[MS-WSH]:
Windows Security Health Agent (WSHA) and Windows Security Health Validator (WSHV) Protocol Specification

Revision Summary

Date	Revision History	Revision Class	Comments
04/10/2007	1.0		Version 1.0 release
05/18/2007	1.2		Version 1.2 release
06/08/2007	1.2.1	Editorial	Revised and edited the technical content.
07/10/2007	1.2.2	Editorial	Revised and edited the technical content.

Date	Revision History	Revision Class	Comments
08/17/2007	1.2.3	Editorial	Revised and edited the technical content.
09/21/2007	1.2.4	Editorial	Revised and edited the technical content.
10/26/2007	1.2.5	Editorial	Revised and edited the technical content.
01/25/2008	2.0	Major	Updated and revised the technical content.

Table of Contents

1 Introduction 4
1.1 Glossary 4
1.2 References 5
1.2.1 Normative References 5
1.2.2 Informative References 5
1.3 Protocol Overview (Synopsis) 5
1.4 Relationship to Other Protocols 5
1.5 Prerequisites/Preconditions 5
1.6 Applicability Statement 6
1.7 Versioning and Capability Negotiation 6
1.8 Vendor-Extensible Fields 6
1.9 Standards Assignments 6

2 Messages 7
2.1 Transport 7
2.2 Message Syntax 7
2.2.1 WSHA SoH 7
2.2.2 WSHV SoHR 13
2.2.3 NAPSystemHealthID 17
2.2.4 Flag 17
2.2.5 Version 17
2.2.6 HealthClassID 17
2.2.7 ProductName 18
2.2.8 ClientStatusCode 18
2.2.9 DurationSinceLastSynch 22
2.2.10 WSUSServerName 22
2.2.11 UpdatesFlag 22
2.2.12 ComplianceCode1 23
2.2.13 ComplianceCode2 27
2.2.13.1 Antivirus and Antispyware 27
2.2.13.2 Security Updates 27

3 Protocol Details 29
3.1 Common Details 29
3.1.1 Abstract Data Model 29
3.1.2 Timers 31
3.1.3 Initialization 31
3.1.4 Higher-Layer Triggered Events 31
3.1.5 Message Processing Events and Sequencing Rules 31
3.1.5.1 General Problems 31
3.1.5.2 SoHR Response to SoH Messages 31
3.1.6 Timer Events 36
3.1.7 Other Local Events 36

4 Protocol Example 37

5 Security 38
5.1 Security Considerations for Implementers 38
5.2 Index of Security Parameters 38

6 Appendix A: Windows Behavior 39

7 Index 40

1 Introduction

The Windows Security Health Agent (WSHA) and Windows Security Health Validator (WSHV) Protocol is included in the packet payload specified in the **Statement of Health (SoH)** for the **Network Access Protection (NAP)** Protocol, as specified in [MS-SOH]. The WSHA reports the system security health state to the WSHV, which responds with **quarantine** and **remediation** instructions if the status reported is not compliant with the defined security health policy. If the status is compliant with the security health policy, the WSHV responds by allowing the client into the network.

This document includes the following:

- How messages are transported and message syntax in section 2.
- Protocol details including abstract data models, state machines, and message processing rules in section 3.
- A protocol example in section 4.
- Security considerations for implementers in section 5.
- An appendix of Windows behavior in section 6.
- An index in section 7.

1.1 Glossary

The following terms are defined in [MS-GLOS]:

Network Access Protection (NAP)
Statement of Health (SoH)
Statement of Health Response (SoHR)

The following terms are specific to this document:

Network Policy Server (NPS): For Windows Server 2008, **NPS** replaces the Internet Authentication Service (IAS) in Windows Server 2003. **NPS** acts as a health policy server for the following technologies:

- Internet Protocol security (IPsec) for host-based authentication
- IEEE 802.1X authenticated network connections
- Virtual private networks (VPNs) for remote access
- Dynamic Host Configuration Protocol (DHCP)

Quarantine: The isolation of a non-compliant computer from protected network resources.

Remediation: Bringing a non-compliant computer into a compliant state.

Security Updates: The software patches released by Microsoft to fix known security issues in released Microsoft software.

MAY, SHOULD, MUST, SHOULD NOT, MUST NOT: These terms (in all caps) are used as specified in [RFC2119]. All statements of optional behavior use either MAY, SHOULD, or SHOULD NOT.

1.2 References

1.2.1 Normative References

We conduct frequent surveys of the normative references to assure their continued availability. If you have any issue with finding a normative reference, please contact dochelp@microsoft.com. We will assist you in finding the relevant information. Please check the archive site, http://msdn2.microsoft.com/en-us/library/E4BD6494-06AD-4aed-9823-445E921C9624, as an additional source.

[MS-GLOS] Microsoft Corporation, "Windows Protocols Master Glossary", March 2007.

[MS-SOH] Microsoft Corporation, "Statement of Health for Network Access Protection (NAP) Protocol Specification", July 2006.

[MSFT-MSRC] Microsoft Corporation, "Microsoft Security Response Center Security Bulletin Severity Rating System (Revised, November 2002)", November 2002, http://www.microsoft.com/technet/security/bulletin/rating.mspx

If you have any trouble finding [MSFT-MSRC], please check here.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997, http://www.ietf.org/rfc/rfc2119.txt

1.2.2 Informative References

[ITUX680] ITU-T, "Abstract Syntax Notation One (ASN.1): Specification of Basic Notation", Recommendation X.680, July 2002, http://www.itu.int/ITU-T/studygroups/com17/languages/X.680-0207.pdf

1.3 Protocol Overview (Synopsis)

The Windows Security Health Agent (WSHA) and Windows Security Health Validator (WSHV) Protocol uses the Statement of Health (SoH) for the Network Access Protection (NAP) Protocol (as specified in [MS-SOH]) to transport a client's security health state to a corresponding **network policy server (NPS)** in a Statement of Health (SoH) message, and then to return remediation instructions to the client in a **Statement of Health Response (SoHR)** message.

1.4 Relationship to Other Protocols

The Windows Security Health Agent (WSHA) and Windows Security Health Validator (WSHV) Protocol MUST be carried in the Statement of Health (SoH) for the Network Access Protection (NAP) Protocol, as specified in [MS-SOH].

1.5 Prerequisites/Preconditions

For a Windows Security Health Agent (WSHA) and Windows Security Health Validator (WSHV) Protocol exchange to occur, there must be a Statement of Health (SoH) for the Network Access Protection (NAP) Protocol (as specified in [MS-SOH]) session with a suitable transport protocol established between the client and a health policy server. There must also be WSHA and WSHV client and server components running on the client and health policy server, respectively.

1.6 Applicability Statement

The Windows Security Health Agent (WSHA) and Windows Security Health Validator (WSHV) Protocol is applicable only in an environment in which Network Access Protection (NAP) is being used, and the Network Access Protection (NAP) service is enabled on the client computer.

1.7 Versioning and Capability Negotiation

The Windows Security Health Agent (WSHA) reports its version in the Statement of Health (SoH), as specified in section 2.2.5. The Windows Security Health Validator (WSHV) parses the status and enforces the policy differently, depending on the WSHA version.

1.8 Vendor-Extensible Fields

The Windows Security Health Agent (WSHA) and Windows Security Health Validator (WSHV) Protocol does not include any vendor-extensible fields.

1.9 Standards Assignments

The Windows Security Health Agent (WSHA) and Windows Security Health Validator (WSHV) Protocol has no standards assignments.

2 Messages

The following sections specify how Windows Security Health Agent (WSHA) and Windows Security Health Validator (WSHV) Protocol messages are transported and WSHA and WSHV Protocol message syntax.

2.1 Transport

The Windows Security Health Agent (WSHA) and Windows Security Health Validator (WSHV) Protocol does not provide its own transport. It MUST be carried in the Statement of Health (SoH) for the Network Access Protection (NAP) Protocol, as specified in [MS-SOH].

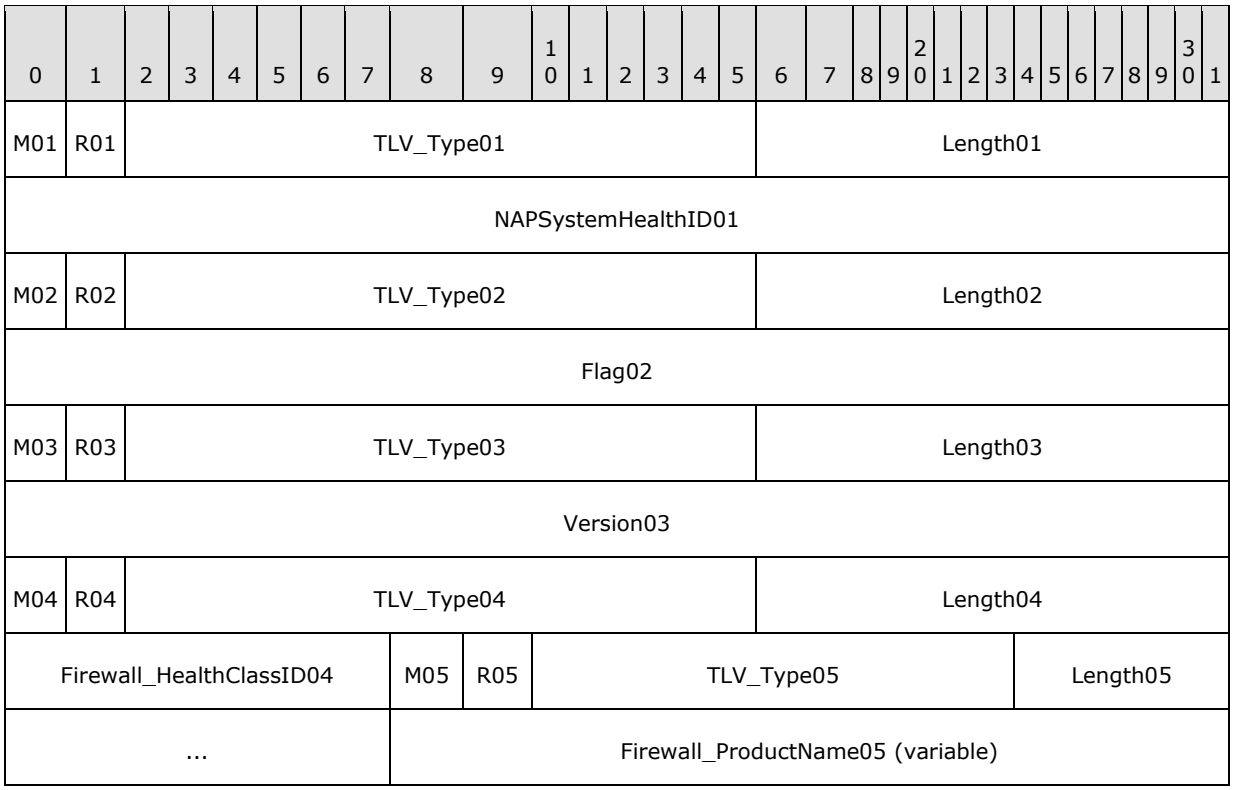
2.2 Message Syntax

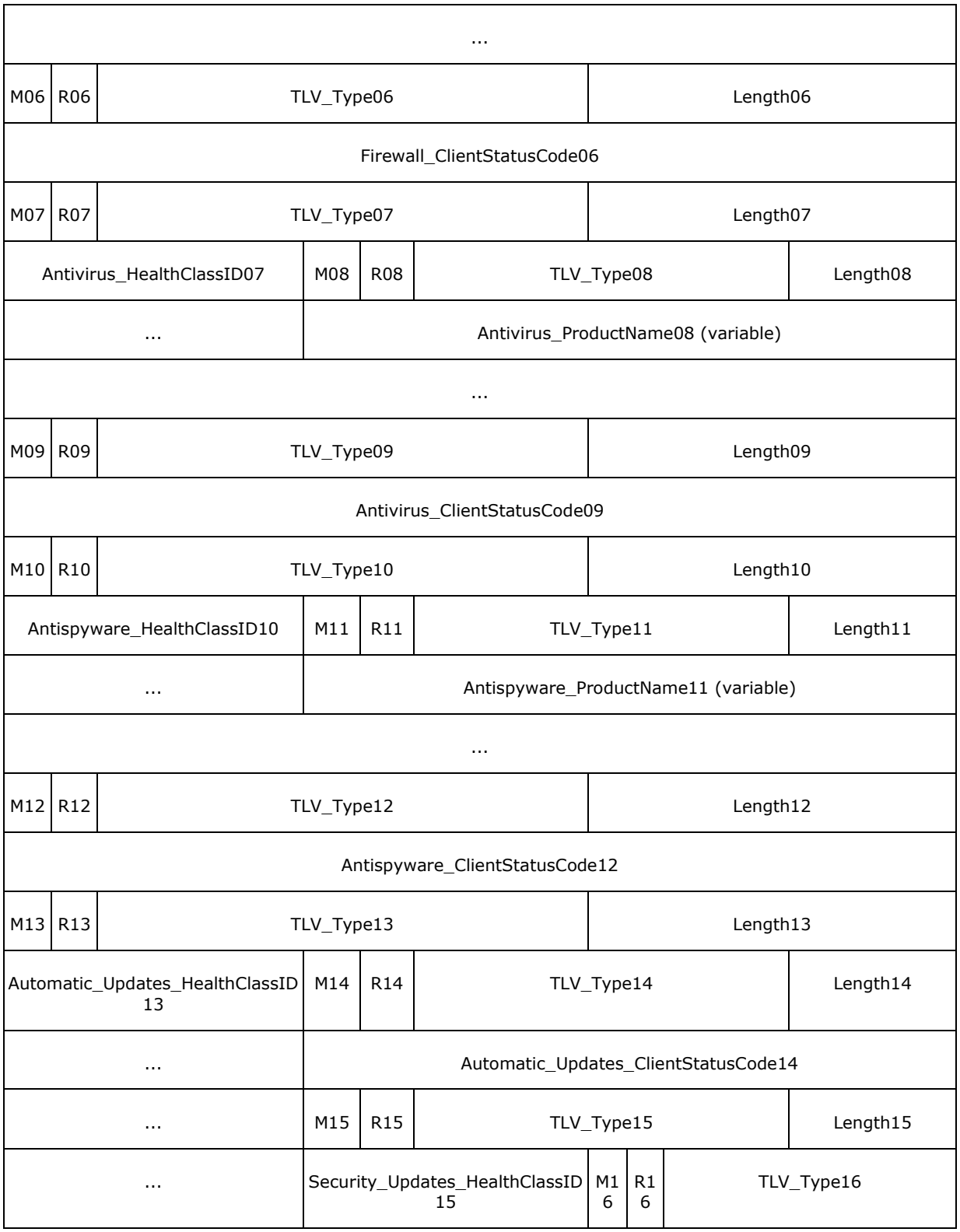
The Windows Security Health Agent (WSHA) and Windows Security Health Validator (WSHV) Protocol is comprised of messages in the form of SoHReportEntries in the Network Access Protection (NAP) Statement of Health (SoH) and Statement of Health Response (SoHR), respectively, as specified in [MS-SOH] sections 2.2.5.2 and 2.2.6.2. The values within both packages are ASN.1-compliant TLVs. For more information on the ASN.1 notation, see [ITUX680].

The respective SoH and SoHR message formats are specified in the following sections.

2.2.1 WSHA SoH

The following are the constituents of the WSHA SoH packet. All of the values MUST be present, unless otherwise noted. The values MUST be in this order.





Length16			Security_Updates_ClientStatusCode16	
...			M17	R17	TLV_Type17
Length17			Security_Updates_DurationSinceLastSynch17 (optional)	
...			M18	R18	TLV_Type18
Length18			Security_Updates_WSUSServerName18 (variable)	
...				
M19	R19	TLV_Type19	Length19	
Security_Updates_UpdatesFlag19				

M01: The **M** bit MUST be set to 0.

R01: The **R** bit is reserved, and MUST be set to 0 and ignored on receipt.

TLV_Type01: A 14-bit unsigned integer that MUST be set to 2.

Length01: A 16-bit unsigned integer in network-byte order that MUST indicate the length (4) in bytes of the **NAPSystemHealthID** field.

NAPSystemHealthID01: A 32-bit unsigned integer, as specified in section 2.2.3.

M02: The **M** bit MUST be set to 0.

R02: The **R** bit is reserved, and MUST be set to 0 and ignored on receipt.

TLV_Type02: A 14-bit unsigned integer that MUST be set to 7.

Length02: A 16-bit unsigned integer in network-byte order that MUST indicate the length (4) in bytes of the **Flag** field.

Flag02: A DWORD, as specified in section 2.2.4.

M03: The **M** bit MUST be set to 0.

R03: The **R** bit is reserved, and MUST be set to 0 and ignored on receipt.

TLV_Type03: A 14-bit unsigned integer that MUST be set to 7.

Length03: A 16-bit unsigned integer in network-byte order that MUST indicate the length (4) in bytes of the **Version** field.

Version03: A DWORD, as specified in section 2.2.5.

M04: The **M** bit MUST be set to 0.

R04: The **R** bit is reserved, and MUST be set to 0 and ignored on receipt.

TLV_Type04: A 14-bit unsigned integer that MUST be set to 8.

Length04: A 16-bit unsigned integer in network-byte order that MUST indicate the length (1) in bytes of the **Firewall_HealthClassID** field.

Firewall_HealthClassID04: A 8-bit unsigned integer, as specified in section 2.2.6.

M05: The **M** bit MUST be set to 0.

R05: The **R** bit is reserved, and MUST be set to 0 and ignored on receipt.

TLV_Type05: A 14-bit unsigned integer that MUST be set to 10.

Length05: A 16-bit unsigned integer in network-byte order that MUST indicate the length in bytes of the **Firewall_ProductName** field.

Firewall_ProductName05: A string, as specified in section 2.2.7.

M06: The **M** bit MUST be set to 0.

R06: The **R** bit is reserved, and MUST be set to 0 and ignored on receipt.

TLV_Type06: A 14-bit unsigned integer that MUST be set to 11.

Length06: A 16-bit unsigned integer in network-byte order that MUST indicate the length (4) in bytes of the **Firewall_ClientStatusCode** field.

Firewall_ClientStatusCode06: A DWORD, as specified section 2.2.8.

M07: The **M** bit MUST be set to 0.

R07: The **R** bit is reserved, and MUST be set to 0 and ignored on receipt.

TLV_Type07: A 14-bit unsigned integer that MUST be set to 8.

Length07: A 16-bit unsigned integer in network-byte order that MUST indicate the length (1) in bytes of the **Antivirus_HealthClassID** field.

Antivirus_HealthClassID07: An 8-bit unsigned integer, as specified in section 2.2.6.

M08: The **M** bit MUST be set to 0.

R08: The **R** bit is reserved, and MUST be set to 0 and ignored on receipt.

TLV_Type08: A 14-bit unsigned integer that MUST be set to 10.

Length08: A 16-bit unsigned integer in network-byte order that MUST indicate the length of the string in bytes of the **Antivirus_ProductName** field.

Antivirus_ProductName08: A string, as specified in section 2.2.7.

M09: The **M** bit MUST be set to 0.

R09: The **R** bit is reserved, and MUST be set to 0 and ignored on receipt.

TLV_Type09: A 14-bit unsigned integer that MUST be set to 11.

Length09: A 16-bit unsigned integer in network-byte order that MUST indicate the length (4) in bytes of the **Antivirus_ClientStatusCode** field.

Antivirus_ClientStatusCode09: A DWORD, as specified in section 2.2.8.

M10: The **M** bit MUST be set to 0.

R10: The **R** bit is reserved, and MUST be set to 0 and ignored on receipt.

TLV_Type10: A 14-bit unsigned integer that MUST be set to 8.

Length10: A 16-bit unsigned integer in network-byte order that MUST indicate the length (1) in bytes of the **Antispyware_HealthClassID** field.

Antispyware_HealthClassID10: An 8-bit unsigned integer, as specified in section 2.2.6.

M11: The **M** bit MUST be set to 0.

R11: The **R** bit is reserved, and MUST be set to 0 and ignored on receipt.

TLV_Type11: A 14-bit unsigned integer that MUST be set to 10.

Length11: A 16-bit unsigned integer in network-byte order that MUST indicate the length of the string in bytes of the **Antispyware_ProductName** field.

Antispyware_ProductName11: A string, as specified in section 2.2.7.

M12: The **M** bit MUST be set to 0.

R12: The **R** bit is reserved, and MUST be set to 0 and ignored on receipt.

TLV_Type12: A 14-bit unsigned integer that MUST be set to 11.

Length12: A 16-bit unsigned integer in network-byte order that MUST indicate the length (4) in bytes of the **Antispyware_ClientStatusCode** field.

Antispyware_ClientStatusCode12: A DWORD, as specified in section 2.2.8.

M13: The **M** bit MUST be set to 0.

R13: The **R** bit is reserved, and MUST be set to 0 and ignored on receipt.

TLV_Type13: A 14-bit unsigned integer that MUST be set to 8.

Length13: A 16-bit unsigned integer in network-byte order that MUST indicate the length (1) in bytes of the **Automatic_Updates_HealthClassID** field.

Automatic_Updates_HealthClassID13: An 8-bit unsigned integer, as specified in section 2.2.6.

M14: The **M** bit MUST be set to 0.

R14: The **R** bit is reserved, and MUST be set to 0 and ignored on receipt.

TLV_Type14: A 14-bit unsigned integer that MUST be set to 11.

Length14: A 16-bit unsigned integer in network-byte order that MUST indicate the length (4) in bytes of the **Automatic_Updates_ClientStatusCode** field.

Automatic_Updates_ClientStatusCode14: A DWORD, as specified in section 2.2.8.

M15: The **M** bit MUST be set to 0.

R15: The **R** bit is reserved, and MUST be set to 0 and ignored on receipt.

TLV_Type15: A 14-bit unsigned integer that MUST be set to 8.

Length15: A 16-bit unsigned integer in network-byte order that MUST indicate the length (1) in bytes of the **Security_Updates_HealthClassID** field.

Security_Updates_HealthClassID15: An 8-bit unsigned integer, as specified in section 2.2.6.

M16: The **M** bit MUST be set to 0.

R16: The **R** bit is reserved, and MUST be set to 0 and ignored on receipt.

TLV_Type16: A 14-bit unsigned integer that MUST be set to 11.

Length16: A 16-bit unsigned integer in network-byte order that MUST indicate the length (4) in bytes of the **Security_Updates_ClientStatusCode** field.

Security_Updates_ClientStatusCode16: A DWORD, as specified in section 2.2.8.

M17: The **M** bit MUST be set to 0.

R17: The **R** bit is reserved, and MUST be set to 0 and ignored on receipt.

TLV_Type17: A 14-bit unsigned integer that MUST be set to 7.

Length17: A 16-bit unsigned integer in network-byte order that MUST indicate the length (4) in bytes of the **Security_Updates_DurationSinceLastSynch** field.

Security_Updates_DurationSinceLastSynch17: A DWORD, as specified in section 2.2.9. Not used if Error is returned in the HealthClassStatus (see section 2.2.6).

M18: The **M** bit MUST be set to 0.

R18: The **R** bit is reserved, and MUST be set to 0 and ignored on receipt.

TLV_Type18: A 14-bit unsigned integer that MUST be set to 7.

Length18: A 16-bit unsigned integer in network-byte order that MUST indicate the length of the string in bytes of the **Security_Updates_WSUSServerName** field.

Security_Updates_WSUSServerName18: String, as specified in section 2.2.10. Not used if Error is returned in the HealthClassStatus (see section 2.2.6).

M19: The **M** bit MUST be set to 0.

R19: The **R** bit is reserved, and MUST be set to 0 and ignored on receipt.

TLV_Type19: A 14-bit unsigned integer that MUST be set to 7.

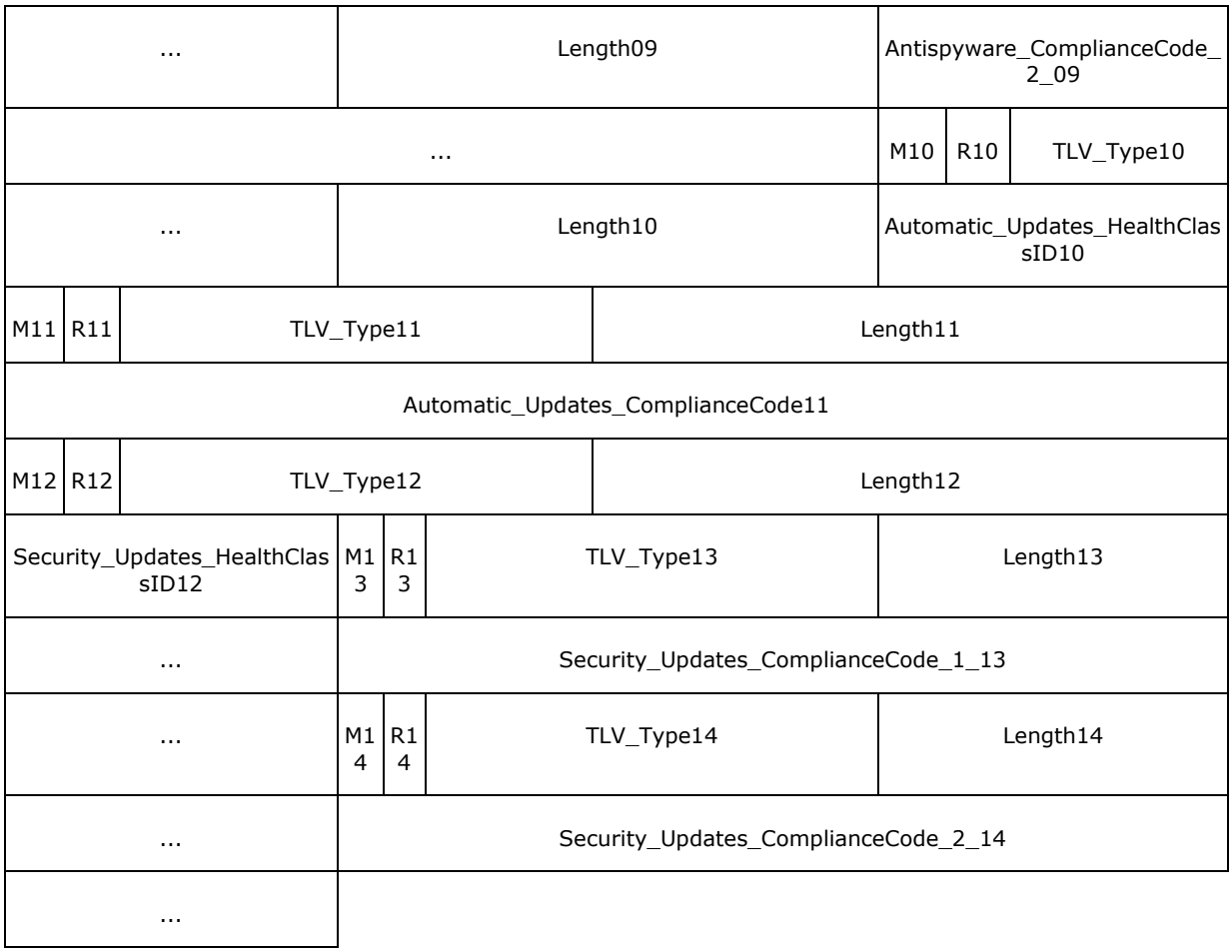
Length19: A 16-bit unsigned integer in network-byte order that MUST indicate the length (4) in bytes of the **Security_Updates_UpdatesFlag** field.

Security_Updates_UpdatesFlag19: A DWORD, as specified in section 2.2.11. Not used if Error is returned in the HealthClassStatus (see section 2.2.6).

2.2.2 WSHV SoHR

The following are the constituents of the WSHV SoHR packet. All of the values MUST be present, unless otherwise noted. The values MUST be in this order.

<table>
<tr><th>0</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>10</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>20</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>30</th><th>1</th></tr>
<tr><td>M01</td><td>R01</td><td colspan="14">TLV_Type01</td><td colspan="16">Length01</td></tr>
<tr><td colspan="32">NAPSystemHealthID01</td></tr>
<tr><td>M02</td><td>R02</td><td colspan="14">TLV_Type02</td><td colspan="16">Length02</td></tr>
<tr><td colspan="16">Firewall_HealthClassID02</td><td>M03</td><td>R03</td><td colspan="12">TLV_Type03</td><td colspan="8">Length03</td></tr>
<tr><td colspan="16">...</td><td colspan="16">Firewall_ComplianceCode03</td></tr>
<tr><td colspan="16">...</td><td>M04</td><td>R04</td><td colspan="12">TLV_Type04</td><td colspan="8">Length04</td></tr>
<tr><td colspan="16">...</td><td colspan="8">Antivirus_HealthClassID04</td><td>M05</td><td>R05</td><td colspan="12">TLV_Type05</td></tr>
<tr><td colspan="16">Length05</td><td colspan="16">Antivirus_ComplianceCode_1_05</td></tr>
<tr><td colspan="16">...</td><td>M06</td><td>R06</td><td colspan="12">TLV_Type06</td></tr>
<tr><td colspan="16">Length06</td><td colspan="16">Antivirus_ComplianceCode_2_06</td></tr>
<tr><td colspan="16">...</td><td>M07</td><td>R07</td><td colspan="12">TLV_Type07</td></tr>
<tr><td colspan="16">Length07</td><td colspan="8">Antispyware_HealthClassID07</td><td>M08</td><td>R08</td><td colspan="6">TLV_Type08</td></tr>
<tr><td colspan="16">...</td><td colspan="16">Length08</td><td colspan="8">Antispyware_ComplianceCode_1_08</td></tr>
<tr><td colspan="24">...</td><td>M09</td><td>R09</td><td colspan="6">TLV_Type09</td></tr>
</table>



M01: The **M** bit MUST be set to 0.

R01: The **R** bit is reserved, and MUST be set to 0 and ignored on receipt.

TLV_Type01: A 14-bit unsigned integer that MUST be set to 2.

Length01: A 16-bit unsigned integer in network-byte order that MUST indicate the length (4) in bytes of the **NAPSystemHealthID** field.

NAPSystemHealthID01: A 32-bit unsigned integer, as specified in section 2.2.3.

M02: The **M** bit MUST be set to 0.

R02: The **R** bit is reserved, and MUST be set to 0 and ignored on receipt.

TLV_Type02: A 14-bit unsigned integer that MUST be set to 8.

Length02: A 16-bit unsigned integer in network-byte order that MUST indicate the length (1) in bytes of the **Firewall_HealthClassID** field.

Firewall_HealthClassID02: An 8-bit unsigned integer, as specified in section 2.2.6.

M03: The **M** bit MUST be set to 0.

R03: The **R** bit is reserved, and MUST be set to 0 and ignored on receipt.

TLV_Type03: A 14-bit unsigned integer that MUST be set to 4.

Length03: A 16-bit unsigned integer in network-byte order that MUST indicate the length (4) in bytes of the **Firewall_ComplianceCode** field.

Firewall_ComplianceCode03: A DWORD, as specified in section 2.2.12.

M04: The **M** bit MUST be set to 0.

R04: The **R** bit is reserved, and MUST be set to 0 and ignored on receipt.

TLV_Type04: A 14-bit unsigned integer that MUST be set to 8.

Length04: A 16-bit unsigned integer in network-byte order that MUST indicate the length (1) in bytes of the **Antivirus_HealthClassID** field.

Antivirus_HealthClassID04: An 8-bit unsigned integer, as specified in section 2.2.6.

M05: The **M** bit MUST be set to 0.

R05: The **R** bit is reserved, and MUST be set to 0 and ignored on receipt.

TLV_Type05: A 14-bit unsigned integer that MUST be set to 4.

Length05: A 16-bit unsigned integer in network-byte order that MUST indicate the length (4) in bytes of the **Antivirus_ComplianceCode_1** field.

Antivirus_ComplianceCode_1_05: A DWORD, as specified in section 2.2.12.

M06: The **M** bit MUST be set to 0.

R06: The **R** bit is reserved, and MUST be set to 0 and ignored on receipt.

TLV_Type06: A 14-bit unsigned integer that MUST be set to 4.

Length06: A 16-bit unsigned integer in network-byte order that MUST indicate the length (4) in bytes of the **Antivirus_ComplianceCode_2** field.

Antivirus_ComplianceCode_2_06: A DWORD, as specified in section 2.2.12.

M07: The **M** bit MUST be set to 0.

R07: The **R** bit is reserved, and MUST be set to 0 and ignored on receipt.

TLV_Type07: A 14-bit unsigned integer that MUST be set to 8.

Length07: A 16-bit unsigned integer in network-byte order that MUST indicate the length (1) in bytes of the **Antispyware_HealthClassID** field.

Antispyware_HealthClassID07: An 8-bit unsigned integer, as specified in section 2.2.6.

M08: The **M** bit MUST be set to 0.

R08: The **R** bit is reserved, and MUST be set to 0 and ignored on receipt.

TLV_Type08: A 14-bit unsigned integer that MUST be set to 4.

Length08: A 16-bit unsigned integer in network-byte order that MUST indicate the length (4) in bytes of the **Antispyware_ComplianceCode_1** field.

Antispyware_ComplianceCode_1_08: A DWORD value, as specified in section 2.2.12.

M09: The **M** bit MUST be set to 0.

R09: The **R** bit is reserved, and MUST be set to 0 and ignored on receipt.

TLV_Type09: A 14-bit unsigned integer that MUST be set to 4.

Length09: A 16-bit unsigned integer in network-byte order that MUST indicate the length (4) in bytes of the **Antispyware_ComplianceCode_2** field.

Antispyware_ComplianceCode_2_09: A DWORD, as specified in section 2.2.12.

M10: The **M** bit MUST be set to 0.

R10: The **R** bit is reserved, and MUST be set to 0 and ignored on receipt.

TLV_Type10: A 14-bit unsigned integer that MUST be set to 8.

Length10: A 16-bit unsigned integer in network-byte order that MUST indicate the length (1) in bytes of the **Automatic_Updates_HealthClassID** field.

Automatic_Updates_HealthClassID10: An 8-bit unsigned integer, as specified in section 2.2.6.

M11: The **M** bit MUST be set to 0.

R11: The **R** bit is reserved, and MUST be set to 0 and ignored on receipt.

TLV_Type11: A 14-bit unsigned integer that MUST be set to 4.

Length11: A 16-bit unsigned integer in network-byte order that MUST indicate the length (4) in bytes of the **Automatic_Updates_ComplianceCode** field.

Automatic_Updates_ComplianceCode11: A DWORD, as specified in section 2.2.12.

M12: The **M** bit MUST be set to 0.

R12: The **R** bit is reserved, and MUST be set to 0 and ignored on receipt.

TLV_Type12: A 14-bit unsigned integer that MUST be set to 8.

Length12: A 16-bit unsigned integer in network-byte order that MUST indicate the length (1) in bytes of the **Security_Updates_HealthClassID** field.

Security_Updates_HealthClassID12: An 8-bit unsigned integer, as specified in section 2.2.6.

M13: The **M** bit MUST be set to 0.

R13: The **R** bit is reserved, and MUST be set to 0 and ignored on receipt.

TLV_Type13: A 14-bit unsigned integer that MUST be set to 4.

Length13: A 16-bit unsigned integer in network-byte order that MUST indicate the length (4) in bytes of the **Security_Updates_ComplianceCode_1** field.

Security_Updates_ComplianceCode_1_13: A DWORD, as specified in section 2.2.12.

M14: The **M** bit MUST be set to 0.

R14: The **R** bit is reserved, and MUST be set to 0 and ignored on receipt.

TLV_Type14: A 14-bit unsigned integer that MUST be set to 4.

Length14: A 16-bit unsigned integer in network-byte order that MUST indicate the length (4) in bytes of the **Security_Updates_ComplianceCode_2** field.

Security_Updates_ComplianceCode_2_14: A DWORD, as specified in section 2.2.13.

2.2.3 NAPSystemHealthID

NAPSystemHealthID is a 32-bit unsigned integer that is assigned by Network Access Protection (NAP). This NAPSystemHealthID is used to differentiate the WSHA SoH packets from those of other security health agents. The default value for the Windows Security Health Agent (WSHA) and the Windows Security Health Validator (WSHV) is 0x00013780 (79744).

2.2.4 Flag

This is a DWORD that is incremented for each new Statement of Health (SoH). It is used to determine if the SoH is a duplicate.

2.2.5 Version

This is a DWORD that differentiates the Windows Security Health Agent (WSHA) client version so that the Windows Security Health Validator (WSHV) knows how to handle client version-specific messages. The Windows client versions are as follows:

Value	Meaning
0x00050001	Windows XP WSHA
0x00060000	Windows Vista WSHA
0x00060001	Windows Vista SP1WSHA

2.2.6 HealthClassID

This is an 8-bit field that specifies to which security health class the data in the following fields pertains.

The Windows Security Health Agent (WSHA) and the Windows Security Health Validator (WSHV) HealthClassIDs are as follows:

Value	Meaning
0x00	Firewall
0x01	Antivirus
0x02<1>	Antispyware
0x03	Automatic Updates

Value	Meaning
0x04	**Security Updates**

2.2.7 ProductName

This is a variable string that contains the product name reported for each health class. This name is passed to the Windows Security Health Agent (WSHA) by Windows Security Center (WSC).

2.2.8 ClientStatusCode

This is a DWORD that reports the specific status for each health class on the client.

The Windows Security Health Agent (WSHA) either provides the specific status for that health class, or it provides an error if the WSHA was unable to determine the status for that health class. If there is no error condition, the WSHA reports the status of the firewall, antivirus, antispyware, and automatic updates using the last four bits of the DWORD. This status is obtained from the Windows Security Center (WSC).

ClientStatusCode status names that begin with "E_" are errors. An error condition is also indicated when the Value begins with 0xC0. An exception to this convention is the ClientStatusCode status E_MSSHAV_WUA_SERVICE_NOT_STARTED_SINCE_BOOT, which starts with 0x00FF but indicates an error.

Security update codes are obtained from the Windows Update Agent (WUA) error codes and security updates status codes, as follows:

Value	ClientStatusCode status	Applicable health classes	Meaning
0x00FF0005	S_MSSHA_NO_MISSING_UPDATES	Security updates	The WUA reports that the client is not missing any updates.
0x00FF0006	S_MSSHA_ MISSING_UPDATES	Security updates	The WUA reports that the client is missing security updates.
0xC0FF000C	E_MSSHAV_NO_WUS_SERVER	Security updates	The WUA reports that the client is configured for WSUS, but no WSUS server has been specified.
0xC0FF000D	E_MSSHAV_NO_CLIENT_ID	Security updates	The WUA reports that the client is

Value	ClientStatusCode status	Applicable health classes	Meaning
			configured for WSUS, but it does not have a valid client ID.
0xC0FF000E	E_MSSHAV_WUA_SERVICE_DISABLED	Security updates	The WUA service on the client has been disabled.
0xC0FF000F	E_MSSHAV_WUA_COMM_FAILURE	Security updates	The WUA service is running, but the WSHA is unable to communicate with it to get security update status.
0xC0FF0010	E_MSSHAV_UPDATES_INSTALLED_REQUIRE_REBOOT	Security updates	The WUA reports that the client requires being restarted to complete the installation of required security updates.
0x00FF0008	E_MSSHAV_WUA_SERVICE_NOT_STARTED_SINCE_BOOT	Security updates	The WUA on the client has not started since the computer started.
0xC0FF0002	E_MSSHAV_PRODUCT_NOT_INSTALLED	Firewall, antivirus, and antispyware	WSC reports that a firewall, antivirus, or antispyware application is not installed.
0xC0FF0003	E_MSSHAV_WSC_SERVICE_DOWN	Firewall, antivirus, antispyware, and automatic	The WSC service is not available to report status.

Value	ClientStatusCode status	Applicable health classes	Meaning
		updates	
0xC0FF0018	E_MSSHAV_WSC_SERVICE_NOT_STARTED_SINCE_BOOT	Firewall, antivirus, antispyware, and automatic updates	The WSC service on the client has not started since the computer started.

The Statement of Health (SoH) can contain information for multiple products in each health class, and so the SoH status can be present multiple times.

The following table represents the possible states for antivirus and antispyware:

Condition	Binary representation (B3,B2,B1,B0)	Hex representation
Microsoft product enabled and up to date, and not snoozed.	0111	0x7
Microsoft product not enabled and not up to date.	0100	0x4
Microsoft product not enabled, but up to date.	0110	0x6
Microsoft product enabled, but not up to date and not snoozed.	0101	0x5
Microsoft product enabled, but not up to date and snoozed.	1101	0xD
Microsoft product enabled and up to date, but snoozed.	1111	0xF
Non-Microsoft product enabled and up to date, and not snoozed.	0011	0x3
Non-Microsoft product not enabled and not up to date.	0000	0x0
Non-Microsoft product not enabled, but up to date.	0010	0x2
Non-Microsoft product enabled, but not up to date and not snoozed.	0001	0x1
Non-Microsoft product enabled, but not up to date and snoozed.	1001	0x9
Non-Microsoft product enabled and up to date, but snoozed.	1011	0xB

The following table represents the possible states for firewall:

Condition	Binary representation (B3,B2,B1,B0)	Hex representation
Microsoft product enabled and not snoozed.	0101	0x5
Microsoft product not enabled.	0100	0x4
Microsoft product enabled and snoozed.	1101	0xD
Non-Microsoft product enabled and not snoozed.	0001	0x1
Non-Microsoft product not enabled.	0000	0x0
Non-Microsoft product enabled and snoozed.	1001	0x9

Automatic updates is handled differently. The following table represents the possible states for automatic updates (AUs):

Condition	Binary representation (B3,B2,B1,B0)	Hex representation
AU not enabled.	0000	0x0
AU enabled, but only check for updates.	0001	0x1
AU enabled, and download updates.	0100	0x4
AU enabled, and download and install updates.	1000	0x8

Because only one compliance code is returned per health class, but multiple products can be reported in each health class, there is a hierarchy of precedence for what condition triggers the compliance code in the WSHV. The following table lists what health class status will take precedence. (This does not apply to AU.)

Precedence:

Value
0x7
0x3
0x4, 0x5, 0x6, 0xD, or 0xF
0x1
0x2 or 0xB
0x0 or 0x9

The ClientStatusCode Packet:

0	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	20	1	2	3	4	5	6	7	8	9	30	1
Ignore																												B3	B2	B1	B0

Ignore: This field MUST be ignored on receipt.

B3: Product snoozed: This bit is set if the product has been temporarily placed into a "snoozed" state. This applies to firewall, antivirus, and antispyware. For automatic updates, this bit is ignored.

B2: Microsoft product: This bit is set if the product being reported in that health class is a Microsoft product. For automatic updates, this bit is ignored.

B1: Product up-to-date: This bit is set if the product reports that it has the current applicable signature definitions. This applies to antivirus and antispyware. For firewall and automatic updates, this bit is ignored.

B0: Product enabled: This bit is set if the product reports that it is enabled. This applies to firewall, antivirus, antispyware, and automatic updates.

2.2.9 DurationSinceLastSynch

This is a DWORD that reports the time since the client last scanned for updates. If the client experienced an error in reporting security update status, this field is not used.

2.2.10 WSUSServerName

This is a string that reports the name of the Windows Server Update Services (WSUS) server with which the client is enlisted. This field is optional, depending on whether or not the client is using WSUS for security updates. If the client experienced an error in reporting security update status, this field is not used.

2.2.11 UpdatesFlag

This is a DWORD that reports specific information on the security update status of the client. For Windows Vista clients, it contains the maximum severity rating of the security updates that it knows about. For Windows XP and Windows Vista SP1 clients, it also contains the security update source that the client is enlisted in. This status is given by setting bits to flag the severity rating and the accepted sources. The values of the flags are listed in the tables below. If the client experienced an error in reporting security update status, this field is not used.

Value	Severity rating
0x00000040	Unspecified
0x00000080	Low
0x00000100	Moderate
0x00000200	Important
0x00000400	Critical

Value	Source enlistments
0x00004000	Windows Update
0x00010000	Windows Server Update Services (WSUS)
0x00020000	Microsoft Update

2.2.12 ComplianceCode1

This is a DWORD that returns to the client whether or not each health class is compliant.

ComplianceCode names that begin with "E_" are errors. An error condition is also indicated when the value begins with 0xC0.

Value	ComplianceCode name	Applicable health classes	Meaning
0x00000000	S_OK	All	The status reported for a particular health class is acceptable.
0xC0FF000C	E_MSSHAV_NO_WUS_SERVER	Security updates	The Windows Update Agent (WUA) reports that the client is configured for Windows Server Update Services (WSUS), but no WSUS server has been specified.
0xC0FF000D	E_MSSHAV_NO_CLIENT_ID	Security updates	The WUA reports that the client is configured for WSUS, but it does not have a valid client ID.
0xC0FF000E	E_MSSHAV_WUA_SERVICE_DISABLED	Security updates	The WUA service on the client has been disabled.

Value	ComplianceCode name	Applicable health classes	Meaning
0xC0FF000F	E_MSSHAV_WUA_COMM_FAILURE	Security updates	The WUA service is running, but the Windows Security Health Agent (WSHA) is unable to communicate with it to get security update status.
0xC0FF0015	E_MSSHV_SHC_FAILURE	All	The Windows Security Health Validator (WSHV) receives an SoH in which it cannot read or interpret one or more of the security health classes, but the SoH is otherwise well formed.
0xC0FF0007	E_MSSHV_SYNC_AND_INSTALL_UPDATES	Security updates	The client has missing required security updates, or it has exceeded the maximum allowable time since it last synched with an update server.
0xC0FF0010	E_MSSHAV_UPDATES_INSTALLED_REQUIRE_REBOOT	Security updates	The WUA reports that the client requires restarting to complete the installation of required

Value	ComplianceCode name	Applicable health classes	Meaning
			security updates.
0xC0FF0012	E_MSSHV_WUS_SHC_FAILURE	Security updates	The WSHV is unable to process the security updates health class received in the SoH.
0x00FF0008	E_MSSHAV_WUA_SERVICE_NOT_STARTED_SINCE_BOOT	Security updates	The WUA on the client has not started since the computer started.
0xC0FF0017	E_MSSHV_INVALID_SOH	All	The WSHV was unable to parse the received SoH.
0xC0FF0001	E_MSSHV_PRODUCT_NOT_ENABLED	Firewall, antivirus, and antispyware	A Microsoft antivirus or antispyware product is installed, but not enabled.
0xC0FF0047	E_MSSHV_THIRD_PARTY_PRODUCT_NOT_ENABLED	Firewall, antivirus, and antispyware	A non-Microsoft antivirus or antispyware product is installed, but not enabled.
0xC0FF0002	E_MSSHAV_PRODUCT_NOT_INSTALLED	Firewall, antivirus, and antispyware	Windows Security Center (WSC) reports that a firewall, antivirus, or antispyware application is not installed.
0xC0FF0003	E_MSSHAV_WSC_SERVICE_DOWN	Firewall, antivirus, antispyware, and automatic updates	The WSC service is not available to report status.

Value	ComplianceCode name	Applicable health classes	Meaning
0xC0FF0018	E_MSSHAV_WSC_SERVICE_NOT_STARTED_SINCE_BOOT	Firewall, antivirus, antispyware, and automatic updates	The WSC service on the client has not started since the computer started.
0xC0FF004E	E_MSSHAV_ BAD_UPDATE_SOURCE_MU	Security updates	The WSHV policy requires clients to get their security updates from Microsoft Update, but the client is getting them from a different source.
0xC0FF004F	E_MSSHAV_BAD_UPDATE_SOURCE_WUMU	Security updates	The WSHV policy requires clients to get their security updates from Microsoft Update or Windows Update, but the client is getting them from a different source.
0xC0FF0050	E_MSSHAV_BAD_UPDATE_SOURCE_MUWSUS	Security updates	The WSHV policy requires clients to get their security updates from Microsoft Update or a Windows Server Updates Services server, but the client is getting them from a different

Value	ComplianceCode name	Applicable health classes	Meaning
			source.
0xC0FF0051	E_MSSHAV_NO_UPDATE_SOURCE	Security updates	The WSHV policy requires clients to have up-to-date security updates, but the client is not configured to get updates from any source.

2.2.13 ComplianceCode2

This is a DWORD that returns additional information for antivirus, antispyware, and security updates. This status code is not used if an error is reported in ComplianceCode1 (section 2.2.12).

2.2.13.1 Antivirus and Antispyware

The following codes are used to echo the antivirus and antispyware signature definition status.

ComplianceCode names that begin with "E_" are errors. An error condition is also indicated when the value begins with 0xC0.

Value	ComplianceCode name	Meaning
0xC0FF0004	E_MSSHV_PRODUCT_NOT_UPTODATE	A Microsoft antivirus or antispyware product is installed and enabled, but not up to date.
0xC0FF0048	E_MSSHV_THIRD_PARTY_PRODUCT_NOT_UPTODATE	A non-Microsoft antivirus or antispyware product is installed and enabled, but not up to date.

2.2.13.2 Security Updates

For the security updates health class, this contains the minimum Microsoft Security Response Center severity rating (as specified in [MSFT-MSRC]) for updates required by the server. This status is given by setting bits to flag the following severity ratings.

Value	Severity rating
0x00000040	Unspecified
0x00000080	Low
0x00000100	Moderate

Value	Severity rating
0x00000200	Important
0x00000400	Critical

3 Protocol Details

The following sections specify details of the Windows Security Health Agent (WSHA) and Windows Security Health Validator (WSHV) Protocol, including abstract data models, state machines, and message processing rules.

3.1 Common Details

This is a simple protocol with a single exchange. The party seeking access to a network resource sends the Statement of Health (SoH) and receives a Statement of Health Response (SoHR). It is represented graphically in the following diagram.

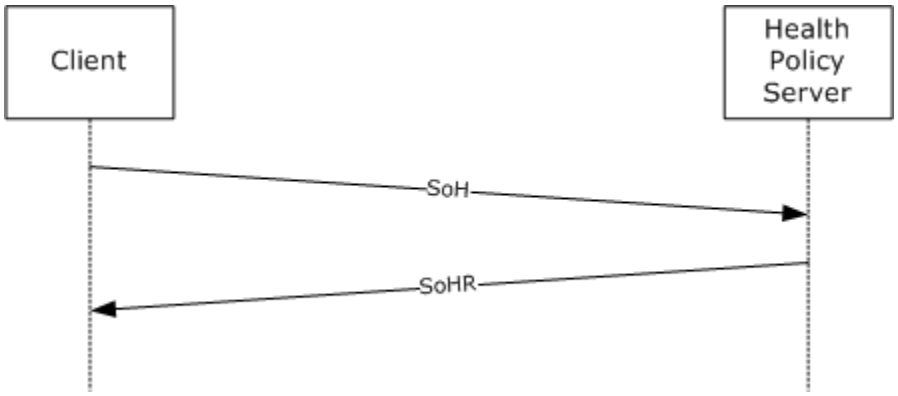


Figure 1: Client SOH request and Health Policy Server response

The Windows Security Health Agent (WSHA) provides status in the form of an SoHReportEntry in the SoH. The Windows Security Health Validator (WSHV) provides a response to that status in the form of an SoHReportEntry in the SoHR.

3.1.1 Abstract Data Model

This section describes a conceptual model of possible data organization that an implementation maintains to participate in this protocol. The described organization is provided to facilitate the explanation of how the protocol behaves. This document does not mandate that implementations adhere to this model as long as their external behavior is consistent with what is described in this document.

The Windows Security Health Agent (WSHA) and Windows Security Health Validator (WSHV) Protocol is comprised of a single exchange. The following should be noted.

- The Windows Security Health Agent (WSHA) reports the client's security health status, and the Windows Security Health Validator (WSHV) compares that status to a policy and returns a quarantine determination.
- The client does not maintain policy information, and the server does not maintain client state information. The following are state diagrams for each of the WSHA and WSHV:

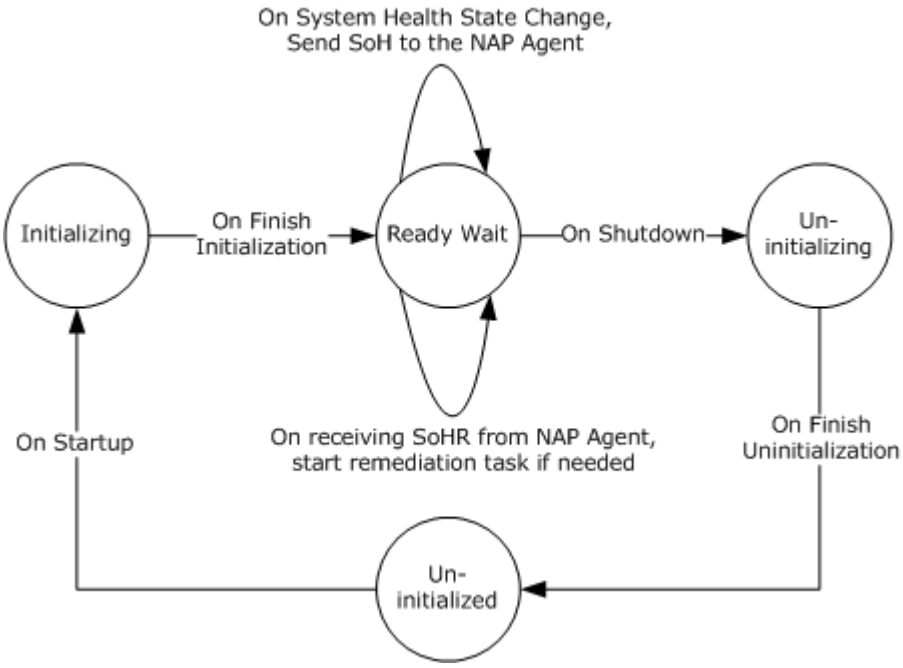


Figure 2: WSHA State Diagram

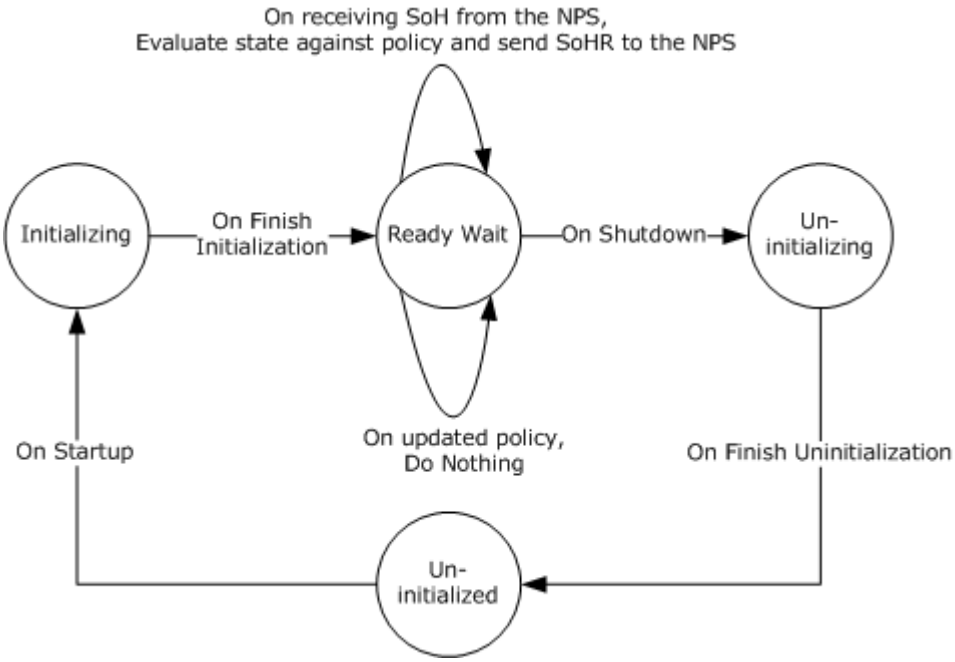


Figure 3: WSHV State Diagram

- If the WSHA is running but the WSHV is not running (or it is not applied to an NPS policy), the WSHA will send its payload in the SoH, but then NPS server will ignore it. This is handled by the [MS-SOH] protocol, and does not involve the [MS-WSH] protocol.

- When the WSHV is running and the NPS receives an SoH from a client that does not have the WSHA running, the NPS returns an error code to the client indicated that it is missing a particular SHA. This is handled by the [MS-SOH] protocol, and does not involve the [MS-WSH] protocol.
- The WSHA and WSHV use a unique identifier, the NAPSystemHealthID, so that the Network Access Protection (NAP) framework knows how to correlate the Statement of Health (SoH) and Statement of Health Response (SoHR) messages between the appropriate WSHA/WSHV pair.
- The WSHA also uses a flag in the SoH to ensure the WSHV knows whether or not that SoH is new or is a duplicate of one previously received.
- The WSHA initializes the value to 0 when the service is started on the client, and then increments that value for each SoH sent.
- If the WSHV receives an SoH with a duplicate flag value, the SoH is discarded.

3.1.2 Timers

The Windows Security Health Agent (WSHA) and Windows Security Health Validator (WSHV) Protocol does not use timers.

3.1.3 Initialization

The Windows Security Health Agent (WSHA) and Windows Security Health Validator (WSHV) Protocol does not require initialization.

3.1.4 Higher-Layer Triggered Events

There are no higher-layer triggered events in the Windows Security Health Agent (WSHA) and Windows Security Health Validator (WSHV) Protocol.

3.1.5 Message Processing Events and Sequencing Rules

3.1.5.1 General Problems

If the Windows Security Health Validator (WSHV) receives a malformed SoH, the WSHV MUST return the error code E_MSSHV_INVALID_SOH in the SoHR.

If the WSHV receives an SoH in which it cannot read or interpret one or more of the security health classes, but the SoH is otherwise well-formed, the WSHV MUST return the error code E_MSSHV_SHC_FAILURE in the SoHR.

If the WSHV is unable to process the security updates health class received in the SoH, the WSHV MUST return the error code E_MSSHV_WUS_SHC_FAILURE in the SoHR.

If the Network Policy Server (NPS) or the WSHV is not running, or if the Windows Security Health Agent (WSHA) never receives an SoHR in response to a SoH that was sent, the client MUST remain in its current state (quarantine or nonquarantine), and MUST NOT send a new SoH unless the client's security health status changes.

3.1.5.2 SoHR Response to SoH Messages

The following messages are sent in the SoH in one or more health classes. The corresponding message is then returned in the SoHR based on the policy defined in the Network Policy Server (NPS).

Status sent in SoH	Policy defined in NPS	ComplianceCode returned in SoHR
E_MSSHAV_WSC_SERVICE_ DOWN	Any.	E_MSSHAV_WSC_SERVICE_ DOWN
E_MSSHAV_WSC_SERVICE_ NOT_STARTED_SINCE_BOOT	Any.	E_MSSHAV_WSC_SERVICE_ NOT_STARTED_SINCE_BOOT
E_MSSHAV_NO_WUS_SERVER	Security updates required.	E_MSSHAV_NO_WUS_ SERVER<2>
E_MSSHAV_NO_CLIENT_ID	Security updates required.	E_MSSHAV_NO_CLIENT_ID
E_MSSHAV_WUA_SERVICE_ NOT_STARTED_SINCE_BOOT	Security updates required.	E_MSSHAV_WUA_SERVICE_ NOT_STARTED_SINCE_BOOT
E_MSSHA_WUA_SERVICE_ DISABLED	Security updates required.	E_MSSHA _WUA_SERVICE_ DISABLED
E_MSSHAV_WUA_COMM_ FAILURE	Security updates required.	E_MSSHAV_WUA_COMM_ FAILURE
E_MSSHAV_PRODUCT_NOT_ INSTALLED	Product required.	E_MSSHAV_PRODUCT_NOT_ INSTALLED
S_MSSHA_NO_MISSING_ UPDATES and DurationSinceLastSynch = X	Security updates required, and X is less than the allowed duration since last sync.	S_OK
S_MSSHA_NO_MISSING_ UPDATES and DurationSinceLastSynch = X	Security updates required, and X is greater than the allowed duration since last sync.	E_MSSHV_SYNC_AND_ INSTALL_UPDATES
S_MSSHA_MISSING_UPDATES	Security updates required.	E_MSSHV_SYNC_AND_ INSTALL_UPDATES
E_MSSHAV_UPDATES_ INSTALLED_REQUIRE_REBOOT	Security updates required.	E_MSSHAV_UPDATES_ INSTALLED_REQUIRE_REBOOT
Client passes its security update source as either Windows Update or Windows Server Update Services in the **UpdatesFlag** field.	Security updates required; must come from Microsoft Update.	E_MSSHAV_BAD_UPDATE_ SOURCE_MU<3>
Client passes its security update source as Windows Server Update Services in the **UpdatesFlag** field.	Security updates required; must come from Microsoft Update or Windows Update.	E_MSSHAV_BAD_UPDATE_ SOURCE_WUMU<4>
Client passes its security update source as Windows Update in the **UpdatesFlag** field.	Security updates required; must come from Microsoft Update or Windows	E_MSSHAV_BAD_UPDATE_ SOURCE_MUWSUS<5>

Status sent in SoH	Policy defined in NPS	ComplianceCode returned in SoHR
	Server Update Services.	
Client passes no security update source in the **UpdatesFlag** field.	Security updates required.	E_MSSHAV_NO_UPDATE_ SOURCE<6>

*This status code is returned in the **ComplianceCode2** field of the SoHR.

For antivirus and antispyware:

Status sent in SoH	Policy defined in NPS	ComplianceCode returned in SoHR
Any	Product not required.	ComplianceCode 1: S_OK
Any	Product not required.	ComplianceCode 2: S_OK
0x7 or 0x3	Product required to be enabled and up to date.	ComplianceCode 1: S_OK
0x7 or 0x3	Product required to be enabled and up to date.	ComplianceCode 2: S_OK
0x7 or 0x3	Product required to be enabled.	ComplianceCode 1: S_OK
0x7 or 0x3	Product required to be enabled.	ComplianceCode 2: S_OK
0x4	Product required to be enabled and up to date.	ComplianceCode 1: E_MSSHV_PRODUCT_NOT_ENABLED
0x4	Product required to be enabled and up to date.	ComplianceCode 2: E_MSSHV_PRODUCT_NOT_UPTODATE
0x4	Product required to be enabled.	ComplianceCode 1: E_MSSHV_PRODUCT_NOT_ENABLED
0x4	Product required to be enabled.	ComplianceCode 2: S_OK
0x5	Product required to be enabled and up to date.	ComplianceCode 1: S_OK
0x5	Product required to be enabled and up to date.	ComplianceCode 2: E_MSSHV_PRODUCT_NOT_UPTODATE
0x5	Product required to be enabled.	ComplianceCode 1: S_OK

Status sent in SoH	Policy defined in NPS	ComplianceCode returned in SoHR
0x5	Product required to be enabled.	ComplianceCode 2: S_OK
0x6	Product required to be enabled and up to date.	ComplianceCode 1: E_MSSHV_PRODUCT_NOT_ENABLED
0x6	Product required to be enabled and up to date.	ComplianceCode 2: S_OK
0x6	Product required to be enabled.	ComplianceCode 1: E_MSSHV_PRODUCT_NOT_ENABLED
0x6	Product required to be enabled.	ComplianceCode 2: S_OK
0xD	Product required to be enabled and up to date.	ComplianceCode 1: E_MSSHV_PRODUCT_NOT_ENABLED
0xD	Product required to be enabled and up to date.	ComplianceCode 2: E_MSSHV_PRODUCT_NOT_UPTODATE
0xD	Product required to be enabled.	ComplianceCode 1: E_MSSHV_PRODUCT_NOT_ENABLED
0xD	Product required to be enabled.	ComplianceCode 2: S_OK
0xF	Product required to be enabled and up to date.	ComplianceCode 1: E_MSSHV_PRODUCT_NOT_ENABLED
0xF	Product required to be enabled and up to date.	ComplianceCode 2: S_OK
0xF	Product required to be enabled.	ComplianceCode 1: E_MSSHV_PRODUCT_NOT_ENABLED
0xF	Product required to be enabled.	ComplianceCode 2: S_OK
0x0	Product required to be enabled and up to date.	ComplianceCode 1: E_MSSHV_THIRD_PARTY_PRODUCT_NOT_ENABLED
0x0	Product required to be enabled and up to date.	ComplianceCode 2: E_MSSHV_THIRD_PARTY_PRODUCT_NOT_UPTODATE
0x0	Product required to be enabled.	ComplianceCode 1: E_MSSHV_THIRD_PARTY_PRODUCT_NOT_ENABLED
0x0	Product required to be enabled.	ComplianceCode 2: S_OK
0x1	Product required to be enabled	ComplianceCode 1:

Status sent in SoH	Policy defined in NPS	ComplianceCode returned in SoHR
	and up to date.	S_OK
0x1	Product required to be enabled and up to date.	ComplianceCode 2: E_MSSHV_THIRD_PARTY_PRODUCT_NOT_UPTODATE
0x1	Product required to be enabled.	ComplianceCode 1: S_OK
0x1	Product required to be enabled.	ComplianceCode 2: S_OK
0x2	Product required to be enabled and up to date.	ComplianceCode 1: E_MSSHV_THIRD_PARTY_PRODUCT_NOT_ENABLED
0x2	Product required to be enabled and up to date.	ComplianceCode 2: S_OK
0x2	Product required to be enabled.	ComplianceCode 1: E_MSSHV_THIRD_PARTY_PRODUCT_NOT_ENABLED
0x2	Product required to be enabled.	ComplianceCode 2: S_OK
0x9	Product required to be enabled and up to date.	ComplianceCode 1: E_MSSHV_THIRD_PARTY_PRODUCT_NOT_ENABLED
0x9	Product required to be enabled and up to date.	ComplianceCode 2: E_MSSHV_THIRD_PARTY_PRODUCT_NOT_UPTODATE
0x9	Product required to be enabled.	ComplianceCode 1: E_MSSHV_THIRD_PARTY_PRODUCT_NOT_ENABLED
0x9	Product required to be enabled.	ComplianceCode 2: S_OK
0xB	Product required to be enabled and up to date.	ComplianceCode 1: E_MSSHV_THIRD_PARTY_PRODUCT_NOT_ENABLED
0xB	Product required to be enabled and up to date.	ComplianceCode 2: S_OK
0xB	Product required to be enabled.	ComplianceCode 1: E_MSSHV_THIRD_PARTY_PRODUCT_NOT_ENABLED
0xB	Product required to be enabled.	ComplianceCode 2: S_OK

For firewall:

Status sent in SoH	Policy defined in NPS	Status returned in SoHR
Any	Firewall not required.	S_OK

Status sent in SoH	Policy defined in NPS	Status returned in SoHR
0x5 or 0x1	Firewall required.	S_OK
0x4	Firewall required.	E_MSSHV_PRODUCT_NOT_ENABLED
0x0	Firewall required.	E_MSSHV_THIRD_PARTY_PRODUCT_NOT_ENABLED
0xD	Firewall required.	E_MSSHV_PRODUCT_NOT_ENABLED
0x9	Firewall required.	E_MSSHV_THIRD_PARTY_PRODUCT_NOT_ENABLED

For automatic updates (AU):

Status sent in SoH	Policy defined in NPS	Status returned in SoHR
Any	AU not required.	S_OK
0x1, 0x4, or 0x8	AU required.	S_OK
0x0	AU required.	E_MSSHV_PRODUCT_NOT_ENABLED

3.1.6 Timer Events

There are no timer events in the Windows Security Health Agent (WSHA) and Windows Security Health Validator (WSHV) Protocol.

3.1.7 Other Local Events

There are no other local events in the Windows Security Health Agent (WSHA) and Windows Security Health Validator (WSHV) Protocol.

4 Protocol Example

The Windows Security Health Agent (WSHA) and Windows Security Health Validator (WSHV) Protocol is a simple protocol with a single exchange. The party seeking access to a network resource sends the Statement of Health (SoH), and then receives a Statement of Health Response (SoHR). For a given compliance code for a given security health class, there is a set of responses that the server can return based on the defined policy.

For example:

1. A policy requires the client to have antivirus software enabled with up-to-date virus definitions.
2. The client reports in the Statement of Health (SoH) that the antivirus application is enabled, but the definitions are out-of-date.
3. The WSHV makes the determination that the client is out of compliance, and then returns the appropriate error code in the Statement of Health Response (SoHR).
4. The client receives the Statement of Health Response (SoHR), and then places itself in quarantine.
5. After the virus definitions are updated, a new Statement of Health (SoH) is sent showing that the client is in compliance with policy.
6. The WSHV returns an S_OK in the Statement of Health Response (SoHR), and then the client is taken out of quarantine.

5 Security

The following sections specify security considerations for implementers of the Windows Security Health Agent (WSHA) and Windows Security Health Validator (WSHV) Protocol.

5.1 Security Considerations for Implementers

There are no other security considerations in the Windows Security Health Agent (WSHA) and Windows Security Health Validator (WSHV) Protocol.

5.2 Index of Security Parameters

There are no security parameters in the Windows Security Health Agent (WSHA) and Windows Security Health Validator (WSHV) Protocol.

6 Appendix A: Windows Behavior

The information in this specification is applicable to the following versions of Windows:

- Windows XP with the Network Access Protection (NAP) client installed
- Windows Vista
- Windows Vista SP1

Exceptions, if any, are noted below. Unless otherwise specified, any statement of optional behavior in this specification prescribed using the terms SHOULD or SHOULD NOT implies Windows behavior in accordance with the SHOULD or SHOULD NOT prescription. Unless otherwise specified, the term MAY implies that Windows does not follow the prescription.

<1> Section 2.2.6: This class is implemented in Windows Vista only.

<2> Section 3.1.5.2: Implemented in Windows Vista. This status code is used only with Windows Vista RTM clients.

<3> Section 3.1.5.2: Implemented in Windows Vista SP1 and Windows XP. This status code is used only with Windows Vista SP1 and Windows XP clients.

<4> Section 3.1.5.2: Implemented in Windows Vista SP1 and Windows XP. This status code is used only with Windows Vista SP1 and Windows XP clients.

<5> Section 3.1.5.2: Implemented in Windows Vista SP1 and Windows XP. This status code is used only with Windows Vista SP1 and Windows XP clients.

<6> Section 3.1.5.2: Implemented in Windows Vista SP1 and Windows XP. This status code is used only with Windows Vista SP1 and Windows XP clients.

7 Index

A

Abstract data model
  WSHA
  WSHV
Antispyware
Antivirus
Applicability

C

Capability negotiation
ClientStatusCode packet
ComplianceCode1
ComplianceCode2

D

Data model - abstract
  WSHA
  WSHV
DurationSinceLastSynch

E

Examples

F

Fields - vendor-extensible
Flag

G

Glossary

H

HealthClassID
Higher-layer triggered events
  WSHA
  WSHV

I

Implementer - security considerations
Index of security parameters
Informative references
Initialization
  WSHA
  WSHV
Introduction

L

Local events
  WSHA
  WSHV

M

Message processing
  WSHA
  WSHV
Messages
  overview
  syntax
  transport

N

NAPSystemHealthID
Normative references

O

Overview (section 1.3, section 3)

P

Parameters - security index
Preconditions
Prerequisites
Problem solving
ProductName

R

References
  informative
  normative
  overview
Relationship to other protocols

S

Security
  implementer considerations
  overview (section 5, section 5.1)
  parameter index
  updates
Sequencing rules
  WSHA
  WSHV
SoHR response to SoH messages
Standards assignments
Syntax

T

Timer events
  WSHA
  WSHV
Timers
  WSHA
  WSHV

Transport
Triggered events - higher-layer
  WSHA
  WSHV

U

UpdatesFlag

V

Vendor-extensible fields
Version
Versioning

W

Windows behavior
WSHA
  abstract data model
  higher-layer triggered events
  initialization
  local events
  message processing
  overview
  sequencing rules
  timer events
  timers
WSHA SoH packet
WSHV
  abstract data model
  higher-layer triggered events
  initialization
  local events
  message processing
  overview
  sequencing rules
  timer events
  timers
WSHV SoHR packet
WSUSServerName