



Microsoft® System Center Configuration Manager 2007 Network Access Protection

Microsoft®
System Center

Assess, Deploy and Update from Desktops to Data Centers and Beyond

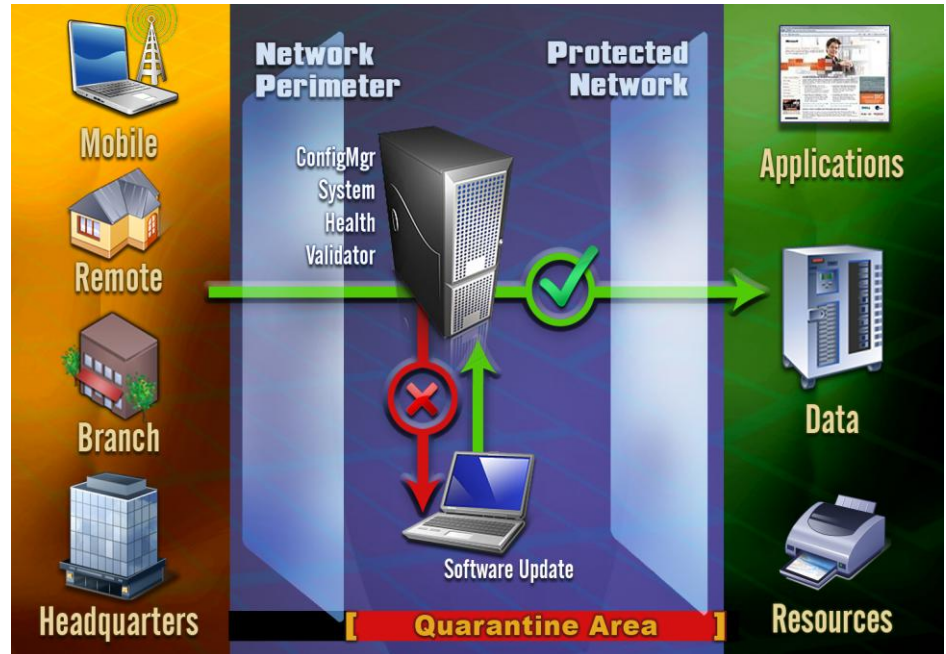
Today's increasingly mobile workforce and the need for interconnectivity between partners and customers present an entirely new set of challenges for IT departments. In addition to ensuring that the desktop computers on the network are up-to-date and meet the company's requirements for system health, network perimeters must also protect networks from roaming devices that may be vulnerable to security exploits.

Configuration Manager 2007 helps protect the integrity of private networks by enforcing compliance with software updates. Through integration with Network Access Protection (NAP), a policy enforcement platform built into Microsoft Windows Vista and Windows Server 2008, Configuration Manager 2007 helps provide continuous network protection and quarantine support for both perimeter and online systems to ensure that computers connecting or communicating on the network meet the organization's requirements for system health.

Securing the Network Perimeter

The threat of malicious software targeting known vulnerabilities on unpatched systems and increasing concerns with regulatory compliance make managing the health of computers that access private networks a top priority for IT organizations. Yet users are increasingly accessing their company's network with devices that are sometimes out of the immediate control of IT.

For example, while laptops and mobile devices give users the flexibility to work from where ever they are these devices



frequently leave and return to the company network. This presents a health threat because these devices are often accessing unprotected public-facing networks like the Internet. What's more, while these devices are away from the company network they might not receive the most recent software updates or configuration changes. Users connecting with their home computers present similar problems.

Visiting laptops and mobile devices are also system health threats. While companies often need to provide network access to consultants, business partners and other guests, to protect their network IT departments must ensure that these devices meet the company's requirements for system health.

Configuration Manager and NAP give IT organizations better control over the

computers that access their private networks by validating a computer's health before allowing network access or communication, and optionally confining non-compliant devices to a restricted network until they meet system health policies. Configuration Manager can then automatically update compliant devices to ensure that they always meet system health policies.

System Health Policies

With NAP, IT administrators can create customized health requirement policies such as requiring that a firewall must be installed and enabled and the latest operating system updates must be installed before a device can access the network. Configuration Manager NAP policies let IT administrators define which software updates to include and specify a date by which the device must be compliant.



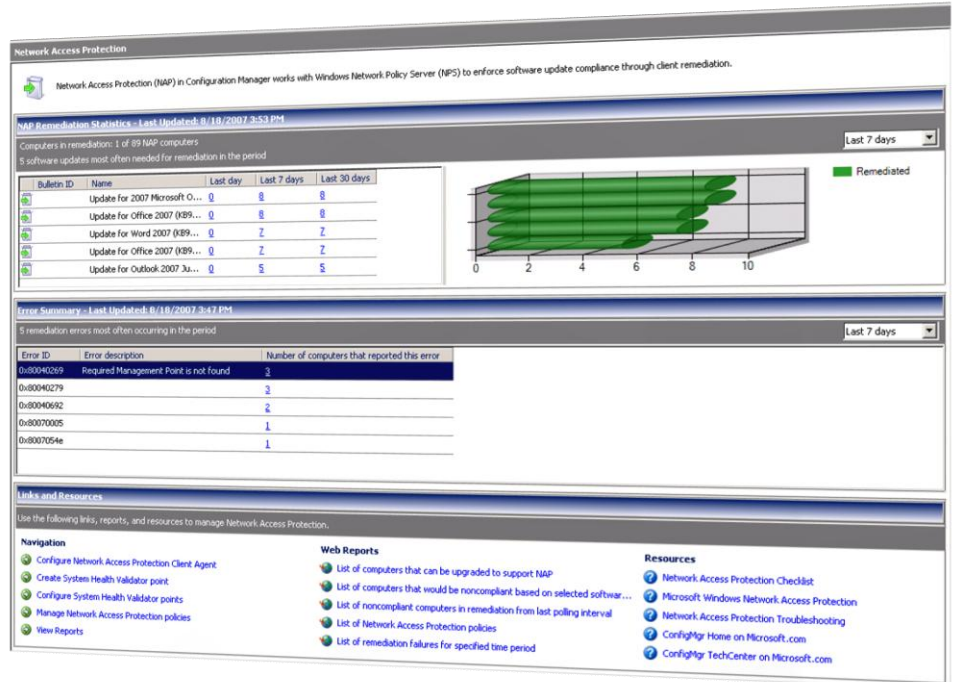
Configuration Manager NAP policies give IT departments the flexibility to support their unique business requirements. For example, they can enforce compliance of software updates as part of a phased deployment, enabling updates through standard mechanisms by a certain target date. Or, they can enforce compliance as part of an expedited deployment to address an urgent software update, such as a zero-day exploit.

Enforcing Compliance

NAP in Configuration Manager works in conjunction with Microsoft Windows Network Policy server to enforce compliance with software updates. When a Configuration Manager client with NAP support attempts to connect to a NAP and Configuration Manager enabled network, the client evaluates whether it has all the required software updates by their effective date. The client passes this information in a statement of health (SoH) to the Configuration Manager System Health Validator, which passes the client's compliant or non-compliant health state to the Network Policy Server. If the client is non-compliant, IT administrator-defined policies on the Network Policy Server then determine whether Configuration Manager will remediate the client and whether the client will have restricted (quarantined) or unrestricted network access until they are compliant.

Remediating Non-Compliance

Configuration Manager remediates non-compliant devices through the software updates feature. Software Update



Management in Configuration Manager is built on familiar Windows Server Update Services (WSUS), providing a unified infrastructure for all security and non-security related updates for Microsoft, 3rd party and line-of-business applications.

Configuration Manager remediation uses software update packages that IT administrators create with the Software Update Management. These packages are stored on Configuration Manager remediation servers that have resources NAP clients need to become compliant with the system health policies.

When Configuration Manager has successfully remediated a client, the client generates a new statement of health reporting compliant status. NAP then removes the client from quarantine gives it unrestricted network access as

long as the device remains in compliance.

The Best Choice for Windows

System Center Configuration Manager is the solution to comprehensively assess, deploy and update servers, clients, and devices—across physical, virtual, distributed and mobile environments—that, optimized for Windows and extensible beyond, is the best choice for gaining enhanced insight into and control over IT systems.

Network Access protection in Configuration Manager provides continuous network protection and quarantine support for both perimeter and online systems helping IT departments ensure that any device that connects to their network meets the company's requirements for system health.

To learn more about System Center Configuration Manager visit <http://www.microsoft.com/systemcenter/configmgr>

© 2006 Microsoft Corporation. All rights reserved. The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication. The information represents the product at the time this document was printed and should be used for planning purposes only. Information subject to change at any time without prior notice. This data sheet is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.

Microsoft, Active Directory, Windows, the Windows logo, and Windows Server System are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other trademarks are property of their respective owners.

Microsoft®
System Center
Knowledge-Driven IT Management