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

---

Revision Summary

Date	Revision History	Revision Class	Comments
04/03/2007	0.1		MCPP Milestone Longhorn Initial Availability
06/01/2007	2.0	Major	Updated and revised the technical content.
07/03/2007	3.0	Major	MLonghorn+90
07/20/2007	4.0	Major	Made fixes to packets.
08/10/2007	4.0.1	Editorial	Revised and edited the technical content.
09/28/2007	4.0.2	Editorial	Revised and edited the technical content.
10/23/2007	4.0.3	Editorial	Revised and edited the technical content.
11/30/2007	4.0.4	Editorial	Revised and edited the technical content.
01/25/2008	5.0	Major	Updated and revised the technical content.
03/14/2008	5.0.1	Editorial	Revised and edited the technical content.
05/16/2008	5.0.2	Editorial	Revised and edited the technical content.
06/20/2008	6.0	Major	Updated and revised the technical content.
07/25/2008	6.1	Minor	Updated the technical content.
08/29/2008	6.2	Minor	Updated the technical content.
10/24/2008	6.2.1	Editorial	Revised and edited the technical content.
12/05/2008	7.0	Major	Updated and revised the technical content.
01/16/2009	8.0	Major	Updated and revised the technical content.
02/27/2009	8.0.1	Editorial	Revised and edited the technical content.
04/10/2009	8.0.2	Editorial	Revised and edited the technical content.
05/22/2009	9.0	Major	Updated and revised the technical content.
07/02/2009	10.0	Major	Updated and revised the technical content.
08/14/2009	11.0	Major	Updated and revised the technical content.
09/25/2009	11.1	Minor	Updated the technical content.
11/06/2009	12.0	Major	Updated and revised the technical content.
12/18/2009	13.0	Major	Updated and revised the technical content.
01/29/2010	13.0.1	Editorial	Revised and edited the technical content.

Date	Revision History	Revision Class	Comments
03/12/2010	14.0	Major	Updated and revised the technical content.
04/23/2010	15.0	Major	Updated and revised the technical content.
06/04/2010	15.0.1	Editorial	Revised and edited the technical content.
07/16/2010	16.0	Major	Significantly changed the technical content.
08/27/2010	17.0	Major	Significantly changed the technical content.
10/08/2010	18.0	Major	Significantly changed the technical content.
11/19/2010	19.0	Major	Significantly changed the technical content.
01/07/2011	20.0	Major	Significantly changed the technical content.
02/11/2011	20.0	No change	No changes to the meaning, language, or formatting of the technical content.

Contents

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 (section 2).
- Protocol details including abstract data models, state machines, and message processing rules (section 3).
- A protocol example (section 4).
- Security considerations for implementers (section 5).
- An appendix of Microsoft Windows® behavior (section 6).
- An index (section 8).

1.1 Glossary

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

Network Access Protection (NAP)
Network Access Protection (NAP) client
network policy server (NPS)
statement of health (SoH)
statement of health response (SoHR)

The following terms are specific to this document:

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.

Windows Security Center (WSC): WSC is the service on Windows XP SP3 and Windows Vista clients that determines the firewall, antivirus, antispyware, and Automatic Updates states that are then reported by the WSHA.

Windows Update Agent (WUA): Provides critical operating system updates to the user, including driver updates, security fixes, and application updates.

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-DTYP] Microsoft Corporation, "Windows Data Types", January 2007.

[MS-SOH] Microsoft Corporation, "Statement of Health for Network Access Protection (NAP) Protocol Specification", January 2007.

[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

[MS-DHCPE] Microsoft Corporation, "Dynamic Host Configuration Protocol (DHCP) Extensions", March 2007.

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

[MS-HCEP] Microsoft Corporation, "Health Certificate Enrollment Protocol Specification", January 2007.

[MS-PEAP] Microsoft Corporation, "Protected Extensible Authentication Protocol (PEAP) Specification", January 2007.

[MS-RNAP] Microsoft Corporation, "Vendor-Specific RADIUS Attributes for Network Access Protection (NAP) Data Structure", January 2007.

[MS-TSGU] Microsoft Corporation, "Terminal Services Gateway Server Protocol Specification", June 2007.

[MS-WUSP] Microsoft Corporation, "Windows Update Services: Client-Server Protocol Specification", September 2007.

[MSDN-INapSysHA] Microsoft Corporation, "INapSystemHealthAgentCallback Interface", http://msdn.microsoft.com/en-us/library/aa369655(v=VS.85).aspx

[MSDN-INapSysHV] Microsoft Corporation, "INapSystemHealthValidator Interface", http://msdn.microsoft.com/en-us/library/aa369692(VS.85).aspx

[MSDN-NAP] Microsoft Corporation, "Network Access Protection", http://msdn.microsoft.com/en-us/library/aa369712(VS.85).aspx

[MSDN-NAPAPI] Microsoft Corporation, "NAP Interfaces", http://msdn.microsoft.com/en-us/library/aa369705(v=VS.85).aspx

[MSDN-NapDatatypes] Microsoft Corporation, "NAP Datatypes", http://msdn.microsoft.com/en-us/library/cc441807(v=VS.85).aspx

[MSDN-WUAAPI] Microsoft Corporation, "Windows Update Agent API", http://msdn.microsoft.com/en-us/library/aa387099(VS.85).aspx

[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.

1.3 Overview

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 an **SoH** message, and then to return remediation instructions to the client in a **Statement of Health Response (SoHR)** message.

For detailed information about the **Network Access Protection (NAP)** system components and developers API, see [MSDN-NAP].

1.3.1 Network Access Protection (NAP) Application Programming Interface (API)

The Network Access Protection (NAP) API provides a set of function calls that allow SHAs from third-party vendors to register with the NAP agent to indicate system health status and to respond to queries for system health status from the NAP agent. The function calls also enable the NAP agent to pass system health remediation information. The NAP API allows SHVs from third-party vendors to register with the network policy server (NPS) to receive system health status for validation and to respond with health evaluation results and remediation information.

For information about the NAP API, see [MSDN-NAPAPI].

1.4 Relationship to Other Protocols

The WSHA and WSHV data is encapsulated in the SoH and SoHR messages, where the WSHA data is packaged as an **SoHReportEntry** set within SoH messages and the WSHV data is packaged as an **SoHRReportEntry** set within SoHRmessages. The exact processing rules for encapsulating WSHA and WSHV data in SoH and SoHR messages are described in [MS-SOH] sections 3.2 and 3.3.

The SoH or the SoHR messages can be carried in one of the following protocols:

- Health Certificate Enrollment Protocol (HCEP), as described in [MS-HCEP].
- Remote Authentication Dial-In User Service (RADIUS), as described in [MS-RNAP] sections 2.2.1.8 and 2.2.1.19.
- Protected Extensible Authentication Protocol (PEAP), as described in [MS-PEAP] section 2.2.4.
- Dynamic Host Configuration Protocol (DHCP), as described in [MS-DHCPE] section 2.2.2.
- Terminal Services Gateway Server Protocol, as described in [MS-TSGU] section 2.2.2.19.

This protocol relationship is demonstrated in the following diagram.

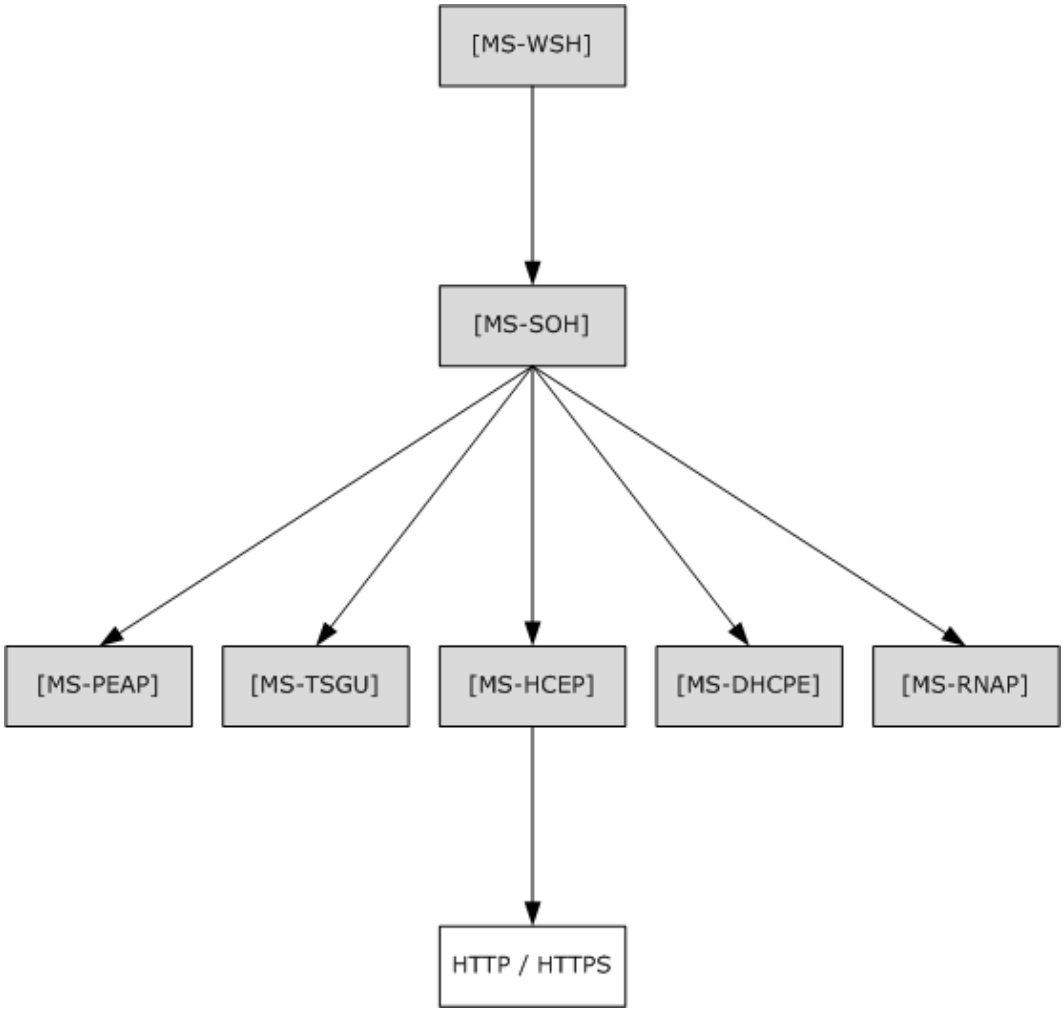


Figure 1: Relationship to other protocols

1.4.1 Relationship with the Windows Update Client-Server Protocol [MS-WUSP]

During operation, the Windows Security Health Agent (WSHA) sends a summary of Windows Update-related information in an SoH message. The WSHA on a client retrieves the summary information by calling the Windows Update Agent API [MSDN-WUAAPI].

The Windows Update Agent communicates with a Windows Update Server using the Windows Update Client-Server Protocol [MS-WUSP]. To operate successfully, the Windows Security Health Agent (WSHA) and Windows Security Health Validator (WSHV) Protocol do not require the Windows Update Client-Server Protocol to be present and functioning.

The codes sent in the SoH message reflect the current state of the Windows Update Agent and are described in section 2.2.8.

The Windows Update Client-Server Protocol [MS-WUSP] is not mentioned in this section regarding the relationships to the WSHA and WSHV Protocol because this protocol operates with or without the Windows Update Client-Server Protocol and simply reports status in an agnostic manner.

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 NAP is being used, and the NAP service is enabled on the client computer.

1.7 Versioning and Capability Negotiation

The WSHA reports its version in the SoH, as specified in section 2.2.5. The WSHV parses the status and enforces the policy differently, depending on the WSHA version.

Based on the implementation configuration, the Network Access Protection (NAP) client must be installed.<1>

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.

This protocol references commonly used data types as defined in [MS-DTYP].

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

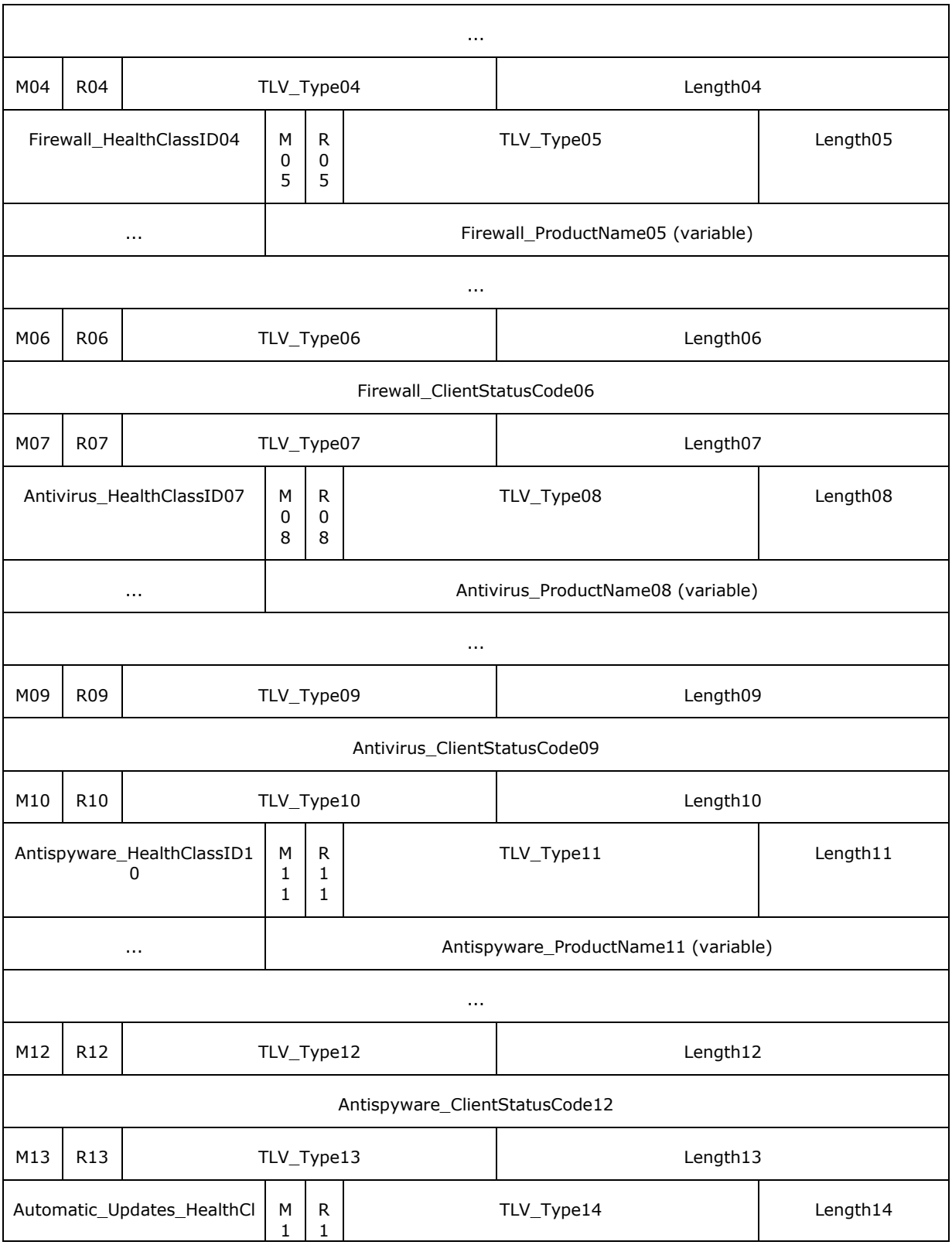
The Windows Security Health Agent (WSHA) and Windows Security Health Validator (WSHV) Protocol is comprised of messages in the form of SoHReportEntries in the NAP SoH and SoHR, respectively, as specified in [MS-SOH] sections 2.2.5.3 and 2.2.6.3. The values within both packages are ASN.1-compliant TLVs. For more information on the ASN.1 notation, see [ITUX680].

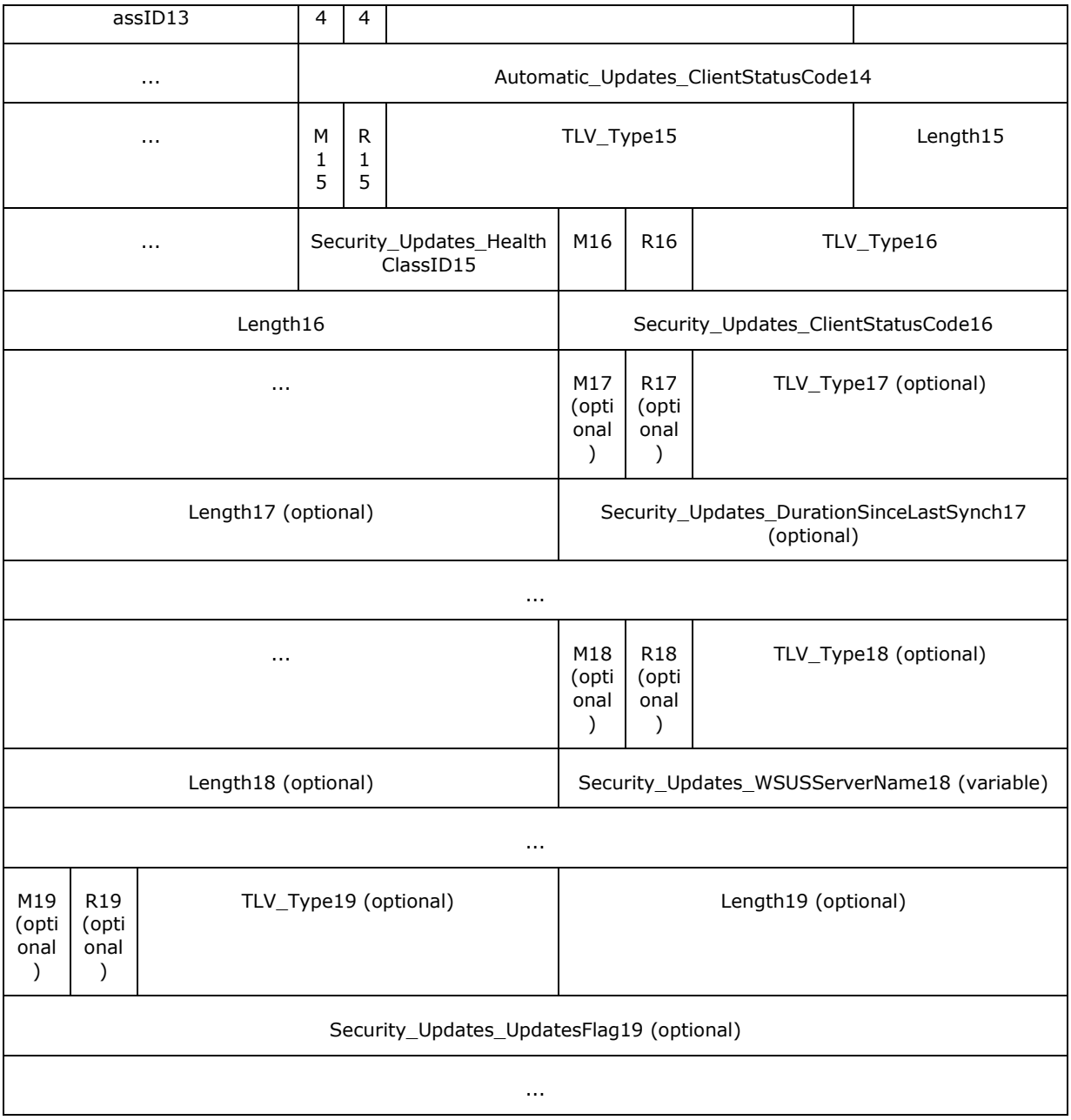
The respective SoH and SoHR message formats are specified in the following sections.

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. TLVs 5, 6, 8, 9, 11, and 12 MUST have at least one instance. They MAY have multiple instances depending on how many firewall, antivirus, and antispyware products are installed. The M and R bits are defined in the Statement of Health for Network Access Protection (NAP) Protocol [MS-SOH] and are ignored by the WSHV upon receipt. All TLV values are sent in network byte order, which is big-endian, except for the Flag02, Version03, Security_Updates_DurationSinceLastSynch17, and Security_Updates_UpdatesFlag19 fields, which are sent in machine byte order and are little-endian.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
M01	R01	TLV_Type01														Length01															
NAPSystemHealthID01																															
M02	R02	TLV_Type02														Length02															
Flag02																															
...																															
M03	R03	TLV_Type03														Length03															
Version03																															





M01 (1 bit): The **M** bit MUST be set to zero.

R01 (1 bit): The **R** bit is reserved, and MUST be set to zero when sent and ignored on receipt.

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

Length01 (2 bytes): A 16-bit unsigned integer in network-byte order that MUST indicate the length (4) in bytes of the **NAPSystemHealthID** field.

NAPSystemHealthID01 (4 bytes): A 32-bit unsigned integer, as specified in section 2.2.3.

M02 (1 bit): The **M** bit MUST be set to zero.

R02 (1 bit): The **R** bit is reserved, and MUST be set to zero when sent and ignored on receipt.

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

Length02 (2 bytes): A 16-bit unsigned integer in network-byte order that MUST indicate the length (8) in bytes of the **Flag** field.

Flag02 (8 bytes): Eight bytes, as specified in section 2.2.4.

M03 (1 bit): The **M** bit MUST be set to zero.

R03 (1 bit): The **R** bit is reserved, and MUST be set to zero when sent and ignored on receipt.

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

Length03 (2 bytes): A 16-bit unsigned integer in network-byte order that MUST indicate the length (8) in bytes of the **Version** field.

Version03 (8 bytes): Eight bytes, as specified in section 2.2.5.

M04 (1 bit): The **M** bit MUST be set to zero.

R04 (1 bit): The **R** bit is reserved, and MUST be set to zero when sent and ignored on receipt.

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

Length04 (2 bytes): A 16-bit unsigned integer in network-byte order that MUST indicate the length (1) in bytes of the **Firewall_HealthClassID** field.

Firewall_HealthClassID04 (1 byte): An 8-bit unsigned integer, as specified in section 2.2.6.

M05 (1 bit): The **M** bit MUST be set to zero.

R05 (1 bit): The **R** bit is reserved, and MUST be set to zero when sent and ignored on receipt.

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

Length05 (2 bytes): A 16-bit unsigned integer in network-byte order that MUST indicate the length in bytes of the **Firewall_ProductName** field.

Firewall_ProductName05 (variable): A string, as specified in section 2.2.7.

M06 (1 bit): The **M** bit MUST be set to zero.

R06 (1 bit): The **R** bit is reserved, and MUST be set to zero when sent and ignored on receipt.

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

Length06 (2 bytes): A 16-bit unsigned integer in network-byte order that MUST indicate the length (4) in bytes of the **Firewall_ClientStatusCode** field.

Firewall_ClientStatusCode06 (4 bytes): A DWORD, as specified in section 2.2.8.

M07 (1 bit): The **M** bit MUST be set to zero.

R07 (1 bit): The **R** bit is reserved, and MUST be set to zero when sent and ignored on receipt.

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

Length07 (2 bytes): A 16-bit unsigned integer in network-byte order that MUST indicate the length (1) in bytes of the **Antivirus_HealthClassID** field.

Antivirus_HealthClassID07 (1 byte): An 8-bit unsigned integer, as specified in section 2.2.6.

M08 (1 bit): The **M** bit MUST be set to zero.

R08 (1 bit): The **R** bit is reserved, and MUST be set to zero when sent and ignored on receipt.

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

Length08 (2 bytes): 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 (variable): A string, as specified in section 2.2.7.

M09 (1 bit): The **M** bit MUST be set to zero.

R09 (1 bit): The **R** bit is reserved, and MUST be set to zero when sent and ignored on receipt.

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

Length09 (2 bytes): A 16-bit unsigned integer in network-byte order that MUST indicate the length (4) in bytes of the **Antivirus_ClientStatusCode** field.

Antivirus_ClientStatusCode09 (4 bytes): A DWORD, as specified in section 2.2.8.

M10 (1 bit): The **M** bit MUST be set to zero.

R10 (1 bit): The **R** bit is reserved, and MUST be set to zero when sent and ignored on receipt.

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

Length10 (2 bytes): A 16-bit unsigned integer in network-byte order that MUST indicate the length (1) in bytes of the **Antispyware_HealthClassID** field.

Antispyware_HealthClassID10 (1 byte): An 8-bit unsigned integer, as specified in section 2.2.6.

M11 (1 bit): The **M** bit MUST be set to zero.

R11 (1 bit): The **R** bit is reserved, and MUST be set to zero when sent and ignored on receipt.

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

Length11 (2 bytes): 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 (variable): A string, as specified in section 2.2.7.

M12 (1 bit): The **M** bit MUST be set to zero.

R12 (1 bit): The **R** bit is reserved, and MUST be set to zero when sent and ignored on receipt.

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

Length12 (2 bytes): A 16-bit unsigned integer in network-byte order that MUST indicate the length (4) in bytes of the **Antispyware_ClientStatusCode** field.

Antispyware_ClientStatusCode12 (4 bytes): A DWORD, as specified in section 2.2.8.

M13 (1 bit): The **M** bit MUST be set to zero.

R13 (1 bit): The **R** bit is reserved, and MUST be set to zero when sent and ignored on receipt.

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

Length13 (2 bytes): 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 (1 byte): An 8-bit unsigned integer, as specified in section 2.2.6.

M14 (1 bit): The **M** bit MUST be set to zero.

R14 (1 bit): The **R** bit is reserved, and MUST be set to zero when sent and ignored on receipt.

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

Length14 (2 bytes): 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 (4 bytes): A DWORD, as specified in section 2.2.8.

M15 (1 bit): The **M** bit MUST be set to zero.

R15 (1 bit): The **R** bit is reserved, and MUST be set to zero when sent and ignored on receipt.

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

Length15 (2 bytes): 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 (1 byte): An 8-bit unsigned integer, as specified in section 2.2.6.

M16 (1 bit): The **M** bit MUST be set to zero.

R16 (1 bit): The **R** bit is reserved, and MUST be set to zero when sent and ignored on receipt.

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

Length16 (2 bytes): 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 (4 bytes): A DWORD, as specified in section 2.2.8.

M17 (1 bit): The **M** bit MUST be set to zero.

R17 (1 bit): The **R** bit is reserved, and MUST be set to zero when sent and ignored on receipt.

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

Length17 (2 bytes): A 16-bit unsigned integer in network-byte order that MUST indicate the length (8) in bytes of the **Security_Updates_DurationSinceLastSynch** field.

Security_Updates_DurationSinceLastSynch17 (8 bytes): Eight bytes, as specified in section 2.2.9. Not used if Error is returned in the Security_Updates_ClientStatusCode (see section 2.2.8).

M18 (1 bit): The **M** bit MUST be set to zero.

R18 (1 bit): The **R** bit is reserved, and MUST be set to zero when sent and ignored on receipt.

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

Length18 (2 bytes): 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 (variable): Four bytes followed by a variable-length string, as specified in section 2.2.10. Not used if Error is returned in the Security_Updates_ClientStatusCode (see section 2.2.8).

M19 (1 bit): The **M** bit MUST be set to zero.

R19 (1 bit): The **R** bit is reserved, and MUST be set to zero when sent and ignored on receipt.

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

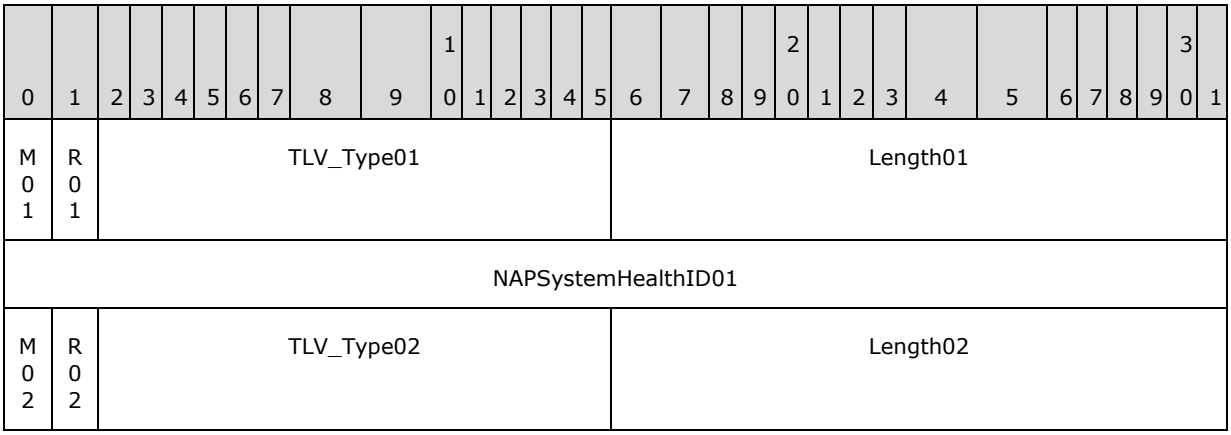
Length19 (2 bytes): A 16-bit unsigned integer in network-byte order that MUST indicate the length (8) in bytes of the **Security_Updates_UpdatesFlag** field.

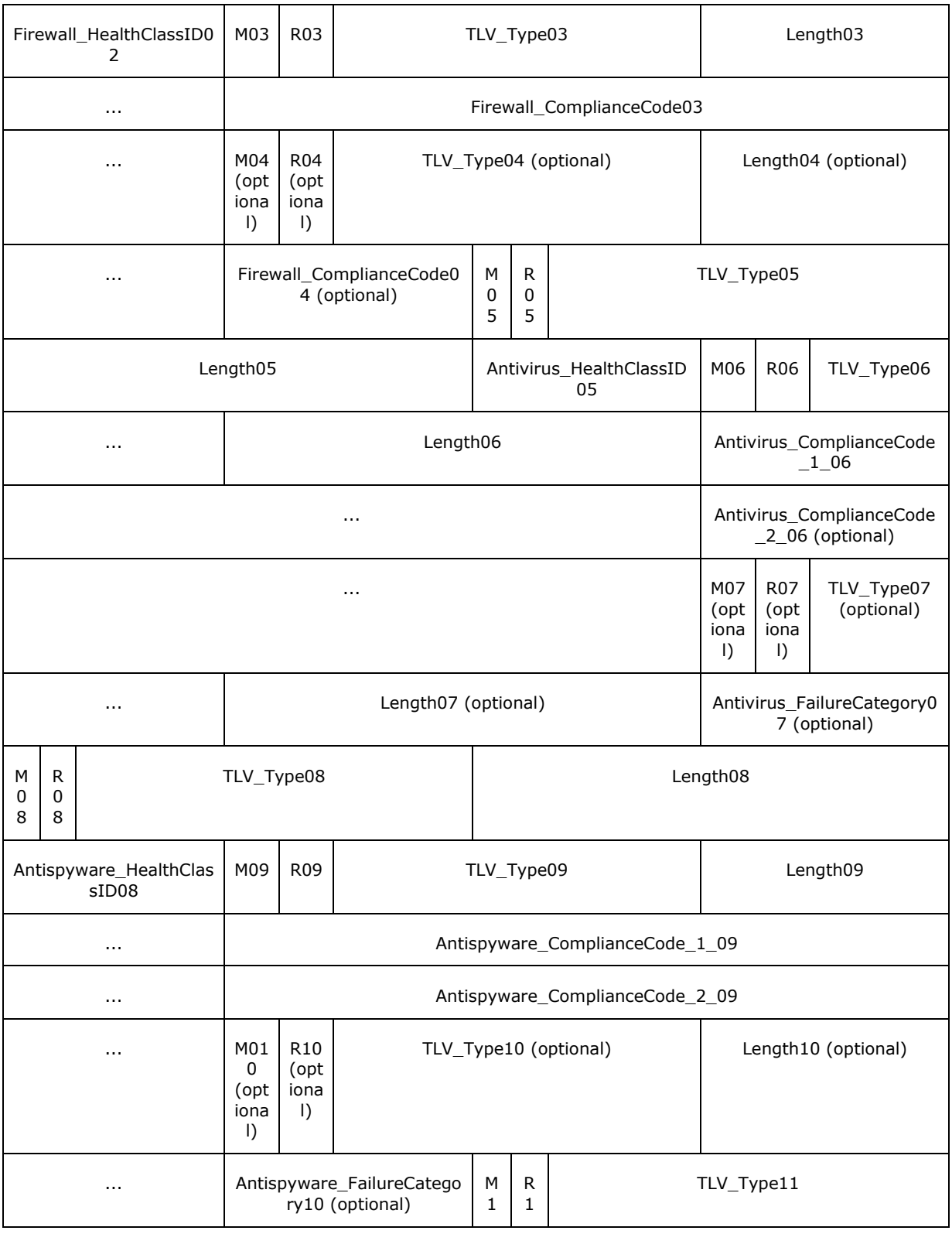
Security_Updates_UpdatesFlag19 (8 bytes): Eight bytes, as specified in section 2.2.11. Not used if Error is returned in the Security_Updates_ClientStatusCode (see section 2.2.8).

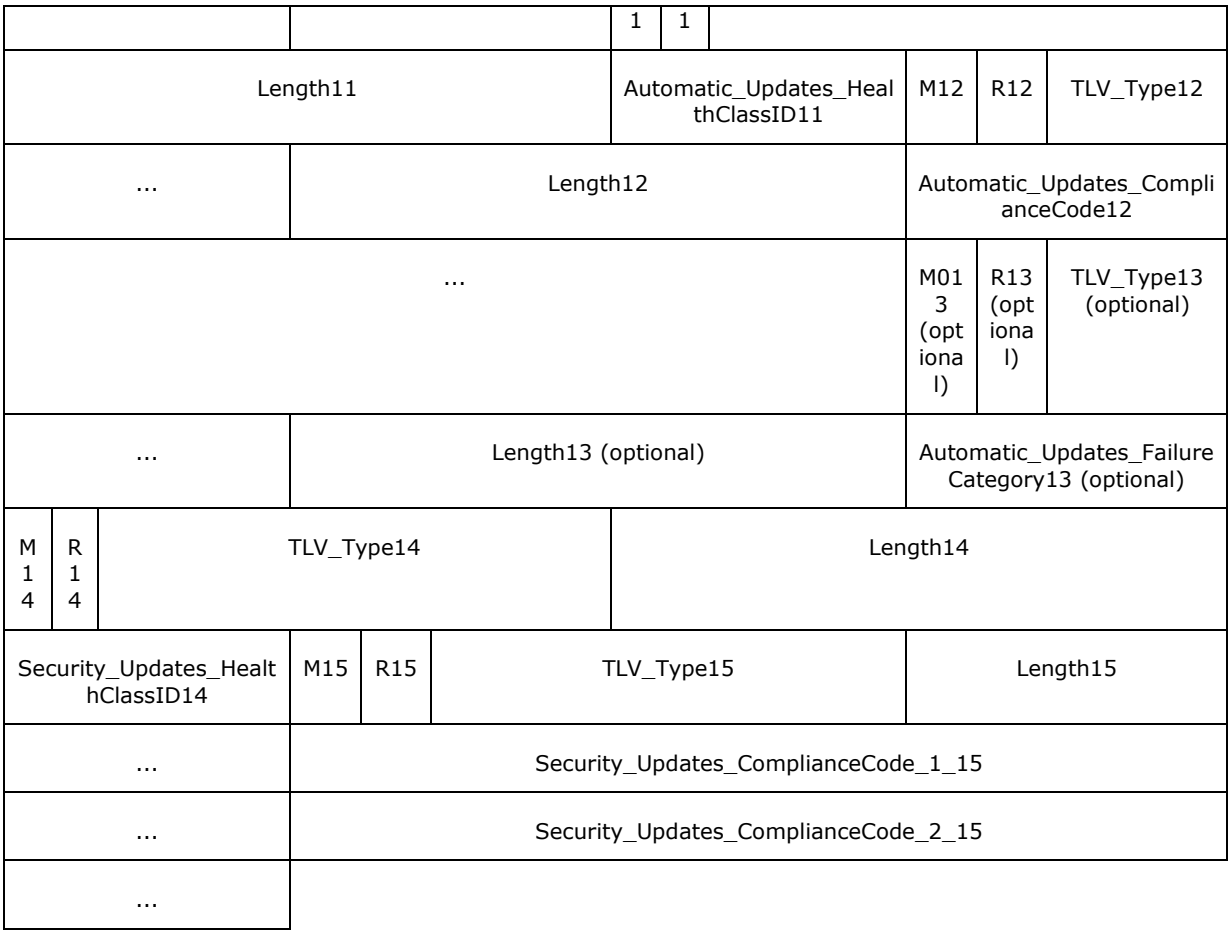
Note If Security_Updates_ClientStatusCode is an error, TLVs 17, 18, and 19 will not be present.

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. The M and R bits are defined in the Statement of Health for Network Access Protection (NAP) Protocol [MS-SOH] and are ignored by the WSHA upon receipt.







M01 (1 bit): The **M** bit MUST be set to zero.

R01 (1 bit): The **R** bit is reserved, and MUST be set to zero when sent and ignored on receipt.

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

Length01 (2 bytes): A 16-bit unsigned integer in network-byte order that MUST indicate the length (4) in bytes of the **NAPSystemHealthID** field.

NAPSystemHealthID01 (4 bytes): A 32-bit unsigned integer, as specified in section 2.2.3.

M02 (1 bit): The **M** bit MUST be set to zero.

R02 (1 bit): The **R** bit is reserved, and MUST be set to zero when sent and ignored on receipt.

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

Length02 (2 bytes): A 16-bit unsigned integer in network-byte order that MUST indicate the length (1) in bytes of the **Firewall_HealthClassID** field.

Firewall_HealthClassID02 (1 byte): An 8-bit unsigned integer, as specified in section 2.2.6.

M03 (1 bit): The **M** bit MUST be set to zero.

R03 (1 bit): The **R** bit is reserved, and MUST be set to zero when sent and ignored on receipt.

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

Length03 (2 bytes): A 16-bit unsigned integer in network-byte order that MUST indicate the length (4) in bytes of the **Firewall_ComplianceCode** field.

Firewall_ComplianceCode03 (4 bytes): A DWORD, as specified in section 2.2.12.

M04 (1 bit): The **M** bit MUST be set to zero.

R04 (1 bit): The **R** bit is reserved and MUST be set to zero when sent and ignored on receipt.

TLV_Type04 (14 bits): The **TLV Type** MUST be set to 14.

Length04 (2 bytes): A 16-bit unsigned integer that MUST be set to 1.

Firewall_ComplianceCode04 (1 byte): An 8-bit field that MUST be set to 2.

M05 (1 bit): The **M** bit MUST be set to zero.

R05 (1 bit): The **R** bit is reserved, and MUST be set to zero when sent and ignored on receipt.

TLV_Type05 (14 bits): A 14-bit unsigned integer that MUST be set to 8.

Length05 (2 bytes): A 16-bit unsigned integer in network-byte order that MUST indicate the length (1) in bytes of the **Antivirus_HealthClassID** field.

Antivirus_HealthClassID05 (1 byte): An 8-bit unsigned integer, as specified in section 2.2.6.

M06 (1 bit): The **M** bit MUST be set to zero.

R06 (1 bit): The **R** bit is reserved, and MUST be set to zero when sent and ignored on receipt.

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

Length06 (2 bytes): A 16-bit unsigned integer in network-byte order that MUST indicate the length (4) in bytes of the **Antivirus_ComplianceCode_1** field if only the **Antivirus_ComplianceCode_1** is used or length (8) if the **Antivirus_ComplianceCode_2** is also present.

Antivirus_ComplianceCode_1_06 (4 bytes): A DWORD, as specified in section 2.2.12.

Antivirus_ComplianceCode_2_06 (4 bytes): A DWORD, as specified in section 2.2.13.

M07 (1 bit): The **M** bit MUST be set to zero.

R07 (1 bit): The **R** bit is reserved and MUST be set to zero when sent and ignored on receipt.

TLV_Type07 (14 bits): The **TLV Type** MUST be set to 14.

Length07 (2 bytes): A 16-bit unsigned integer that MUST be set to 1.

Antivirus_FailureCategory07 (1 byte): An 8-bit field that MUST be set to 2.

M08 (1 bit): The **M** bit MUST be set to zero.

R08 (1 bit): The **R** bit is reserved, and MUST be set to zero when sent and ignored on receipt.

TLV_Type08 (14 bits): A 14-bit unsigned integer that MUST be set to 8.

Length08 (2 bytes): A 16-bit unsigned integer in network-byte order that MUST indicate the length (1) in bytes of the **Antispyware_HealthClassID** field.

Antispyware_HealthClassID08 (1 byte): An 8-bit unsigned integer, as specified in section 2.2.6.

M09 (1 bit): The **M** bit MUST be set to zero.

R09 (1 bit): The **R** bit is reserved, and MUST be set to zero when sent and ignored on receipt.

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

Length09 (2 bytes): A 16-bit unsigned integer in network-byte order that MUST indicate the length (4) in bytes of the **Antispyware_ComplianceCode_1** field if only the **Antispyware_ComplianceCode_1** is used, or length (8) if the **Antispyware_ComplianceCode_2** is also present.

Antispyware_ComplianceCode_1_09 (4 bytes): A DWORD value, as specified in section 2.2.12.

Antispyware_ComplianceCode_2_09 (4 bytes): A DWORD, as specified in section 2.2.13.

M010 (1 bit): The **M** bit MUST be set to zero.

R10 (1 bit): The **R** bit is reserved and MUST be set 0 and ignored on receipt.

TLV_Type10 (14 bits): The **TLV Type** MUST be set to 14.

Length10 (2 bytes): A 16-bit unsigned integer that MUST be set to 1.

Antispyware_FailureCategory10 (1 byte): An 8-bit field that MUST be set to 2.

M11 (1 bit): The **M** bit MUST be set to zero.

R11 (1 bit): The **R** bit is reserved, and MUST be set to zero when sent and ignored on receipt.

TLV_Type11 (14 bits): A 14-bit unsigned integer that MUST be set to 8.

Length11 (2 bytes): 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_HealthClassID11 (1 byte): An 8-bit unsigned integer, as specified in section 2.2.6.

M12 (1 bit): The **M** bit MUST be set to zero.

R12 (1 bit): The **R** bit is reserved, and MUST be set to zero when sent and ignored on receipt.

TLV_Type12 (14 bits): A 14-bit unsigned integer that MUST be set to 4.

Length12 (2 bytes): 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_ComplianceCode12 (4 bytes): A DWORD, as specified in section 2.2.12.

M013 (1 bit): The **M** bit MUST be set to zero.

R13 (1 bit): The **R** bit is reserved and MUST be set to zero when sent and ignored on receipt.

TLV_Type13 (14 bits): The **TLV Type** MUST be set to 14.

Length13 (2 bytes): A 16-bit unsigned integer that MUST be set to 1.

Automatic_Updates_FailureCategory13 (1 byte): An 8-bit field that MUST be set to 2.

M14 (1 bit): The **M** bit MUST be set to zero.

R14 (1 bit): The **R** bit is reserved, and MUST be set to zero when sent and ignored on receipt.

TLV_Type14 (14 bits): A 14-bit unsigned integer that MUST be set to 8.

Length14 (2 bytes): 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_HealthClassID14 (1 byte): An 8-bit unsigned integer, as specified in section 2.2.6.

M15 (1 bit): The **M** bit MUST be set to zero.

R15 (1 bit): The **R** bit is reserved, and MUST be set to zero when sent and ignored on receipt.

TLV_Type15 (14 bits): A 14-bit unsigned integer that MUST be set to 4.

Length15 (2 bytes): A 16-bit unsigned integer in network-byte order that MUST indicate the length (4) in bytes of the **Security_Updates_ComplianceCode_1** field if only the **Security_Updates_ComplianceCode_1** is used or length (8) if the **Security_Updates_ComplianceCode_2** is also present.

Security_Updates_ComplianceCode_1_15 (4 bytes): A DWORD, as specified in section 2.2.12.

Security_Updates_ComplianceCode_2_15 (4 bytes): A DWORD, as specified in section 2.2.13.

2.2.3 NAPSystemHealthID

NAPSystemHealthID is a 32-bit unsigned integer that is assigned by NAP. This NAPSystemHealthID is used to differentiate the WSHA SoH packets and WSHV SoHR packets from those of other security health agents. The NAPSystemHealthID value for the WSHA and the WSHV MUST be set to 0x00013780 (79744) which is the NAP assigned ID for WSHA and WSHV.

2.2.4 Flag

This consists of eight bytes. The first four bytes are the VendorID and MUST be 0x00013780. The second four bytes are a DWORD that is incremented for each new SoH. It is used to determine if the SoH is a duplicate.

2.2.5 Version

This consists of eight bytes. The first four bytes are the VendorID and MUST be 0x00013780. The second four bytes are a DWORD that differentiates the WSHA client version so that the WSHV knows how to handle client version-specific messages. The Microsoft Windows® client versions are as follows:

Value	Meaning
0x00050001	Windows® XP operating system WSHA
0x00060000	Windows Vista® operating system WSHA
0x00060001	Windows Vista® operating system with Service Pack 1 (SP1)WSHA

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 WSHA and the WSHV HealthClassIDs are as follows.

Value	Meaning
0x00	Firewall
0x01	Antivirus
0x02<2>	Antispyware
0x03	Automatic Updates
0x04	**Security Updates**

2.2.7 ProductName

This is a variable Unicode string that contains the product name reported for each health class. This name is passed to the WSHA by Microsoft Windows® Security Center **(WSC)**. When the ClientStatusCode for firewall, antivirus, or antispyware is 0xC0FF0002 (Product Not Installed), then there will be no corresponding ProductName TLV. If the ClientStatusCode for firewall, antivirus, or antispyware is 0xC0FF0003 (E_MSSHAV_WSC_SERVICE_DOWN) or 0x00FF0008 (E_MSSHAV_WSC_SERVICE_ NOT_STARTED_SINCE_BOOT), then the ProductName TLV MUST NOT be present. There can be multiple ProductName TLVs.

2.2.8 ClientStatusCode

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

The 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 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 forWindows 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.
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	The WUA

Value	ClientStatusCode status	Applicable health classes	Meaning
		updates	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 updates	The WSC service is not available to report status.
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 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	0101	0x5

Condition	Binary representation (B3,B2,B1,B0)	Hex representation
and not snoozed.		
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.	0001	0x1
AU enabled, but check only for updates.	0010	0x2

Condition	Binary representation (B3,B2,B1,B0)	Hex representation
AU enabled, and download updates.	0011	0x3
AU enabled, and download and install updates.	0100	0x4
AU never configured	0101	0x5

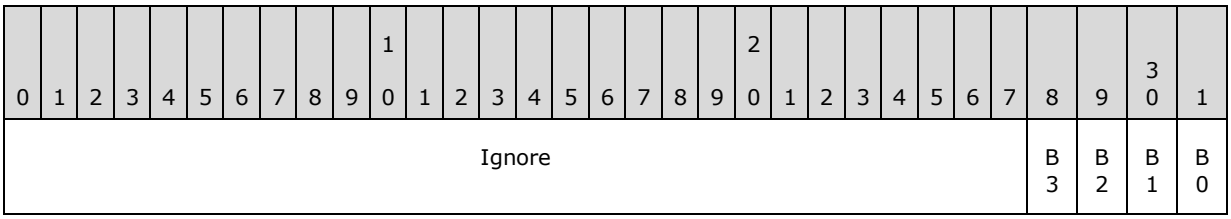
Independent of the above states, the last bit of the third byte of the AU ClientStatusCode can take the value of 1 if the AU settings on the client are controlled by policy. So the ClientStatusCode can be of either of the following two forms (where 'X' is described by the preceding table):

- 0x0000000X – Not configured by policy
- 0x0000010X – Configured by policy

Because a product within a health class may have more than one state, but each product can be reported only once 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.)

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

The ClientStatusCode Packet



Ignore (28 bits): This field MUST be ignored on receipt.

B3 (1 bit): 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 (1 bit): 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 (1 bit): 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 (1 bit): 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 comprised of eight bytes. The first four bytes are the VendorID and MUST be 0x00013780. The second four bytes are a DWORD that contains the time in seconds since the client last scanned for updates. If the Security_Updates_ClientStatusCode is an error, then this TLV is not used.<3>

2.2.10 WSUSServerName

This consists of four bytes plus a variable-length string. The first four bytes are the Vendor ID and MUST be 0x0013780. The string reports the name of the Microsoft Windows® Server Update Services (WSUS) server with which the client is enlisted. This TLV is optional, depending on whether or not the client is using WSUS for security updates. If the Security_Updates_ClientStatusCode is an error, then this TLV is not used. If the client is not registered with WSUS, the Vendor ID MUST be followed by a single byte of zeros (0x00) rather than a variable-length string.

2.2.11 UpdatesFlag

This consists of eight bytes. The first four bytes are the VendorID and MUST be 0x00013780. The second four bytes are a DWORD that reports specific information on the security update status of the client.<4> 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 following tables. If the Security_Updates_ClientStatusCode is an error, then this TLV is not used.

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

Value	Source enlistments
0x00004000	Microsoft Windows® Update
0x00010000	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 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 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.
0xC0FF0007	E_MSSHV_SYNC_AND_INSTALL_UPDATES	Security updates	The client has missing required security updates, or it has exceeded the maximum allowable

Value	ComplianceCode name	Applicable health classes	Meaning
			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 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.
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	WSC reports that a firewall, antivirus, or antispyware application is not installed.

Value	ComplianceCode name	Applicable health classes	Meaning
0xC0FF0003	E_MSSHAV_WSC_SERVICE_DOWN	Firewall, antivirus, antispyware, and automatic updates	TheWSC service is not available to report status.
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 Microsoft 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

Value	ComplianceCode name	Applicable health classes	Meaning
			Server Updates Services server, but the client is getting them from a different 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 compliance code is not used for antivirus and anti-spyware 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. The severity ratings are defined as follows.

Rating	Definition
Critical	A vulnerability whose exploitation could allow the propagation of an Internet worm without user action.
Important	A vulnerability whose exploitation could result in compromise of the confidentiality, integrity, or availability of users' data, or of the integrity or availability of processing resources.
Moderate	Exploitability is mitigated to a significant degree by factors such as default configuration, auditing, or difficulty of exploitation.
Low	A vulnerability whose exploitation is extremely difficult or whose impact is minimal.

The status is given by setting bits to flag the severity ratings. If the ClientStatusCode sent in the SoH for Security Updates is S_MSSHA_NO_MISSING_UPDATES (0x00FF0005) or S_MSSHA_MISSING_UPDATES (0x00FF0006), then the value returned for ComplianceCode2 in the SoHR is 0x00000000.

Value	Severity rating
0x00000040	Unspecified
0x00000080	Low
0x00000100	Moderate
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 SoH and receives an SoHR. It is represented graphically in the following diagram.

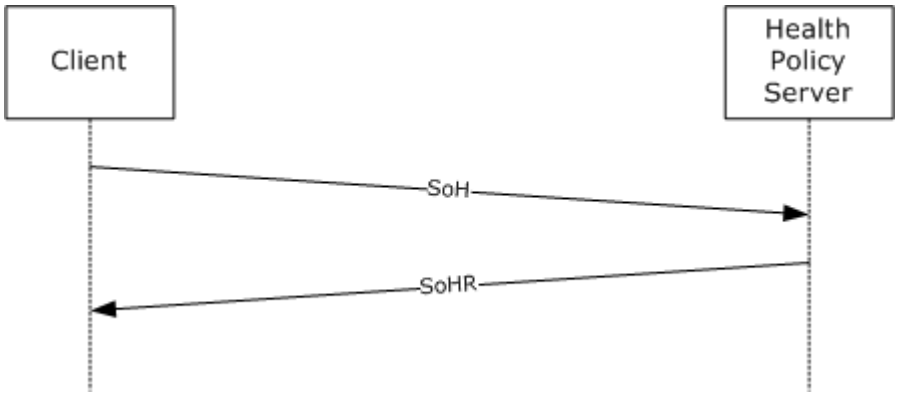


Figure 2: Client SOH request and Health Policy Server response

The WSHA provides status in the form of an SoHReportEntry in the SoH. The 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 consist of a single exchange. The following should be noted:

- The WSHA reports the client's security health status, and the 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:

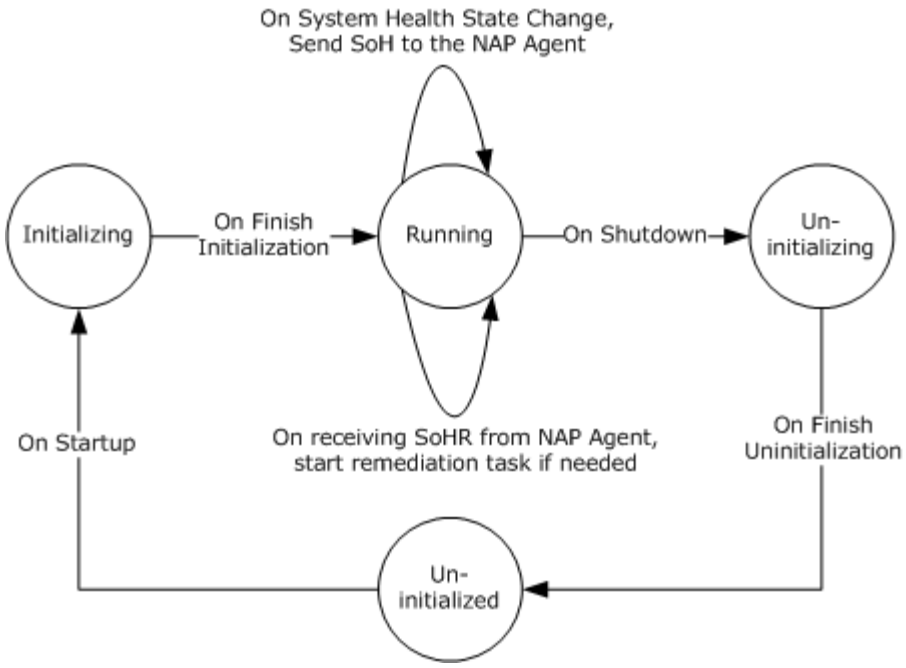


Figure 3: WSHA state

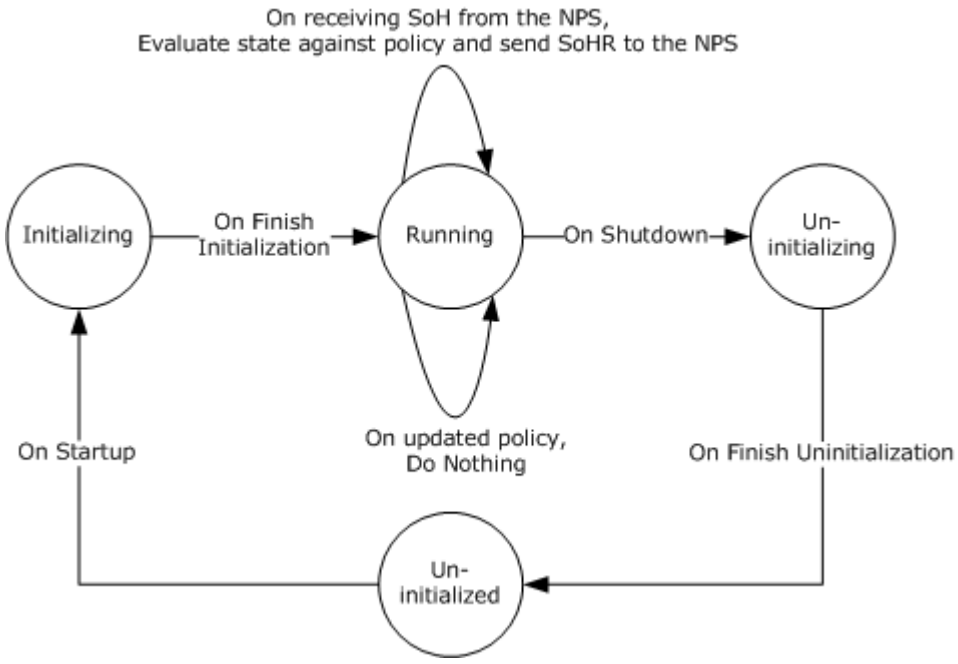


Figure 4: WSHV state

- 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 set the value of the NAPSystemHealthID field to 0x13780 for both the SoH and SoHR messages. This value is used to identify the messages that were sent by either the WSHA or WSHV to ensure that the message is received correctly by the corresponding WSHA or WSHV.
- 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.<5>
- The WSHA initializes the value to 0 when the service is started on the client, and then increments that value for each SoH sent. The service is restarted when the client is rebooted or when the NAP Agent service on the client is restarted.
- The WSHA is stateless, so when it sends an SoH, it does not actively wait for an SoHR. If the client sends an SoH, the client will not send a new SoH unless the security health status changes or a new SoH is requested by the NAP agent.
- The health policy configuration ADM elements used by the WSHV are stored in the registry.<6> The health policy is used to evaluate the SoH sent by the client to the WSHV as described in section 3.1.5.3. The values for the ADM elements are as follows:

Name	Type	Description
MaxDurationSinceLastSync	DWORD	Specifies the maximum number of seconds allowed since software updates were last synchronized. The maximum value is 259,200 seconds (72 hours).
AntiVirusUptoDate	DWORD	When the value of this ADM element is 1, the client is required to have antivirus signatures that are up-to-date. When the value is 0, the client can have antivirus signatures that are not up-to-date.
AntiVirusRealTime	DWORD	When the value of this ADM element is 1, the client is required to have the antivirus software enabled. When the value is 0, the client can have the antivirus software disabled or not installed.
AutoUpdate	DWORD	When the value of this ADM element is 1, the client is required to have the Automatic Updates feature enabled. When the value is 0, the client can have the Automatic Updates feature disabled.
WUAllowed	DWORD	When the value of this ADM element is 1, the WSHA can query Microsoft Windows® Update for software updates. When the value is 0, the WSHA should not query Windows Update.
EnforceUpdates	DWORD	When the value of this ADM element is 1, the WSHA enforces software updates on the client. When the value is 0, the WSHA does not enforce software updates on the client.
WSUSAllowed	DWORD	When the value of this ADM element is 1, the WSHA can query Windows Software Updates Services for software updates. When the value is 0, the WSHA should not query

Name	Type	Description
		Windows Software Update Services for software updates.
MinimumSeverityRating	DWORD	When the value of this ADM element is 1, the client is required to have all Low, Moderate, Important, and Critical software updates installed. When the value is 2, the client is required to have all Moderate, Important, and Critical software updates installed. When the value is 3, the client is required to have all Important and Critical software updates installed. When the value is 4, the client is required to have all Critical software updates installed.
Firewall	DWORD	When the value of this ADM element is 1, the client is required to have a firewall enabled. When the value is 0, the client can have the firewall disabled.
AntiSpywareScanEnabled<7>	DWORD	When the value of this ADM element is 1, the client is required to have antispyware software enabled. When the value is 0, the client can have antispyware software disabled or not installed.
AntiSpywareUptoDate<8>	DWORD	When the value of this ADM element is 1, the client is required to have antispyware signatures that are up-to-date. When the value is 0, the client can have antispyware signatures that are not up-to-date.

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

None.

3.1.5 Processing Events and Sequencing Rules

3.1.5.1 General Problems

If the WSHV is unable to process the security updates health class received in the WSHA SoH, or if the WSHV is unable to interpret or evaluate the received WSHA SoH, the WSHV MUST return the error code E_MSSHV_WUS_SHC_FAILURE in the SoHR. Examples of this include, but are not limited to, when the received WSHA SoH is not formatted properly or when the WSHV cannot access its policy store.

The WSHA is stateless, so when it sends an SoH, it does not actively wait for an SoHR. If the client sends an SoH, it will not send a new SoH unless the security health status changes or a new SoH is requested by the NAP agent.

3.1.5.2 Setting the NAP System Health ID Field

The NAPSystemHealthID (section 2.2.3) is used to differentiate the WSHA SoH packets and the WSHV SoHR packets from those of other security health agents. The NAPSystemHealthID01 value for the WSHA SoH packets and the WSHV SoHR packets MUST always be set to 0x00013780 (79744), which is the NAP assigned ID for WSHA and WSHV. The processing rules for setting the NAPSystemHealthID01 value in the WSHA SoH packets or the WSHV SoHR packets are called in the following scenarios:

- For WSHA, the NAPSystemHealthID01 value is set whenever a WSHA SoH packet is created. Creation of the WSHA SoH packet is triggered during creation of an SoH, as specified in [MS-SOH] section 3.2.5. When processing an SoHR packet, the NAPSystemHealthID01 value MUST equal 0x00013780 (79744) prior to passing the packet to WSHA, as specified in [MS-SOH] section 3.2.5.4.
- For WSHV, the NAPSystemHealthID01 value is set whenever a WSHV SoHR packet is created. Creation of the WSHV SoHR packet is triggered during creation of an SoHR, as specified in [MS-SOH] section 3.3.5.3. When processing an SoH packet, the NAPSystemHealthID01 value MUST equal 0x00013780 (79744) prior to passing the packet to WSHV, as specified in [MS-SOH] section 3.3.5.2.

3.1.5.3 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 NPS.

Status sent in SoH	Policy defined in NPS	ComplianceCode returned in SoHR
E_MSSHAV_WSC_SERVICE_DOWN	At least one of the following is required: firewall, antivirus, antispyware, or automatic updates, as defined by the **AntiVirusRealTime**, **AutoUpdate**, **Firewall**, and **AntiSpywareScanEnabled** ADM elements specified in section 3.1.1.<9>	E_MSSHAV_WSC_SERVICE_DOWN
E_MSSHAV_WSC_SERVICE_ NOT_STARTED_SINCE_BOOT	At least one of the following is required: firewall, antivirus, antispyware, or automatic updates, as defined by the **AntiVirusRealTime**, **AutoUpdate**, **Firewall**, and **AntiSpywareScanEnabled** ADM elements specified in section 3.1.1.<10>	E_MSSHAV_WSC_SERVICE_ NOT_STARTED_SINCE_BOOT Failure Category 0x000E0102, defined in [MS-SOH], is inserted immediately after this compliance code indicating a failure in a client component.
E_MSSHAV_NO_WUS_SERVER	Security updates required, as defined by the **EnforceUpdates** ADM element specified in section 3.1.1.	E_MSSHAV_NO_WUS_ SERVER<11>
E_MSSHAV_NO_CLIENT_ID	Security updates required, as defined by the	E_MSSHAV_NO_CLIENT_ID

Status sent in SoH	Policy defined in NPS	ComplianceCode returned in SoHR
	EnforceUpdates ADM element specified in section 3.1.1.	
E_MSSHAV_WUA_SERVICE_ NOT_STARTED_SINCE_BOOT	Security updates required, as defined by the **EnforceUpdates** ADM element specified in section 3.1.1.	E_MSSHAV_WUA_SERVICE_ NOT_STARTED_SINCE_BOOT
E_MSSHA_WUA_SERVICE_ DISABLED	Security updates required, as defined by the **EnforceUpdates** ADM element specified in section 3.1.1.	E_MSSHA _WUA_SERVICE_ DISABLED
E_MSSHAV_WUA_COMM_ FAILURE	Security updates required, as defined by the **EnforceUpdates** ADM element specified in section 3.1.1.	E_MSSHAV_WUA_COMM_ FAILURE
E_MSSHAV_PRODUCT_NOT_ INSTALLED	Product required, as defined by the **AntiVirusRealTime**, **AutoUpdate**, **Firewall**, and **AntiSpywareScanEnabled** ADM elements specified in section 3.1.1.	E_MSSHV_THIRD_PARTY_PRODUCT_ NOT_ENABLED
S_MSSHA_NO_MISSING_ UPDATES and DurationSinceLastSynch = X	Security updates required, as defined by the **EnforceUpdates** ADM element specified in section 3.1.1, and X is less than or equal to the value of the **MaxDurationSinceLastSync** ADM element specified in section 3.1.1.	ComplianceCode1: S_OK ComplianceCode2: 0x00000000
S_MSSHA_NO_MISSING_ UPDATES and DurationSinceLastSynch = X	Security updates required, as defined by the **EnforceUpdates** ADM element specified in section 3.1.1, and X is greater than the value of the **MaxDurationSinceLastSync** ADM element specified in section 3.1.1.	ComplianceCode1: E_MSSHV_SYNC_AND_ INSTALL_UPDATES ComplianceCode2: Defined in Section 2.2.13.2.
S_MSSHA_MISSING_UPDATES	Security updates required, as defined by the **EnforceUpdates** ADM element specified in section 3.1.1, and available updates are of a severity equivalent to the value of the **MinimumSeverityRating**	ComplianceCode1: E_MSSHV_SYNC_AND_ INSTALL_UPDATES ComplianceCode2: Defined in Section 2.2.13.2.

Status sent in SoH	Policy defined in NPS	ComplianceCode returned in SoHR
	ADM element specified in section 3.1.1.	
E_MSSHAV_UPDATES_ INSTALLED_REQUIRE_REBOOT	Security updates required, as defined by the **EnforceUpdates** ADM element specified in section 3.1.1.	E_MSSHAV_UPDATES_ INSTALLED_REQUIRE_REBOOT
Client passes its security update source as either Microsoft Windows® Update or Windows Server Update Services in the **UpdatesFlag** field.	Security updates required, as defined by the **EnforceUpdates** ADM element specified in section 3.1.1; the updates are required to come from Windows Update as defined by the **WUAllowed** and **WSUSAllowed** ADM elements specified in section 3.1.1.	E_MSSHAV_BAD_UPDATE_ SOURCE_MU<12>
Client passes its security update source as both Windows Update and Windows Server Update Services in the **UpdatesFlag** field.	Security updates required, as defined by the **EnforceUpdates** ADM element specified in section 3.1.1; the updates are required to come from Windows Update as defined by the **WUAllowed** and **WSUSAllowed** ADM elements specified in section 3.1.1.	E_MSSHAV_BAD_UPDATE_ SOURCE_WUMU<13>
Client passes its security update source as both Windows Update and Windows Server Update Services in the **UpdatesFlag** field.	Security updates required, as defined by the **EnforceUpdates** ADM element specified in section 3.1.1; the updates are required to come from Windows Update as defined by the **WUAllowed** and **WSUSAllowed** ADM elements specified in section 3.1.1.	E_MSSHAV_BAD_UPDATE_ SOURCE_MU<14>
Client passes its security update source as Windows Server Update Services in the **UpdatesFlag** field.	Security updates required, as defined by the **EnforceUpdates** ADM element specified in section 3.1.1; the updates are required to come from Windows Update or Windows Server Update Services as defined by the **WUAllowed** and **WSUSAllowed** ADM elements specified in section	E_MSSHAV_BAD_UPDATE_ SOURCE_WUMU<15>

Status sent in SoH	Policy defined in NPS	ComplianceCode returned in SoHR
	3.1.1.	
Client passes its security update source as Windows Update in the **UpdatesFlag** field.	Security updates required, as defined by the **EnforceUpdates** ADM element specified in section 3.1.1; the updates are required to come from Windows Update or Windows Server Update Services as defined by the **WUAllowed** and **WSUSAllowed** ADM elements specified in section 3.1.1.	E_MSSHAV_BAD_UPDATE_ SOURCE_MUWSUS<16><17>
Client passes no security update source in the **UpdatesFlag** field.	Security updates required, as defined by the **EnforceUpdates** ADM element specified in section 3.1.1.	E_MSSHAV_NO_UPDATE_ SOURCE<18>

The following are for antivirus and antispyware.

Status sent in SoH	Policy defined in NPS	ComplianceCode returned in SoHR
Any	Product not required, as defined by the **AntiVirusRealTime** and **AntiSpywareScanEnabled** ADM elements specified in section 3.1.1.	ComplianceCode 1: S_OK
Any	Product not required, as defined by the **AntiVirusRealTime** and **AntiSpywareScanEnabled** ADM elements specified in section 3.1.1.	ComplianceCode 2: S_OK
0x7 or 0x3	Product required to be enabled and up-to-date, as defined by the **AntiVirusRealTime**, **AntiVirusUptoDate**, **AntiSpywareScanEnabled**, and **AntiSpywareUptoDtate** ADM elements specified in section 3.1.1.	ComplianceCode 1: S_OK
0x7 or 0x3	Product required to be enabled and up-to-date, as defined by the **AntiVirusRealTime**, **AntiVirusUptoDate**, **AntiSpywareScanEnabled**, and **AntiSpywareUptoDtate** ADM elements specified in section 3.1.1.	ComplianceCode 2: S_OK
0x7 or 0x3	Product required to be enabled, as defined by the **AntiVirusRealTime** and **AntiSpywareScanEnabled** ADM	ComplianceCode 1: S_OK

Status sent in SoH	Policy defined in NPS	ComplianceCode returned in SoHR
	elements specified in section 3.1.1.	
0x7 or 0x3	Product required to be enabled, as defined by the **AntiVirusRealTime** and **AntiSpywareScanEnabled** ADM elements specified in section 3.1.1.	ComplianceCode 2: S_OK
0x4	Product required to be enabled and up-to-date, as defined by the **AntiVirusRealTime**, **AntiVirusUptoDate**, **AntiSpywareScanEnabled**, and **AntiSpywareUptoDtate** ADM elements specified in section 3.1.1.	ComplianceCode 1: E_MSSHV_PRODUCT_NOT_ENABLED
0x4	Product required to be enabled and up-to-date, as defined by the **AntiVirusRealTime**, **AntiVirusUptoDate**, **AntiSpywareScanEnabled**, and **AntiSpywareUptoDtate** ADM elements specified in section 3.1.1.	ComplianceCode 2: E_MSSHV_PRODUCT_NOT_UPTODATE
0x4	Product required to be enabled, as defined by the **AntiVirusRealTime** and **AntiSpywareScanEnabled** ADM elements specified in section 3.1.1.	ComplianceCode 1: E_MSSHV_PRODUCT_NOT_ENABLED
0x4	Product required to be enabled, as defined by the **AntiVirusRealTime** and **AntiSpywareScanEnabled** ADM elements specified in section 3.1.1.	ComplianceCode 2: S_OK
0x5	Product required to be enabled and up-to-date, as defined by the **AntiVirusRealTime**, **AntiVirusUptoDate**, **AntiSpywareScanEnabled**, and **AntiSpywareUptoDtate** ADM elements specified in section 3.1.1.	ComplianceCode 1: S_OK
0x5	Product required to be enabled and up-to-date, as defined by the **AntiVirusRealTime**, **AntiVirusUptoDate**, **AntiSpywareScanEnabled**, and **AntiSpywareUptoDtate** ADM elements specified in section 3.1.1.	ComplianceCode 2: E_MSSHV_PRODUCT_NOT_UPTODATE
0x5	Product required to be enabled, as defined by the **AntiVirusRealTime** and **AntiSpywareScanEnabled** ADM elements specified in section 3.1.1.	ComplianceCode 1: S_OK
0x5	Product required to be enabled, as defined by the **AntiVirusRealTime**	ComplianceCode 2:

Status sent in SoH	Policy defined in NPS	ComplianceCode returned in SoHR
	and **AntiSpywareScanEnabled** ADM elements specified in section 3.1.1.	S_OK
0x6	Product required to be enabled and up-to-date, as defined by the **AntiVirusRealTime**, **AntiVirusUptoDate**, **AntiSpywareScanEnabled**, and **AntiSpywareUptoDtate** ADM elements specified in section 3.1.1.	ComplianceCode 1: E_MSSHV_PRODUCT_NOT_ENABLED
0x6	Product required to be enabled and up-to-date, as defined by the **AntiVirusRealTime**, **AntiVirusUptoDate**, **AntiSpywareScanEnabled**, and **AntiSpywareUptoDtate** ADM elements specified in section 3.1.1.	ComplianceCode 2: S_OK
0x6	Product required to be enabled, as defined by the **AntiVirusRealTime** and **AntiSpywareScanEnabled** ADM elements specified in section 3.1.1.	ComplianceCode 1: E_MSSHV_PRODUCT_NOT_ENABLED
0x6	Product required to be enabled, as defined by the **AntiVirusRealTime** and **AntiSpywareScanEnabled** ADM elements specified in section 3.1.1.	ComplianceCode 2: S_OK
0xD	Product required to be enabled and up-to-date, as defined by the **AntiVirusRealTime**, **AntiVirusUptoDate**, **AntiSpywareScanEnabled**, and **AntiSpywareUptoDtate** ADM elements specified in section 3.1.1.	ComplianceCode 1: S_OK
0xD	Product required to be enabled and up-to-date, as defined by the **AntiVirusRealTime**, **AntiVirusUptoDate**, **AntiSpywareScanEnabled**, and **AntiSpywareUptoDtate** ADM elements specified in section 3.1.1.	ComplianceCode 2: E_MSSHV_PRODUCT_NOT_UPTODATE
0xD	Product required to be enabled, as defined by the **AntiVirusRealTime** and **AntiSpywareScanEnabled** ADM elements specified in section 3.1.1.	ComplianceCode 1: S_OK
0xD	Product required to be enabled, as defined by the **AntiVirusRealTime** and **AntiSpywareScanEnabled** ADM elements specified in section 3.1.1.	ComplianceCode 2: S_OK
0xF	Product required to be enabled and up-	ComplianceCode 1:

Status sent in SoH	Policy defined in NPS	ComplianceCode returned in SoHR
	to-date, as defined by the **AntiVirusRealTime**, **AntiVirusUptoDate**, **AntiSpywareScanEnabled**, and **AntiSpywareUptoDtate** ADM elements specified in section 3.1.1.	S_OK
0xF	Product required to be enabled and up-to-date, as defined by the **AntiVirusRealTime**, **AntiVirusUptoDate**, **AntiSpywareScanEnabled**, and **AntiSpywareUptoDtate** ADM elements specified in section 3.1.1.	ComplianceCode 2: S_OK
0xF	Product required to be enabled, as defined by the **AntiVirusRealTime** and **AntiSpywareScanEnabled** ADM elements specified in section 3.1.1.	ComplianceCode 1: S_OK
0xF	Product required to be enabled, as defined by the **AntiVirusRealTime** and **AntiSpywareScanEnabled** ADM elements specified in section 3.1.1.	ComplianceCode 2: S_OK
0x0	Product required to be enabled and up-to-date, as defined by the **AntiVirusRealTime**, **AntiVirusUptoDate**, **AntiSpywareScanEnabled**, and **AntiSpywareUptoDtate** ADM elements specified in section 3.1.1.	ComplianceCode 1: E_MSSHV_THIRD_PARTY_PRODUCT_NOT_ENABLED
0x0	Product required to be enabled and up-to-date, as defined by the **AntiVirusRealTime**, **AntiVirusUptoDate**, **AntiSpywareScanEnabled**, and **AntiSpywareUptoDtate** ADM elements specified in section 3.1.1.	ComplianceCode 2: E_MSSHV_THIRD_PARTY_PRODUCT_NOT_UPTODATE
0x0	Product required to be enabled, as defined by the **AntiVirusRealTime** and **AntiSpywareScanEnabled** ADM elements specified in section 3.1.1.	ComplianceCode 1: E_MSSHV_THIRD_PARTY_PRODUCT_NOT_ENABLED
0x0	Product required to be enabled, as defined by the **AntiVirusRealTime** and **AntiSpywareScanEnabled** ADM elements specified in section 3.1.1.	ComplianceCode 2: S_OK
0x1	Product required to be enabled and up-to-date, as defined by the **AntiVirusRealTime**, **AntiVirusUptoDate**, **AntiSpywareScanEnabled**, and	ComplianceCode 1: S_OK

Status sent in SoH	Policy defined in NPS	ComplianceCode returned in SoHR
	AntiSpywareUptoDtate ADM elements specified in section 3.1.1.	
0x1	Product required to be enabled and up-to-date, as defined by the **AntiVirusRealTime**, **AntiVirusUptoDate**, **AntiSpywareScanEnabled**, and **AntiSpywareUptoDtate** ADM elements specified in section 3.1.1.	ComplianceCode 2: E_MSSHV_THIRD_PARTY_PRODUCT_NOT_UPTODATE
0x1	Product required to be enabled, as defined by the **AntiVirusRealTime** and **AntiSpywareScanEnabled** ADM elements specified in section 3.1.1.	ComplianceCode 1: S_OK
0x1	Product required to be enabled, as defined by the **AntiVirusRealTime** and **AntiSpywareScanEnabled** ADM elements specified in section 3.1.1.	ComplianceCode 2: S_OK
0x2	Product required to be enabled and up-to-date, as defined by the **AntiVirusRealTime**, **AntiVirusUptoDate**, **AntiSpywareScanEnabled**, and **AntiSpywareUptoDtate** ADM elements specified in section 3.1.1.	ComplianceCode 1: E_MSSHV_THIRD_PARTY_PRODUCT_NOT_ENABLED
0x2	Product required to be enabled and up-to-date, as defined by the **AntiVirusRealTime**, **AntiVirusUptoDate**, **AntiSpywareScanEnabled**, and **AntiSpywareUptoDtate** ADM elements specified in section 3.1.1.	ComplianceCode 2: S_OK
0x2	Product required to be enabled, as defined by the **AntiVirusRealTime** and **AntiSpywareScanEnabled** ADM elements specified in section 3.1.1.	ComplianceCode 1: E_MSSHV_THIRD_PARTY_PRODUCT_NOT_ENABLED
0x2	Product required to be enabled, as defined by the **AntiVirusRealTime** and **AntiSpywareScanEnabled** ADM elements specified in section 3.1.1.	ComplianceCode 2: S_OK
0x9	Product required to be enabled and up-to-date, as defined by the **AntiVirusRealTime**, **AntiVirusUptoDate**, **AntiSpywareScanEnabled**, and **AntiSpywareUptoDtate** ADM elements specified in section 3.1.1.	ComplianceCode 1: S_OK
0x9	Product required to be enabled and up-	ComplianceCode 2:

Status sent in SoH	Policy defined in NPS	ComplianceCode returned in SoHR
	to-date, as defined by the **AntiVirusRealTime**, **AntiVirusUptoDate**, **AntiSpywareScanEnabled**, and **AntiSpywareUptoDtate** ADM elements specified in section 3.1.1.	E_MSSHV_THIRD_PARTY_PRODUCT_NOT_UPTODATE
0x9	Product required to be enabled, as defined by the **AntiVirusRealTime** and **AntiSpywareScanEnabled** ADM elements specified in section 3.1.1.	ComplianceCode 1: S_OK
0x9	Product required to be enabled, as defined by the **AntiVirusRealTime** and **AntiSpywareScanEnabled** ADM elements specified in section 3.1.1.	ComplianceCode 2: S_OK
0xB	Product required to be enabled and up-to-date, as defined by the **AntiVirusRealTime**, **AntiVirusUptoDate**, **AntiSpywareScanEnabled**, and **AntiSpywareUptoDtate** ADM elements specified in section 3.1.1.	ComplianceCode 1: S_OK
0xB	Product required to be enabled and up-to-date, as defined by the **AntiVirusRealTime**, **AntiVirusUptoDate**, **AntiSpywareScanEnabled**, and **AntiSpywareUptoDtate** ADM elements specified in section 3.1.1.	ComplianceCode 2: S_OK
0xB	Product required to be enabled, as defined by the **AntiVirusRealTime** and **AntiSpywareScanEnabled** ADM elements specified in section 3.1.1.	ComplianceCode 1: S_OK
0xB	Product required to be enabled, as defined by the **AntiVirusRealTime** and **AntiSpywareScanEnabled** ADM elements specified in section 3.1.1.	ComplianceCode 2: S_OK

The following are for firewall.

Status sent in SoH	Policy defined in NPS	Status returned in SoHR
Any	Firewall not required, as defined by the **Firewall** ADM element specified in section 3.1.1.	S_OK
0x5 or 0x1	Firewall required, as defined by the **Firewall** ADM element specified in	S_OK

Status sent in SoH	Policy defined in NPS	Status returned in SoHR
	section 3.1.1.	
0x4	Firewall required, as defined by the **Firewall** ADM element specified in section 3.1.1.	E_MSSHV_PRODUCT_NOT_ENABLED
0x0	Firewall required, as defined by the **Firewall** ADM element specified in section 3.1.1.	E_MSSHV_THIRD_PARTY_PRODUCT_NOT_ENABLED
0xD	Firewall required, as defined by the **Firewall** ADM element specified in section 3.1.1.	S_OK
0x9	Firewall required, as defined by the **Firewall** ADM element specified in section 3.1.1.	S_OK

The following are for automatic updates (AU).

Status sent in SoH	Policy defined in NPS	Status returned in SoHR
Any	AU not required, as defined by the **AutoUpdate** ADM element specified in section 3.1.1.	S_OK
0x002, 0x0102, 0x003, 0x103, 0x004, or 0x104	AU required, as defined by the **AutoUpdate** ADM element specified in section 3.1.1.	S_OK
0x001, 0x101, 0x005, or 0x105<19>	AU required, as defined by the **AutoUpdate** ADM element specified in section 3.1.1.	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

3.1.7.1 Client and Server Abstract Interfaces

The **Network Access Protection (NAP) client** communicates with the WSHA using public APIs described in [MSDN-INapSysHA]. The WSHA APIs enable the NAP client to query for an SoH message to send an SoH to the WSHV and to receive an SoHR for remediation.

The network policy server (NPS) communicates with the WSHV using public APIs described in [MSDN-INapSysHV]. The WSHV APIs enable the NPS to pass the received SoH from the SHA and to query for the SoHR to send to the WSHA.

The data types that are used with the NAP interfaces are described in [MSDN-NapDatatypes].

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 SoH, and then receives a 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 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 SoHR.
4. The client receives the SoHR, and then places itself in quarantine.
5. After the virus definitions are updated, a new SoH is sent showing that the client is in compliance with policy.
6. The WSHV returns an S_OK in the 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

None.

5.2 Index of Security Parameters

None.

6 Appendix A: Product Behavior

The information in this specification is applicable to the following Microsoft products or supplemental software. References to product versions include released service packs:

- Windows® XP operating system
- Windows Vista® operating system
- Windows Vista® operating system with Service Pack 1 (SP1)
- Windows Server® 2008 operating system
- Windows® 7 operating system
- Windows Server® 2008 R2 operating system

Exceptions, if any, are noted below. If a service pack or Quick Fix Engineering (QFE) number appears with the product version, behavior changed in that service pack or QFE. The new behavior also applies to subsequent service packs of the product unless otherwise specified. If a product edition appears with the product version, behavior is different in that product edition.

Unless otherwise specified, any statement of optional behavior in this specification that is prescribed using the terms SHOULD or SHOULD NOT implies product behavior in accordance with the SHOULD or SHOULD NOT prescription. Unless otherwise specified, the term MAY implies that the product does not follow the prescription.

<1> Section 1.7: When the implementation is configured with Windows XP, the Network Access Protection (NAP) client must be installed.

<2> Section 2.2.6: This class is implemented in Windows Vista and Windows 7. An SoH from a Windows XP client will not include the antispyware TLVs. Similarly, an SoHR back to a Windows XP client will not include the antispyware TLVs. The WSHV uses the Version field in the SoH to determine whether the client is a Windows XP, Windows Vista, or Windows 7 client. If it is from a Windows XP client, the WSHV will not expect any antispyware data to be present.

<3> Section 2.2.9: In Windows Vista and Windows 7, the DurationSinceLastSynch TLV is updated only when the statement of health (SoH) has changed.

<4> Section 2.2.11: For Windows Vista clients, the field contains the maximum severity rating of the security updates that it knows about. For Windows XP, Windows Vista SP1, and Windows 7 clients, it also contains the security update source that the client is enlisted in.

<5> Section 3.1.1: Implemented in Windows Server 2008 and Windows Server 2008 R2. The WSHV on Windows Server 2008 and Windows Server 2008 R2 does not evaluate the flag value, and therefore, will process any SoH it receives, even if the flag is a duplicate of the flag in an SoH that was received earlier.

<6> Section 3.1.1: The policy for Windows XP clients is stored in the registry key path "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows System Health Validator\{51fecd48-263c-4ea2-b304-47a3b5136809}". The policy for all clients other than Windows XP is stored in the registry key path "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows System Health Validator\{d40a68da-831c-4ca3-a273-1ac569205353}". These registry keys are consumed by the WSHV.

<7> Section 3.1.1: The **AntiSpywareScanEnabled** ADM element is used only with Windows 7 and Windows Vista clients.

<8> Section 3.1.1: The **AntiSpywareUptoDate** ADM element is used only with Windows 7 and Windows Vista clients.

<9> Section 3.1.5.3: In Windows Server 2008 and Windows Server 2008 R2, for firewall, antivirus, and antispyware, if the status is E_MSSHAV_WSC_SERVICE_DOWN and the ProductName is present (which indicates a protocol violation), then the value of the returned ComplianceCode is S_OK.

<10> Section 3.1.5.3: In Windows Server 2008 and Windows Server 2008 R2, for firewall, antivirus and antispyware, if the status is E_MSSHAV_WSC_SERVICE_ NOT_STARTED_SINCE_BOOT and the ProductName is present (which indicates a protocol violation), then the value of the returned ComplianceCode is E_MSSHV_THIRD_PARTY_PRODUCT_NOT_ENABLED. In addition, there is no accompanying Failure Category for this status as defined in [MS-SOH].

<11> Section 3.1.5.3: Implemented in Windows Vista. This status code is used only with Windows Vista RTM clients.

<12> Section 3.1.5.3: Implemented in Windows 7, Windows Vista SP1, and Windows XP. This status code is used only with Windows 7, Windows Vista SP1, and Windows XP clients.

<13> Section 3.1.5.3: Implemented in Windows 7, Windows Vista SP1, and Windows XP. This status code is used only with Windows 7, Windows Vista SP1, and Windows XP clients.

<14> Section 3.1.5.3: Implemented in Windows 7, Windows Vista SP1, and Windows XP. This status code is used only with Windows 7, Windows Vista SP1, and Windows XP clients.

<15> Section 3.1.5.3: Implemented in Windows 7, Windows Vista SP1, and Windows XP. This status code is used only with Windows 7, Windows Vista SP1, and Windows XP clients.

<16> Section 3.1.5.3: Implemented in Windows 7, Windows Vista SP1, and Windows XP. This status code is used only with Windows 7, Windows Vista SP1, and Windows XP clients.

<17> Section 3.1.5.3: In Windows Server 2008 and Windows Server 2008 R2, if the WSUSServerName TLV is missing, then the WSHV returns S_OK regardless of the update source.

<18> Section 3.1.5.3: Implemented in Windows 7, Windows Vista SP1, and Windows XP. This status code is used only with Windows 7, Windows Vista SP1, and Windows XP clients.

<19> Section 3.1.5.3: If the WSHV receives anything other than these four values for Automatic Updates, it will return S_OK in the SoHR.

7 Change Tracking

No table of changes is available. The document is either new or has had no changes since its last release.

8 Index

U

V

W