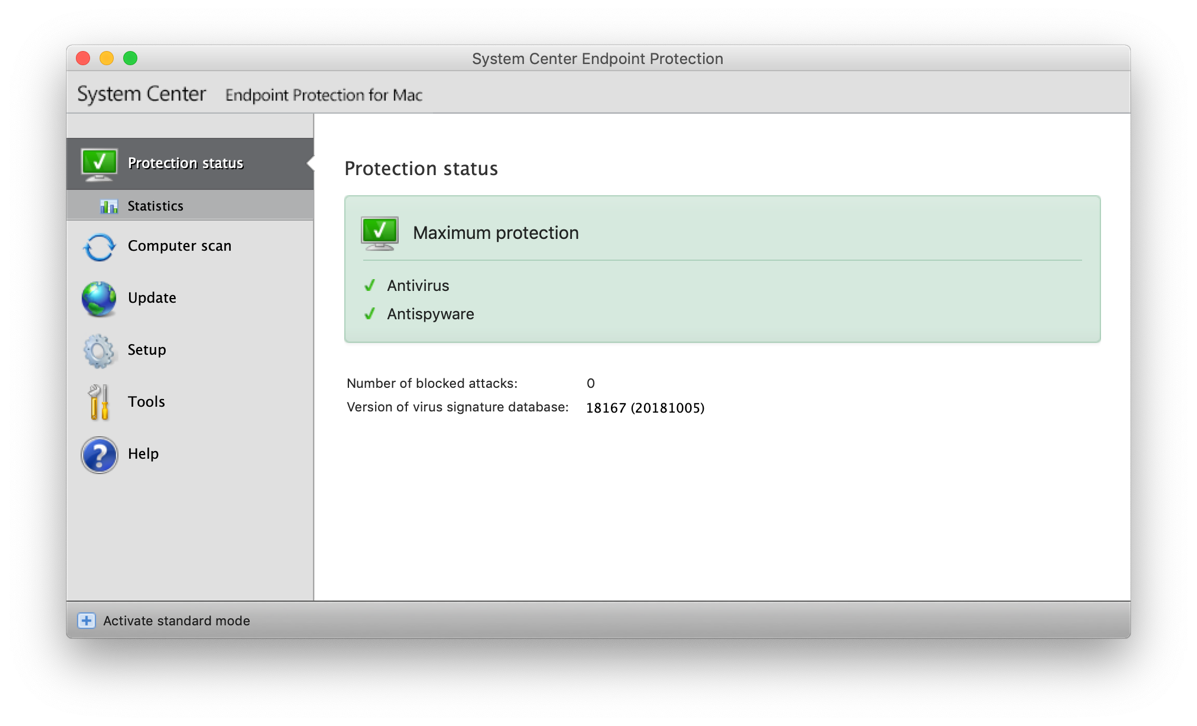
**The System Center Endpoint Protection user interface allows users to toggle between Standard and Advanced mode. Standard mode provides access to features required for common operations. It does not display any advanced options. To toggle between modes, click the plus icon (+) next to Activate advanced mode/Advanced standard mode in the bottom left corner of the main program window or press cmd+M**

**4.2 Screen Images**

**Windows**

****

**Mac**



**4.3 Screen Objects and Actions**

**Windows**

**The main program window of System Center Endpoint Protection is divided into four main sections which can be accessed by the tab structures at the top of the program.**

**The following is a description of options within the tab structure:**

* **Home – Provides information about the protection status of System Center Endpoint Protection. Home is also where you can perform on-demand Quick, Full, or Custom scans.**
* **Update – Displays information about updates to the virus signature database.**
* **History – Allows you to view items that were detected as potentially harmful and the action taken on them.**
* **Settings – Displays settings that are managed by System Center Endpoint Protection through the System Center Configuration Manager by an administrator.**

**Mac**

**The main program window of System Center Endpoint Protection is divided into two main sections. The primary window on the right displays information that corresponds to the option selected from the main menu on the left.**

**The following is a description of options within the main menu:**

* **Protection status – provides information about the protection status of System Center Endpoint Protection. If Advanced mode is activated, the Statistics submenu will display.**
* **Computer scan – This option allows you to configure and launch the On-demand computer scan.**
* **Update – Displays information about updates to the virus signature database.**
* **Setup – Select this option to adjust our computer’s security level. If Advanced mode is activated, the Antivirus and antispyware submenu will display.**
* **Tools – Provides access to Log files, Quarantine and Scheduler. This option only displays in Advanced mode.**
* **Help – Provides program information and access to help files.**
  1. Requirements Matrix

The following recommendations are guidelines to help you scale your System Center Configuration Manager environment to support more than a very basic deployment of sites, site systems, and clients. They are not intended to cover all possible site and hierarchy configurations.

Use the information in the following sections as a guide to help you plan for hardware that can meet the processing loads for clients and sites that use the available Configuration Manager features with the default configurations.

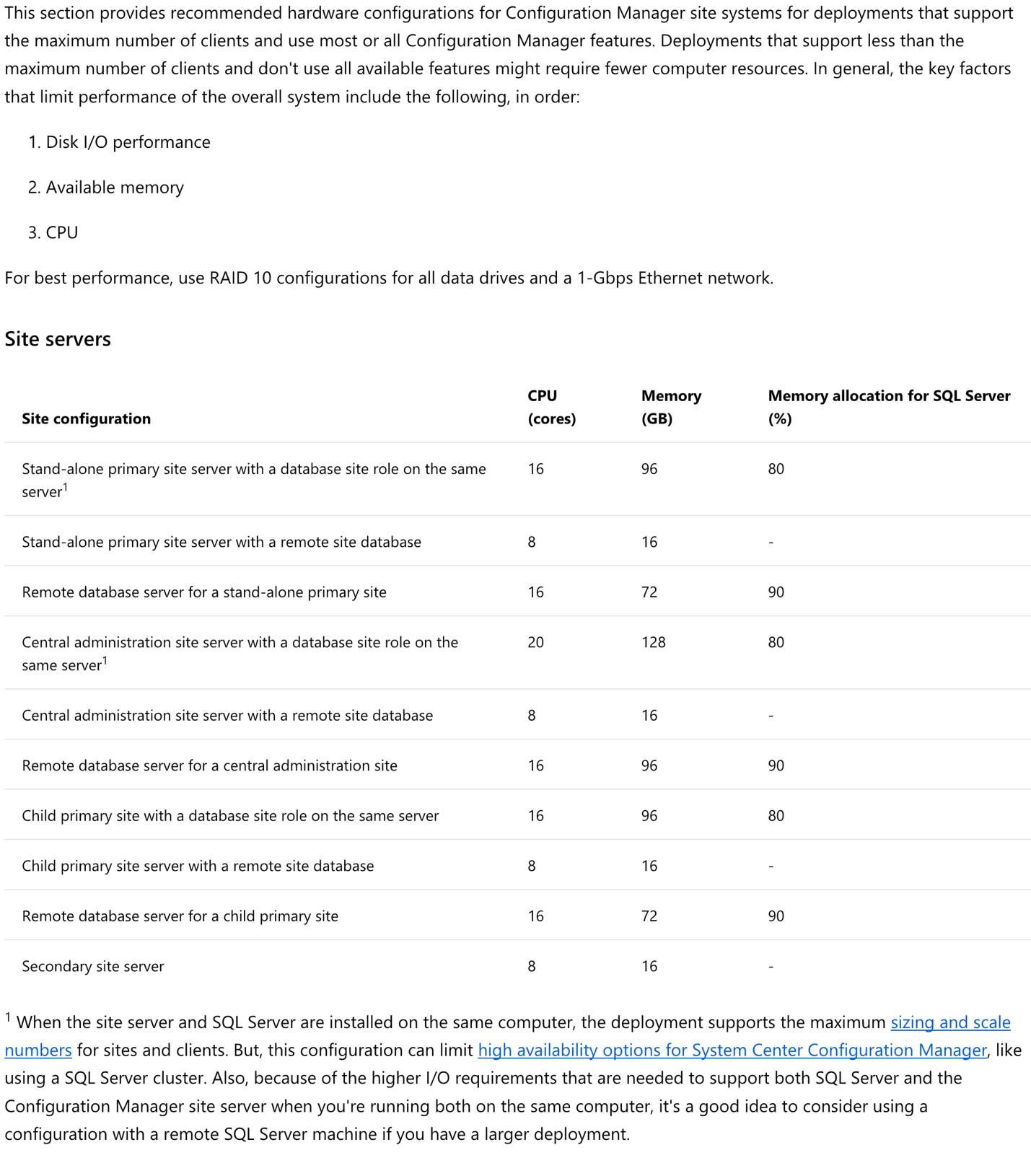
**5.1 Site Systems**

This section provides recommended hardware configurations for Configuration Manager site systems for deployments that support the maximum number of clients and use most or all Configuration Manager features. Deployments that support less than the maximum number of clients and don't use all available features might require fewer computer resources. In general, the key factors that limit performance of the overall system include the following, in order:

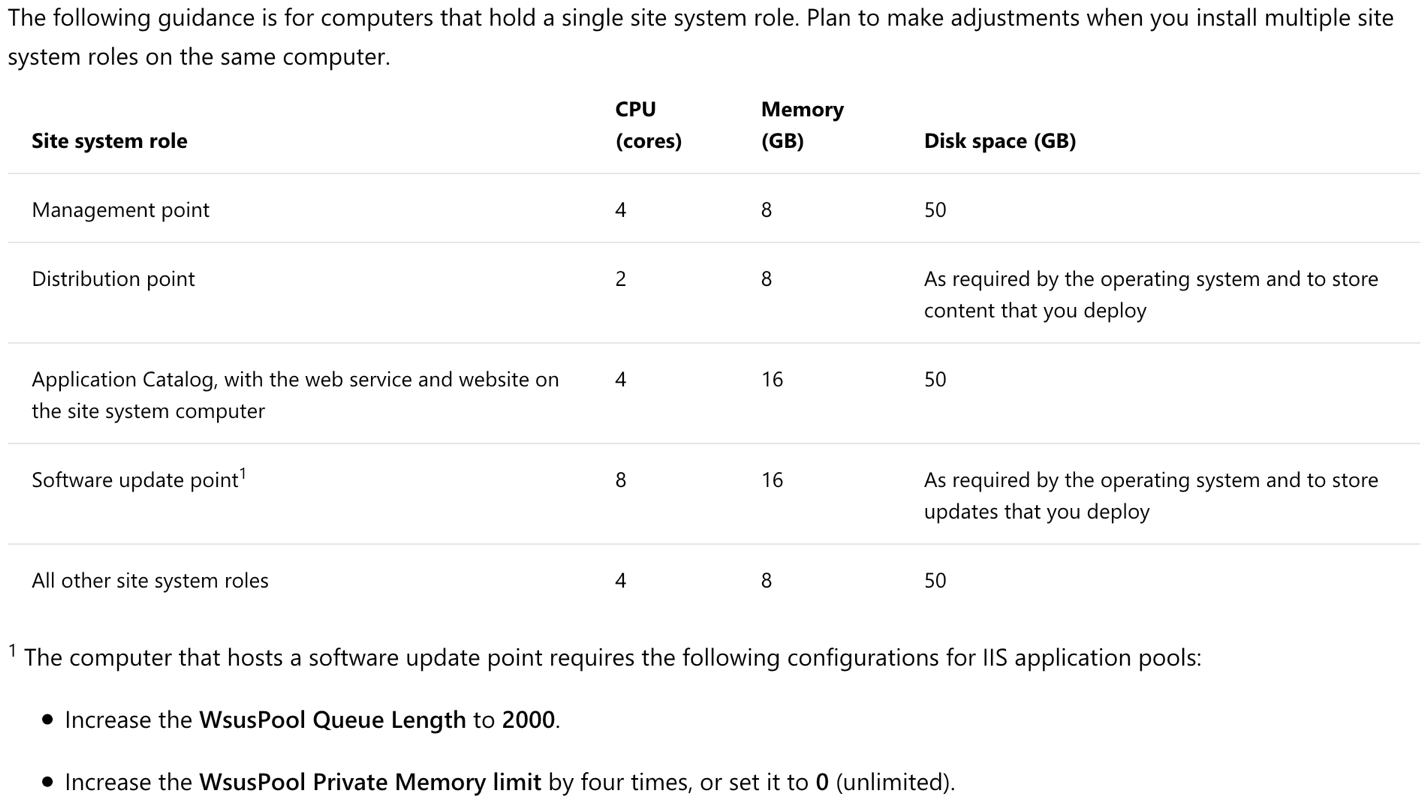
1. Disk I/O performance
2. Available memory
3. CPU

For best performance, use RAID 10 configurations for all data drives and a 1-Gbps Ethernet network

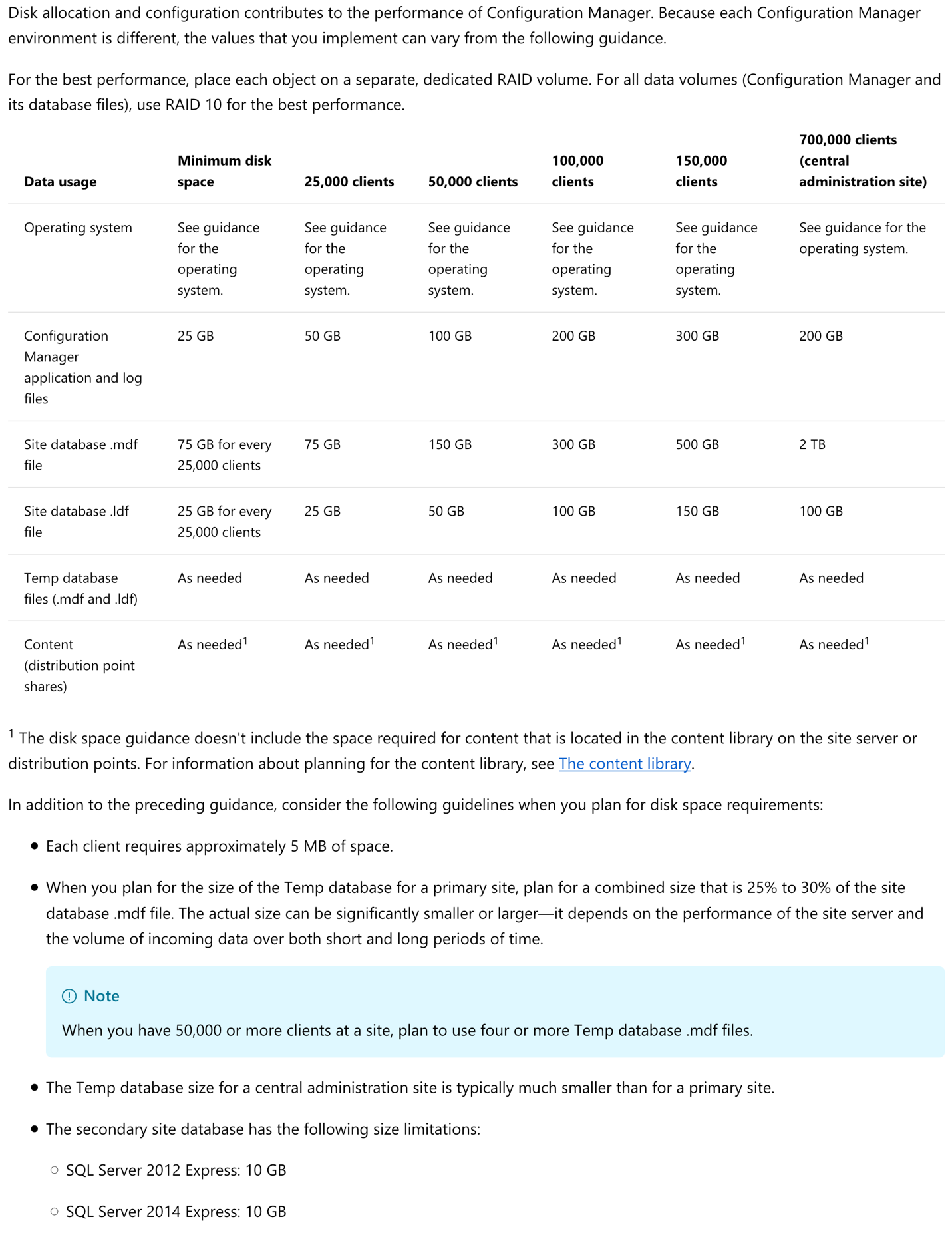
**Site server**

****

**Remote site system servers**

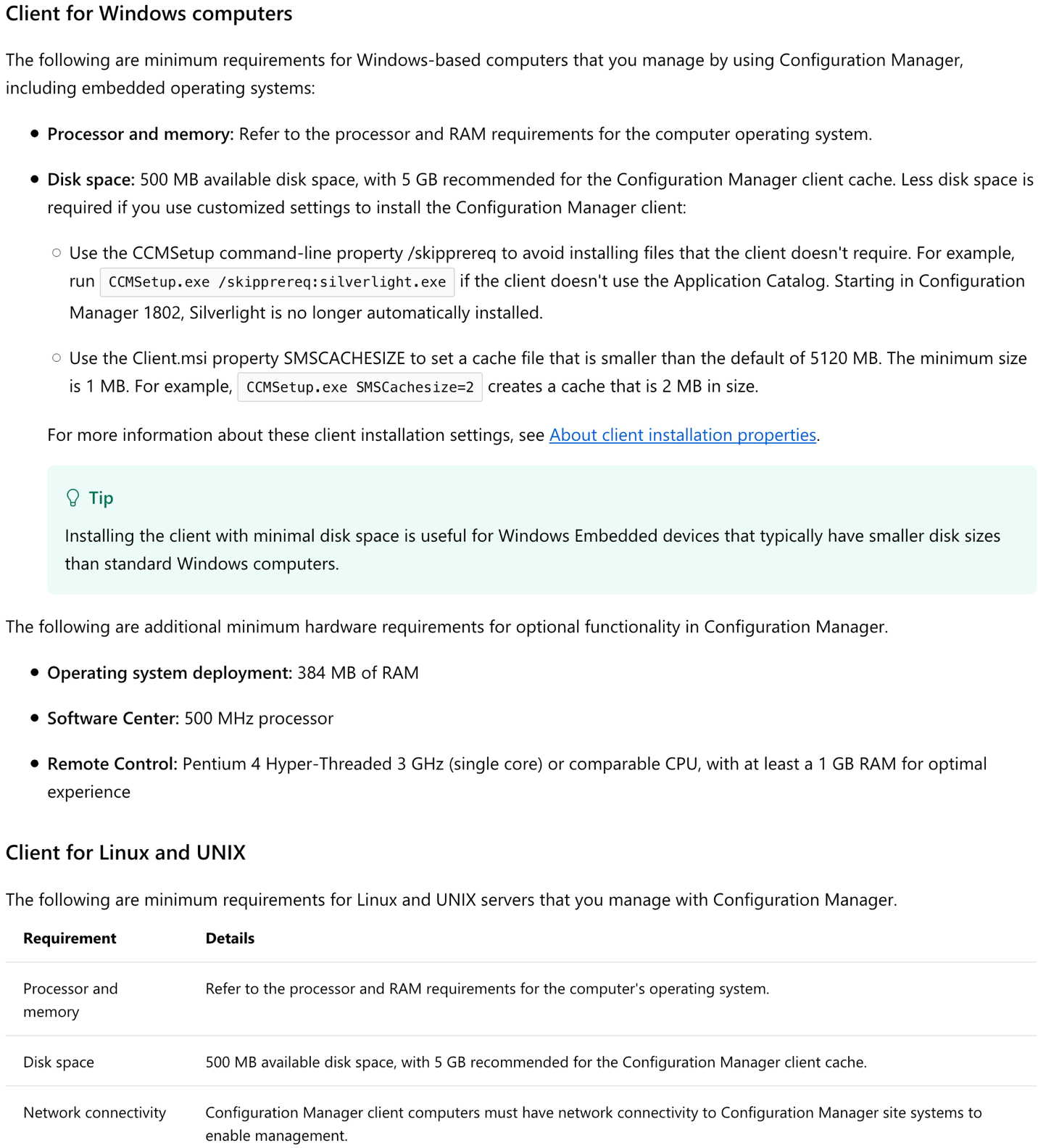
****

**Disk space for site systems**

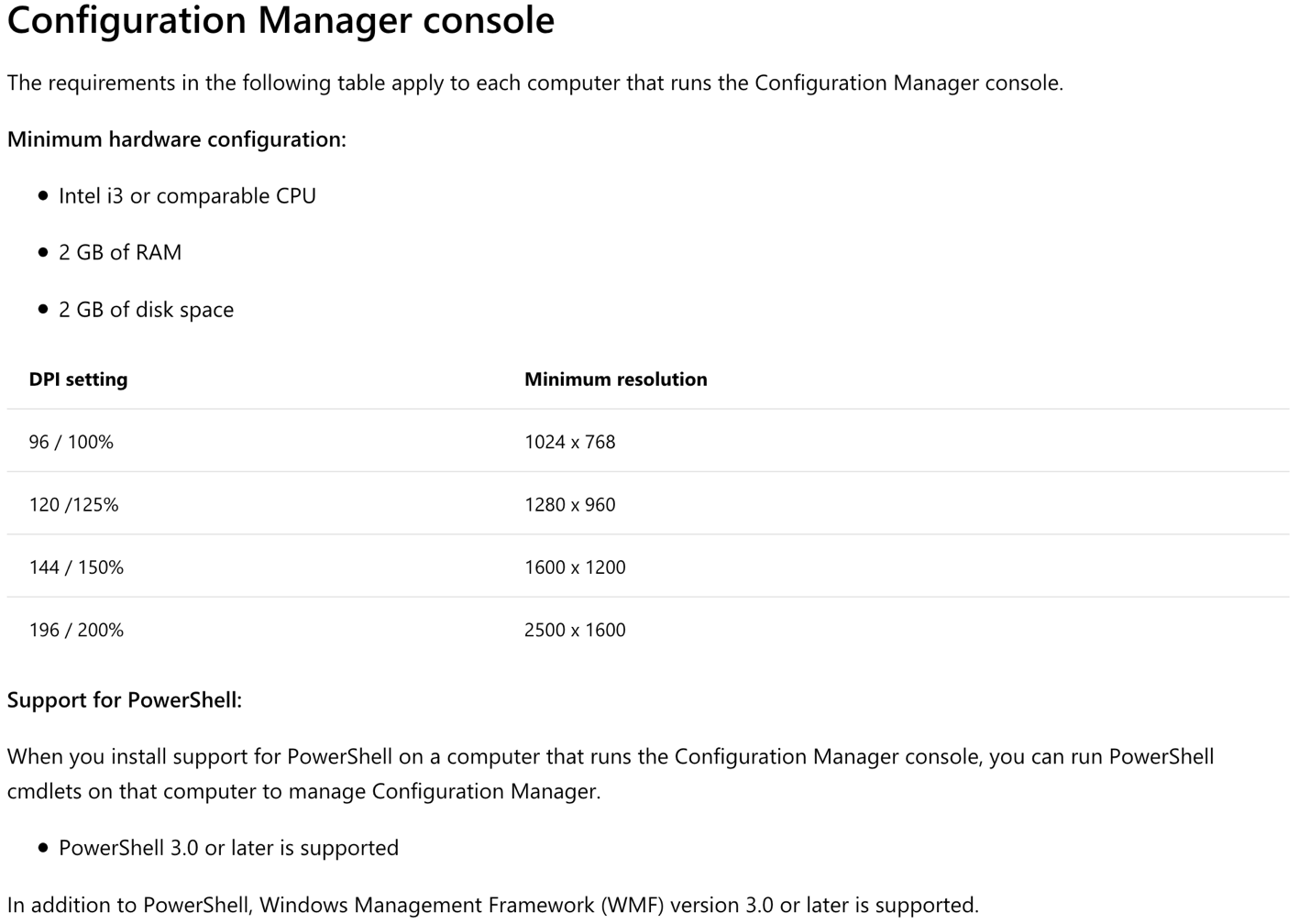
****

**5.2 Clients**

This section provides recommended hardware configurations for computers that you manage by using Configuration Manager client software.



**5.3 Configuration Manager console**



**Supported configurations**

**Supported configurations for System Center Configuration Manager can be found** [here](https://docs.microsoft.com/en-us/sccm/core/plan-design/configs/supported-configurations)**.**