



# Windows Server® 2008

## Network Access Protection



Microsoft®  
**Forefront™**

## **NAP and Forefront Client Security Readiness Assessment**

Summary Proposal

Version 4.0

Created By: Samudra Dutta Gupta, HexCode Technologies K K

Date: Wednesday, September 30, 2009



**Microsoft®**

Use of the Microsoft Assessment and Planning Toolkit ("Toolkit") is completely voluntary on the part of the end user. The information, hardware assessment, or reports contained within or generated by use of the Toolkit are for informational purposes only and Microsoft makes no warranties, express or implied, with respect to the Toolkit or the accuracy of any information or hardware assessments generated as a result of its usage. Additionally, use of the Toolkit cannot be understood as substituting for customized service and information that might be developed by Microsoft Corporation for a particular user based upon that user's particular environment.

# Table of Contents

<b>Executive Overview</b> .....	<b>1</b>
Where Is Your Organization Now?.....	1
Why Network Access Protection? .....	2
Why Forefront Client Security?.....	3
Unified Protection .....	3
Simplified Administration .....	3
Critical Visibility and Control.....	3
Total Cost of Ownership.....	3
<b>Assessment Results Summary</b> .....	<b>4</b>
Readiness Analysis .....	4
NAP Readiness Analysis .....	4
Forefront Readiness Analysis .....	6
<b>Forefront with Network Access Protection</b> .....	<b>8</b>
<b>Next Steps</b> .....	<b>10</b>
<b>Appendix: NAP Migration Pilot Plan</b> .....	<b>11</b>



# Executive Overview

This document summarizes the results from the NAP and Forefront Client Security Readiness Assessment generated by the Microsoft Assessment and Planning (MAP) Toolkit. The accompanying Microsoft Office Excel® workbook, the Security Assessment report, provides detailed information about each inventoried computer on your organization's network.

Based upon information discovered about your computer environment, this document provides specific recommendations for improving the overall security of your network. In addition, it provides an overview of the integration between Microsoft® Network Access Protection (NAP) and Microsoft Forefront™ Client Security, enabling network administrators to assess the health of networked computers before accessing them.

This assessment describes the current status of your firewall, antivirus, and antispyware products as reported by Windows Security Center as well your environment's readiness to support client software for NAP and Forefront Client Security.

Inventory results (data, charts, and tables) shown in this summary document are for computers that are already running a Windows® operating system, such as Windows XP Professional, Windows Vista® or Windows 7®.

## *Where Is Your Organization Now?*

According to the assessment, your organization could realize the benefits of a comprehensive line-of-business (LOB) security product that integrates through your existing IT infrastructure.

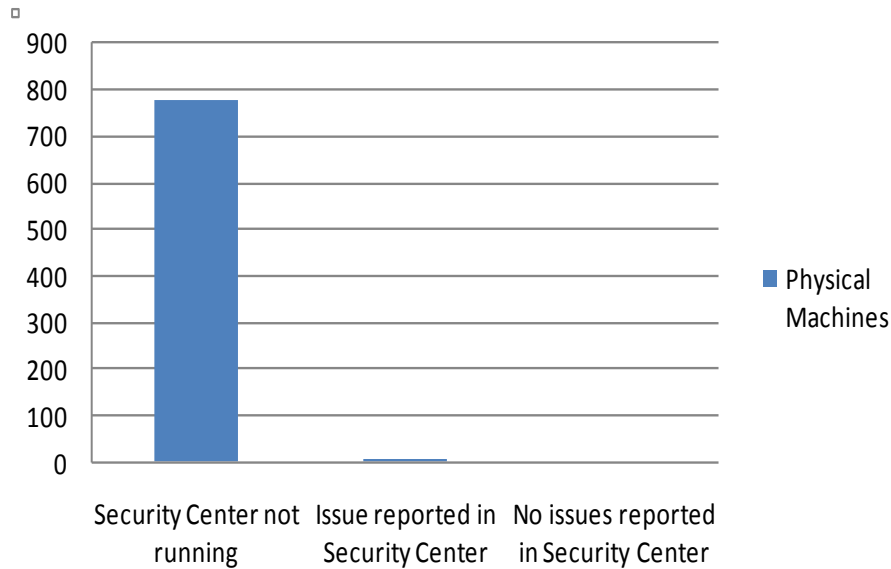
You can use the accompanying Security Assessment report, along with the Windows Vista Hardware and Windows Server 2008 Hardware assessment reports, as a source of detailed information about the state of the firewall, antivirus, and antispyware products installed in your organization as well as the operating systems, hardware components, and installed software found in your computer environment. This information can help you improve the overall security of your organization's IT infrastructure while simplifying administration and reducing the costs of these efforts.

The following table summarizes the overall discovery and inventory of your computer environment.

**Table 1. Inventory Results Overall Summary**

Description	Physical Computer Count
Inventoried client computers	776
Inventoried servers	109
Insufficient Data	0
Total	885

During the inventory process, MAP discovered 776 physical machines running a Windows client operating system. At this time, 100 percent of the client machine population requires a review of their Security Center, firewall, antivirus, or antispyware settings. The chart and accompanying table provide a summary of the security assessment results.



**Figure 1. Client inventory requiring a security review**

For more information about [Windows Security Center](http://go.microsoft.com/fwlink/?LinkId=129573), see <http://go.microsoft.com/fwlink/?LinkId=129573>. The following table provides detailed information about the Security Center analysis.

**Table 2. Security Center Analysis Details**

Area Assessed	Not Found	Not Running	Out-of-Date
Firewall	0	0	N/A
Antivirus	1	0	0
Antispyware	0	0	0
Security Center	N/A	775	N/A
Total	1	775	0

## *Why Network Access Protection?*

Exposure of client devices to malicious software, such as viruses and worms, continues to increase. When these programs gain entry to an unprotected or incorrectly configured host system, they can use this system as a staging point to propagate to other devices on the corporate network. A new set of operating system components is included with Windows 7, Windows Server 2008, Windows Server 2008 R2, Windows Vista, and Windows XP with Service Pack 3 that provides network administrators with a platform to help ensure that client computers on a private network meet administrator-defined requirements for system health.

NAP enforces health requirements by monitoring and assessing the health of client computers when those computers attempt to connect or communicate on a network. Client computers that are not in compliance with the health policy can be provided with restricted network access until their configurations are updated and brought into compliance with policy. Depending on how NAP is deployed, noncompliant clients can be quarantined or automatically updated so that users can quickly regain full network access without having to manually update or reconfigure their computers.

In your environment, NAP can help you with issues like those found during the inventory process (See Table 1) by quickly bringing those machines back into compliance with your specific health policy.

## *Why Forefront Client Security?*

Forefront Client Security provides unified virus and spyware protection for desktops, laptops, and server operating systems that is easy to manage and control. It simplifies administration through centralized management and provides critical visibility into threats and vulnerabilities, helping you protect your business with confidence and efficiency.

### **Unified Protection**

Forefront Client Security delivers unified protection from a broad range of current and emerging threats. It uses a single security agent to provide both real-time and scheduled scanning and to prevent and remove malware on client and server operating systems. It uses the Windows Filter Manager, the Microsoft prescribed scanning platform, to apply “mini-filter” technology for scanning malware in real time. This same technology enables Forefront Client Security to scan for viruses, spyware, and other files before they run, effectively protecting against blended threats and minimizing end-user disruption.

In addition, the Forefront Client Security antimalware engine uses advanced detection technologies, such as static analysis, emulation, heuristics, and tunneling, for comprehensive protection. It also provides advanced cleaning technology to ensure that systems are not only clean, but also returned to a “restored state” and functioning normally after malware has been removed, which is particularly important as threats become increasingly complex.

### **Simplified Administration**

Forefront Client Security simplifies administration by centralizing management on a single console, saving time and reducing complexity. The Forefront Client Security management server configures and updates the malware protection agents, as well as generates reports and alerts about the security of your environment. Forefront Client Security protects and manages up to 10,000 computers in standard deployments. For organizations with more than 10,000 protected systems, Forefront Client Security Enterprise Manager enables administrators to centrally manage multiple Forefront Client Security deployments in their enterprise environments, aggregate reporting and alerting, and initiate enterprise-wide malware scanning.

Forefront Client Security uses Group Policy to configure security agents and Windows Server Update Services (WSUS) to distribute definition updates. Administrators can also choose to use other software distribution systems for policy, signature, or software deployment. Forefront Client Security uses database and reporting systems from Microsoft SQL Server®.

### **Critical Visibility and Control**

Forefront Client Security produces insightful, prioritized security reports, so you have visibility into and control over malware threats. The Forefront Client Security Summary Report provides key information on the state of security within your environment along with a snapshot of the top trends and issues that administrators can use to take action against threats or communicate to management. Administrators can also quickly investigate report details because each report is hyperlinked directly to the critical underlying data. You can schedule to have reports delivered regularly through e-mail.

Finally, Forefront Client Security provides state assessment scans to help determine which managed computers need updates or are not configured securely. Its reporting enables administrators to measure the risk profile for their organization based on security best practices. Security alerts create notifications when threats appear in the environment, eliminating the need to search through volumes of data.

### **Total Cost of Ownership**

According to a current total cost of ownership (TCO) study performed by Value Prism Consulting on Forefront Client Security, customers experienced noticeable savings and cost reductions using this

solution: 85 percent average reduction in security issues, 75 percent average security issue response time reduction, and an average of 24.00 (USD) annual TCO savings per computer.

## Assessment Results Summary

According to the assessment performed using the MAP Toolkit, your organization could benefit from implementing central security controls within your client operating system environment in a very short time.

The assessment discovered and successfully inventoried 885 physical computers running in your environment. Using the data from the Forefront TCO study, this represents a yearly savings opportunity of 21,240.00 (USD) for an organization of your size.

### *Readiness Analysis*

With the results of the Security Assessment report and this proposal document, you can make informed decisions about the deployment of Network Access Protection (NAP) and Forefront Client Security in your organization. The information in this section summarizes the results of the assessment conducted on your network and describes what is required to make NAP and Forefront Client Security work for your organization.

### **NAP Readiness Analysis**

The following sections provide you with an assessment of your readiness to deploy NAP in your environment based upon the inventory performed to date.

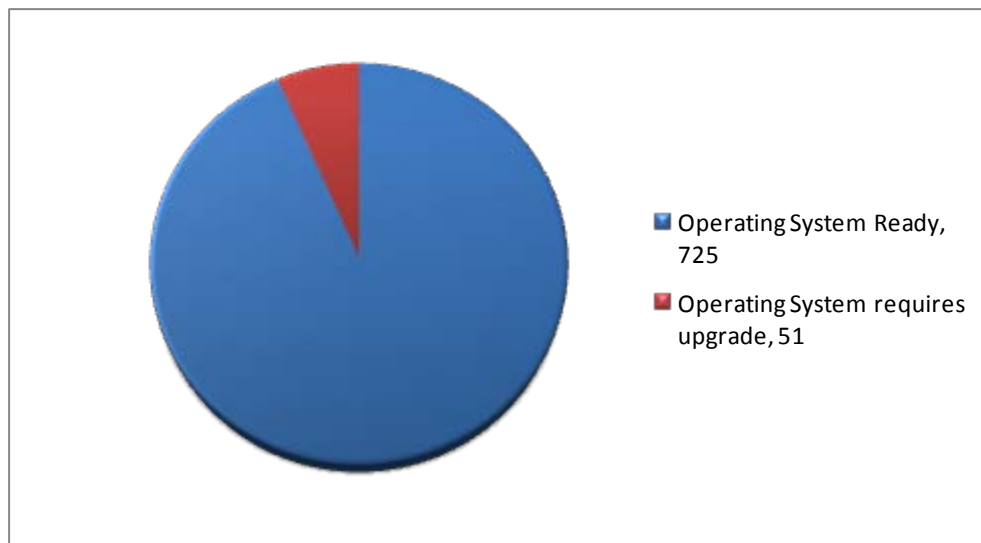
#### ***NAP Client Agent Readiness***

During the inventory and assessment process, MAP discovered the Windows client operating systems and versions listed in the following table.

**Table 3. Client Operating System Inventory Results**

<b>Operating System Name and Version</b>	<b>Count</b>
Microsoft Windows XP Professional with Service Pack 2	3
Microsoft Windows XP Professional with Service Pack 3	53
Windows 2000 Professional with Service Pack 4	4
Windows 7 Ultimate	1
Windows XP Professional with Service Pack 2	38
Windows XP Professional with Service Pack 3	677
Total	776

To run the NAP client, an operating system must be running Windows XP with SP3, Windows Vista, or Windows 7. The following figure summarizes the NAP Readiness Assessment results in terms of the client operating systems found during the inventory process.



**Figure 2. NAP Client Readiness Summary**

Additionally, each client computer must have the NAP Agent service and the DHCP service Start Modes set to Auto. The following table shows the readiness of your physical client computer environment in terms of those services.

**Table 4. Client Operating Systems Service Start Mode Readiness**

Service Readiness	Ready Count	Not Ready Count
NAP Agent service	0	776
DHCP Service	776	0
EAP Service	0	776

### **Windows Vista and Windows 7 Readiness**

To help you better understand your environment's readiness to run Windows Vista, the MAP tool provides a Windows Vista and a Windows 7 Readiness assessment. By using these features, you will receive a detailed report on the hardware, devices, and applications running in your network. Additionally, this information is summarized in documents that prescribe your next steps in a very specific and actionable manner.

For more information about this scenario and other scenarios that the [MAP](http://go.microsoft.com/fwlink/?LinkId=130699) tool supports, see <http://go.microsoft.com/fwlink/?LinkId=130699>.

### **NAP Server Requirements**

During the inventory and assessment, MAP assessed your Windows server operating systems. The following table shows the results by operating system and version.

**Table 5. Server Operating System Inventory Results**

Operating System Name and Version	Count
Microsoft(R) Windows(R) Server 2003 Enterprise x64 Edition with Service Pack 2	1
Microsoft(R) Windows(R) Server 2003, Enterprise Edition with Service Pack 1	1
Microsoft(R) Windows(R) Server 2003, Enterprise Edition with Service Pack 2	2
Windows 2000 Server with Service Pack 4	2
Windows Server 2003 with Service Pack 1	11

Operating System Name and Version	Count
Windows Server 2003 with Service Pack 2	92
Total	109

To run NAP, your IT infrastructure will require servers running Windows Server 2008 and at least one the following:

- Network Policy Server that provides centralized health policy configuration and evaluation of NAP client health state.
- Routing and Remote Access that provides health requirements enforcement for remote access virtual private network connections.
- Dynamic Host Configuration Protocol (DHCP) that provides health requirements.

Based upon the inventory and assessment that MAP has performed to date, the following table indicates the readiness of your environment to support these requirements.

**Table 6. NAP Server Infrastructure Readiness**

Server Role	Found in your environment?
Windows Server 2008 or Windows Server 2008 R2	No
Network Policy Server	No
Routing and Remote Access Server	Yes
DHCP Server	Yes

To fully support your environment with Forefront Client Security, you will need 1 or more NAP servers. MAP has found 0 servers running Windows Server 2008. Monitor the performance of these Windows Server 2008-based servers to ensure that the NAP workload can be supported by these computers. If not, use the Windows Server 2008 Hardware Assessment report to determine which computers meet the hardware requirements for this operating system and plan your migration.

### **Windows Server 2008 Readiness**

To help you better understand your environment's readiness to run Windows Server 2008 and Windows Server 2008 R2, the MAP tool provides Windows Server 2008 and Windows Server 2008 R2 Readiness assessments. These assessments provide a detailed report on the hardware capabilities and server roles and services currently running in your environment. Additionally, you will receive a summary of this information in a document that provides specific and actionable next steps to achieve your migration goals.

For more information about this scenario and other scenarios that the [MAP](#) tool supports, see <http://go.microsoft.com/fwlink/?LinkId=130699>.

### **Selecting the Right NAP Architecture**

When deploying NAP, organizations can choose from several enforcement methods. Each method has strengths and drawbacks with regard to complexity, ease of deployment, and cost. To plan your NAP migration, use the Infrastructure Planning and Design (IPD) Guide for [Selecting the Right NAP Architecture](#) at <http://go.microsoft.com/fwlink/?LinkId=129574>.

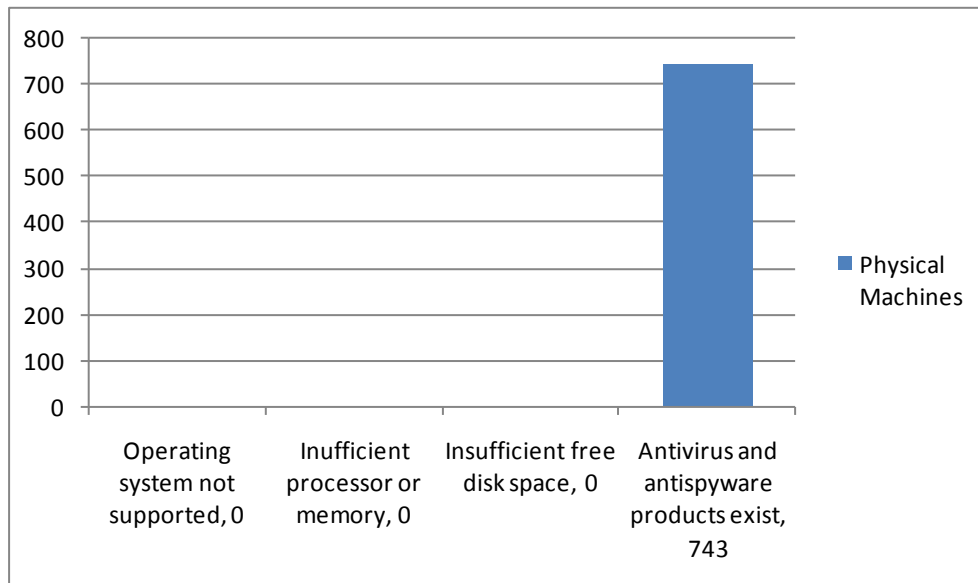
## **Forefront Readiness Analysis**

Forefront Client Security provides unified virus and spyware protection for business desktops, laptops, and server operating systems that is easy to manage and control. Based upon the inventory performed to date, the following sections provide you with an assessment of your readiness to deploy Forefront Client Security in your environment.

### **Forefront Client Agent Readiness**

The first step in planning your implementation of Forefront Client Security is to understand the readiness of your infrastructure. Microsoft Forefront Client Security is designed to protect Windows 2000 SP4, Windows XP SP2 or later, Windows Server 2003 SP1 or later, Windows Server 2008 (including Hyper-V technology), Windows Vista and Windows 7 based systems. It supports real-time virus and spyware protection for 32- and 64-bit operating system environments.

MAP has found that 142 physical machines meet the minimum requirements for the Forefront Client Security agent software. It also found that 743 will require upgrades as indicated below.



**Figure 3. Forefront Client Security Readiness Summary**

#### ▪ Other Antispyware or Antivirus Software

Forefront Client Security does not support running other antispyware or antivirus software in conjunction with Forefront Client Security. Before installing Forefront Client Security on a client computer, you must disable or uninstall any existing antispyware or antivirus software on that computer.

#### **Forefront Client Security Server Infrastructure Requirements**

- 1 GHz processor; minimum 1 GB of RAM; 6 GB of available hard-disk space or more required
- Microsoft Windows Server 2003 SP1 Standard Edition or Enterprise Edition, or Windows Server 2003 R2 Standard Edition or Enterprise Edition, or Windows Server 2008 operating system.
- Microsoft SQL Server 2005 Enterprise Edition or Standard Edition with SP1 (including Database Services, Reporting Services, Workstation Components, and Integration Services).
- Windows Server Update Services (WSUS) 2.0 with SP1 or Windows Server Update Services 3.0.

For [detailed system requirements](http://go.microsoft.com/fwlink/?LinkId=129576), see <http://go.microsoft.com/fwlink/?LinkId=129576>.

#### ▪ Windows Server Update Services

Forefront Client Security uses WSUS to download the agent components and definition and engine updates from Microsoft Update and distribute the updates to the Forefront Client Security agents in your organization.

WSUS allows you to choose whether to store information about updates in a SQL Server database or in a Microsoft SQL Server Desktop Engine (MSDE) database. Due to the large number of Forefront Client Security updates that WSUS will download from Microsoft Update, it is highly recommended that you install the WSUS server for Forefront Client Security to a SQL Server database. Malware definition updates are distributed from Microsoft Update. Client Security simplifies the distribution of definition updates to client computers through optimization with WSUS.

You can also use any existing software distribution system in your environment. For more information about receiving and distributing definitions, see the "[Distributing definitions and engine updates](#)" chapter in the Forefront Client Security Administrator's Guide, at <http://go.microsoft.com/fwlink/?LinkId=87350>.

- **Active Directory**

Forefront Client Security uses Group Policy to define the settings for the Forefront Client Security agent on managed computers. Group Policy determines when to perform malware and SSA scans, when to raise alerts, when to download definition updates, and how much control your users have over the Forefront Client Security settings.

You can deploy Group Policy to the domain, organizational units (OUs), security groups, or existing Group Policy objects (GPOs) by using the Client Security console.

- **System Center Operations Manager**

Forefront Client Security setup installs Microsoft Operations Manager (MOM) 2005. Your use of an existing installation of MOM instead is not supported. When using the Client Security installation of MOM 2005, be aware of the following issues:

- Changing the MOM settings specified by Forefront Client Security is not supported.
- MOM agentless management is not supported. All of the managed client computers must have the MOM agent installed on them.
- In cases where you have an existing installation of MOM 2005, MOM 2000, or Microsoft System Center Operations Manager 2007, you can continue to use that installation in conjunction with the installation of MOM 2005 associated with Forefront Client Security. All three versions support multihomed MOM agents, which allow your client computers to communicate with both your existing MOM server and the MOM server associated with Forefront Client Security.

### SQL Server 2005

Forefront Client Security uses SQL Server 2005 to store information reported from the managed computers in the organization. Forefront Client Security uses two databases to store data:

- Forefront Client Security collection database (also called the MOM OnePoint database)
- Forefront Client Security reporting database (also called the MOM SystemCenterReporting database)

The following table provides an assessment of your readiness to support these components.

**Table 7. Forefront Client Security Server Infrastructure Readiness**

Server Role, Service or Application	Found in Your Environment?
Windows Server Update Services	Yes
Active Directory	Yes
System Center Operations Manager	No
SQL Server 2005	Yes

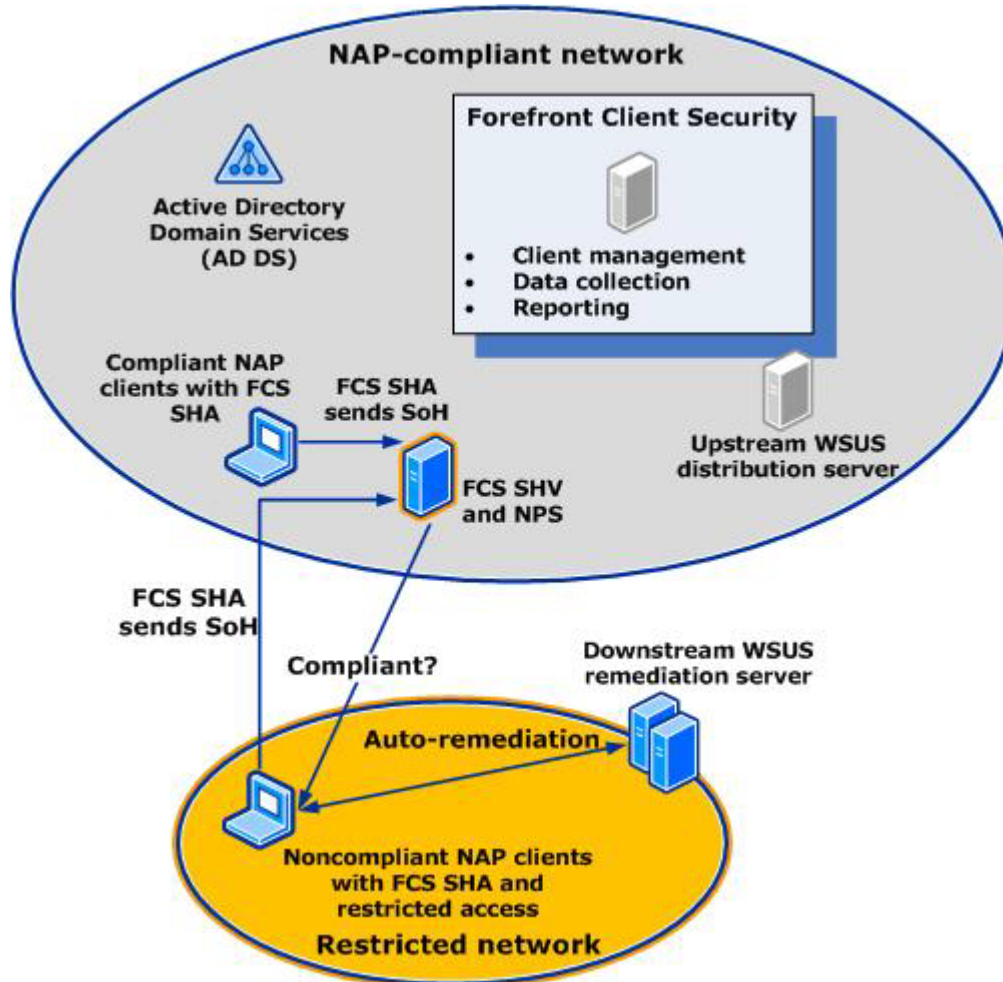
## Forefront with Network Access Protection

The Microsoft Forefront Integration Kit for Network Access Protection integrates Forefront Client Security and NAP. Together, these two Microsoft technologies can provide an additional defense-in-depth layer against malicious attacks and give administrators a significant degree of control over the security and health of networked computers.

You can use this integration kit to help protect your network infrastructure by configuring a Forefront Client Security compliance health policy across your network, monitoring the operational health of Forefront Client Security in real time, and remediating problems that arise.

The integration kit includes the following functionalities and components:

- **Configure.** The kit's System Health Validator (SHV) establishes the Forefront Client Security compliance health policy that will be enforced on managed computers. For example, Forefront Client Security must be installed, running, and its signature files must be up-to-date.
- **Monitor.** The kit's System Health Agent (SHA) component monitors in real time the health of the computers on which the SHA and Forefront Client Security are installed to ensure they comply with the organization's health policy.
- **Remediate.** If NAP detects a compliance issue with Forefront Client Security on one of the managed computers, NAP will attempt to remediate the issue or restrict the computer's access to network resources, depending on the health policies.



**Figure 4. Microsoft Forefront Integration Kit for Network Access Protection components**

For more information or to download the [Microsoft Forefront Integration Kit for Network Access Protection](http://go.microsoft.com/fwlink/?LinkId=129577), see <http://go.microsoft.com/fwlink/?LinkId=129577>.

## Next Steps

1. Review results of the Security Assessment report and take steps to remediate security risks identified in your client environment.
2. Review and understand [NAP deployment scenarios and components](http://go.microsoft.com/fwlink/?LinkId=129578) by visiting <http://go.microsoft.com/fwlink/?LinkId=129578>.
3. Plan your Network Access Protection deployment. Use the [Selecting the Right NAP Architecture IPD guide](http://go.microsoft.com/fwlink/?LinkId=129574) at <http://go.microsoft.com/fwlink/?LinkId=129574>.
4. [Review the pilot and enforcement modes](http://go.microsoft.com/fwlink/?LinkId=129582) in the Appendix. For more information, see <http://go.microsoft.com/fwlink/?LinkId=129582>.
5. Plan your Forefront Client Security deployment. [Understand system requirements and best practices for planning and integration](http://go.microsoft.com/fwlink/?LinkId=129583). See <http://go.microsoft.com/fwlink/?LinkId=129583>.

## Appendix: NAP Migration Pilot Plan

The following table outlines best practice stages for deploying NAP in your IT infrastructure.

**Table A. NAP Deployment Best Practices**

Stage	Description	Benefit
Lab pilot	Set up NAP in a lab using step-by-step documentation.	Familiarity with product and processes.
Architecture, design, and threat modeling	Identify threats, decide on enforcement types, identify pilot sites.	Add new enforcement types as needed per the architecture and design.
Reporting mode pilot	Deploy NAP to report compliance levels. Start with a contained site or subnet and expand.	Ongoing state of compliance reported, automatic remediation initiated.
Guest access pilot	Restrict connectivity of unauthenticated users and devices (for example, Guest VLAN or IPsec SDI).	Server infrastructure is protected from guests.
Deferred enforcement pilot	Notify users of noncompliance. Identify reasons for noncompliance and address. Stay in this mode until 90 percent + compliant.	Help desk impact understood, users start fixing themselves manually, update infrastructure improved.
Enforcement mode pilot	Lock out noncompliant users based on group membership.	Noncompliant systems are isolated until healthy.
Add health agents	Add additional health agents. Configure NAP to first report and then later enforce compliance levels that are sufficiently high.	Additional criteria for compliance added.
Add sites, scale out	Scale beyond initial pilot into global deployment.	NAP benefits realized throughout the corporate environment.
Repeat process for new enforcement types	Add new enforcement types as needed per the architecture and design.	Additional threats are mitigated.