IDS Working Group

2009-12-10 Face-to-face Meeting Minutes

1. Attendees

Randy Turner*	Amalfi Systems
Lee Farrell	Canon
Jacob Brown	Dell
Rick Landau	Dell
Jody Steele	Dell
Glen Petrie*	Epson
Ira McDonald*	High North
Jerry Thrasher	Lexmark
Nancy Chen	Oki Data
Brian Smithson*	Ricoh
Joe Murdock	Sharp
Bill Wagner	TIC
Pete Zehler*	Xerox

* via telephone

2. Agenda

Joe Murdock opened the IDS session and provided the planned agenda topics:

- Administrivia:
  - Select minute-taker– Lee?
  - IP policy statement
  - Approve Minutes from December 3 conference Call
  - Review Action Items from December 3 conference call
- Status of HCD Attribute document
- Review revisions to NAP Binding document
  - Status of NAP Binding document
- Review NEA Binding document
- Discuss TNC Vendor document
- Discuss Symantec NAC Datasheet
- Discussion on SHV issues:
  - SHV development alternatives Take 2
- Discussion on remediation Take 2
  - A pseudo proposal
- More administrivia
  - IDS futures and “phase II” activity (?)
  - New action items and open issues
  - Conference call / F2F schedule
  - Adjournment

3. Minutes Taker

Lee Farrell

4. PWG Operational Policy

It was noted that all attendees should be aware that the meeting is conducted under the PWG Membership and Intellectual Property rules. There were no objections.

5. Approve Minutes from December 3 Conference Call

There were no objections to the previous Minutes.

6. Review Action Items

NOTE: The latest Action Item spreadsheet is available at: ftp://ftp.pwg.org/pub/pwg/ids/ActionItems/

AI 023: Mike Fenelon will take on the responsibility for creating a "value proposition" document to help justify the reason behind HCD NAP development. Peter Cybuck and Ron Nevo will provide market information as possible.

→ ***OPEN***

AI 025: Peter Cybuck will do some market research about whether customers will accept the proposed method of gaining network access via SCCM.

→ *Pete Cybuck has sent Joe some information, but the Action Item remains open.*
→ ***OPEN***

Discussion of AI 025 generated the following Action Item:

AI 029: Joe Murdock will [edit and] post Peter Cybuck's information about market research.

→ ***NEW***

AI 026: Joe Murdock will follow up with Eran Dvir (Microsoft) about the SCCM issues, questions, and capabilities.

→ *No new information available, despite several e-mails sent to Eran.*
→ ***OPEN***

AI 027: Joe Murdock will add NAP System Health ID to NAP Binding document and determine how to register a PWG system health ID value.

→ ***PARTIALLY CLOSED***

AI 028: Jerry Thrasher will send a note to Mike Fenelon to find out if/how it is possible to handle multiple SHVs for the same environment, the same device class, and [possibly] the same SMI number (i.e., PWG)?

→ *A call has been made; a message has been left. No response yet.*
→ ***OPEN***

7. HCD Health Attributes Document

There has been no update of the Attributes specification since June. This document status is currently labeled “Stable,” but there was some concern raised that it should actually be labeled “Prototype.” It was generally agreed that the group will leave the document as Stable.

8. NAP Binding Document

Joe led a review of the latest draft, and highlighted the recent modifications to the document. The changes were not very controversial, and were accepted as proposed.

NAPSystemHealthID was added to the document under SoH Attribute Conformance.

AI 030:	Brian Smithson or Joe Murdock will clean up the NAP document, accepting the Dec 3 modifications, and will distribute an updated revision as Prototype status.

→ ***NEW***

AI 031:	Brian Smithson or Joe Murdock will update the note in Appendix X in the NAP document to indicate that the PWG Secretary will “remove this Section.”

→ ***NEW***

9. NEA Binding Document

The NEA Binding document was updated and reviewed at the Dec 3 teleconference. There was no additional discussion.

10. TNC Vendors Document and Symantec NAC Datasheet

Randy Turner’s document on NAP/NAC Vendors Landscape was accepted as an “informational document.” Randy noted that it is no surprise that Symantec is developing NEA-compliant products, which is why he also distributed their data sheet on Endpoint Security.

He also explained that there are other TNC interfaces that “go beyond” the NEA specification. The TNC server will be a superset of what’s in the NEA specification. The plug-in interface is not standardized. Only the data exchanged over that interface is standardized.

Are any of the vendors that Randy has talked to willing to work with the PWG? Randy says he has not yet found any.

Bill Wagner wondered that if none of the vendors are interested, is there really any market perception of a need for HCD network health assessment? Randy pointed out that HCDs have [unfortunately] always been an afterthought when dealing with network devices. It is a typical oversight, and they need reminding.

During the discussion, it was suggested that the PWG could look at creating a validator code set that could be used by other groups to incorporate into their specific applications and plug-ins.

It was suggested that contact with Symantec should be made, and possibly invite them to a PWG meeting for further discussion.

Joe volunteered to investigate the Symantec product offering to evaluate its applicability to the PWG developing a prototype health validator.

Rather than continuing to wait for Microsoft to respond on the Market Rationale information, it was suggested that the group try to do something themselves. Everyone was requested to supply Joe with any market information that they might have or can reference. It was suggested that some public documents might already be available on this topic.

AI 032: Joe Murdock will to develop a "Market Rationale" document – with help from within Sharp.

→ ***NEW***

AI 033: Randy Turner will contact Symantec (when appropriate) to encourage discussion with the PWG about a SHV.

→ ***NEW***

11. System Health Validation

As stated earlier, the group wanted to consider the idea of developing a System Health Validator (SHV).

Joe reported that he is still investigating the SCCM/Forefront environment from Microsoft. He said that there has been no response yet received from Microsoft about their possible HCD SHV.

12. Remediation

Joe said that it is possible for the PWG to define a standard, generic remediation process for the HCD attributes indicated below. He said that remediation of any other attributes would require a vendor-supplied remediation process.

HCD_Default_Password_Enabled	Could be remediated by providing new password value as part of remediation
HCD_Firewall_Setting	Would require that PWG standardize the firewall values
HCD_Forwarding_Enabled	Can be set on/off. The device would be responsible to make sure the correct actions were performed.
HCD_PSTN_Fax_Enabled	Can be set on/off. The device would be responsible to make sure the correct actions were performed.
HCD_Time_Source	Device must support URIs for time source, or standardized string ("onboard") for internal clock

HCD_User_Application_Enabled	Can be set on/off
HCD_User_Application_Persistence_Enabled	Can be set on/off

Is there enough value in the above set of attributes to justify investigation and effort into defining how the remediation might be achieved?

It was again suggested that the answer to the above question is directly dependent on the market need.

MIB extension, Web Service SOAP action, and MFD model additions were all suggested as possible methods for addressing remediation.

It was noted that the Symantec data sheet includes a reference to the ability to "Remediate noncompliant endpoints." Jerry recommended that the IDS group should understand how this is achieved by Symantec.

AI 034: Randy Turner will investigate Symantec's products and their method(s) to "remediate noncompliant endpoints."

→ ***NEW***

AI 035: Joe Murdock will investigate Microsoft's method(s) of remediation. [Is it accomplished by passing a URL?]

→ ***NEW***

13. Summary of New Action Items and Open Issues

AI 029: Joe Murdock will [edit and] post Peter Cybuck's information about market research.

AI 030: Brian Smithson or Joe Murdock will clean up the NAP document, accepting the Dec 3 modifications, and will distribute an updated revision as Prototype status.

AI 031: Brian Smithson or Joe Murdock will update the note in Appendix X in the NAP document to indicate that the PWG Secretary will "remove this Section."

AI 032: Joe Murdock will to develop a "Market Rationale" document – with help from within Sharp.

AI 033: Randy Turner will contact Symantec (when appropriate) to encourage discussion with the PWG about a SHV.

AI 034: Randy Turner will investigate Symantec's products and their method(s) to "remediate noncompliant endpoints."

AI 035: Joe Murdock will investigate Microsoft’s method(s) of remediation. [Is it accomplished by passing a URL?]

14. Next Teleconference

The next IDS teleconference will be held on January 7, 1pm Eastern time.

IDS meeting adjourned.