# ARUBA CLEARPASS ONGUARD™

Enterprise-class endpoint posture assessments and health checks

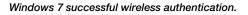
Aruba ClearPass OnGuard<sup>™</sup> agents perform advanced endpoint posture assessments, as well as traditional network access control (NAC) and network access protection (NAP) health checks to ensure compliance and safeguard networks before devices connect.

Purchased as a software license with the Aruba ClearPass Policy Manager, OnGuard agents for Windows, Mac OS X and Linux deliver exceptional visibility to determine the vulnerability and compliance of endpoints that connect to wired and wireless networks.

# THE CLEARPASS DIFFERENCE

In addition to anti-virus, anti-spyware and personal firewall audits performed by traditional NAC and NAP products, OnGuard agents perform advanced posture and health checks, such as how to handle the use of peer-to-peer applications and USB storage devices.

Wireless Network Connection	
	INFO: Authentication successful
$\checkmark$	13:39:03 Started new Session Show Old Sessions
Wireless Network Connection Wireless 10.2.50.75	
	More information Retry Logout



When running persistent OnGuard agents on endpoints, the Aruba ClearPass Policy Manager can centrally configure and manage posture and health-check settings, send system-wide notifications and alerts, and allow or deny network access.

## Persistent and dissolvable agents

Persistent and dissolvable web-based OnGuard agents provide the same posture assessment capabilities with slight exceptions. The persistent agent provides nonstop monitoring and automatic remediation and control.

Alternatively, the dissolvable web-based agent is ideal for personal, non IT-issued devices and does not require software to be permanently installed. Once the browser page that was used during the authentication process is closed, the dissolvable agent is removed.

# **KEY FEATURES**

- Enhanced capabilities for endpoint compliance and control.
- Microsoft Support for Windows 7, Windows Vista, Windows XP and Windows 2003.
- Apple Support for Mac OS X.
- Linux Support for Red Hat Enterprise Linux 4 and above, Community Enterprise Operating System (CEntOS) 4 and above, Fedora Core 5 and above, and SUSE Linux 10.x.
- Anti-virus, anti-spyware and firewall checks with auto-remediation.
- Peer-to-peer application checks, process checks and registry-key checks with remediation.
- System-wide endpoint messaging, notifications and access control.
- Online status of all devices can be viewed in the Aruba ClearPass Policy Manager.

## Automatic remediation

If an unhealthy endpoint does not meet compliance requirements, the user receives a message about the endpoint status and instructions on how to achieve compliance if auto-remediation is not used.

Messages can include reasons for remediation, links to helpful URLs and helpdesk contact information. Aruba ClearPass OnGuard agents provide the same message and remediation capabilities for 802.1X, non-802.1X, and combined environments.



Detailed Mac OS X quarantine message.

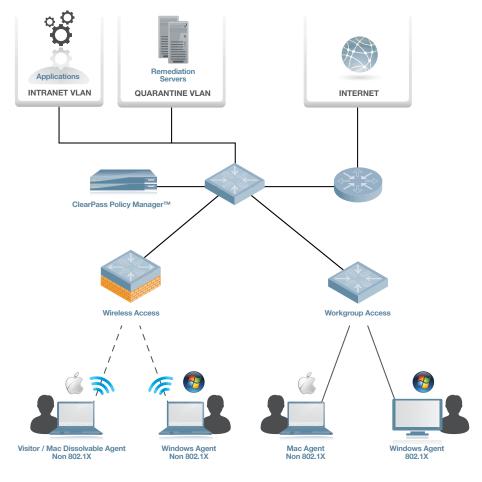


### **Extending NAP capabilities**

The Aruba ClearPass Policy Manager and OnGuard agents use Microsoft NAP and health-check capabilities to perform granular posture assessments with remediation. OnGuard also extends traditional NAC health-check capabilities to Mac and Linux platforms.

### IT-managed and BYOD endpoint compliance

OnGuard persistent and dissolvable agents can be used together in environments with endpoints owned by the organization, employees, or visitors to ensure that all devices are assessed and granted proper privileges prior to gaining network access.



# ClearPass OnGuard<sup>™</sup>

This diagram shows how persistent and dissolvable OnGuard agents are used.

### Complete endpoint visibility

To simplify troubleshooting, the sending of notification messages and compliance tracking, Aruba ClearPass Policy Manager provides a single, centralized view of user and device activity.

This makes it easy to automatically send warning notifications about potential copyright law violations on music-sharing sites when overuse of peer-to-peer applications is detected.

Endpoints can also be removed from the network via forced re-authentications associated with maintenance or compliance actions.

# **COMPREHENSIVE ENDPOINT ASSESSMENTS**

### Full endpoint protection

- Auto-remediation ensures that anti-virus and anti-spyware protection are up to date.
- Verifies firewall status with optional auto-remediation.
- Ensures that Windows Automatic Updates is running.
- Operating system fingerprinting verifies that approved images are installed.

#### Advanced posture assessments

- Runs anti-virus, anti-spyware, and firewall audits for product, engine and data versions, and checks when scans were last performed.
- Identifies approved peer-to-peer applications, registry keys, and system processes.
- Approves the use of USB storage devices.
- Checks for up-to-date Microsoft service packs and patches.
- Use with external patch management applications Altiris, BigFix, Creston, Lumension, Microsoft, Norman and Shavlik.
- Limits the use of client VM operating systems and applications.
- Detects the use of bridged interfaces within computers that may be used as Wi-Fi hotspots.

### Visibility and control

- Endpoint enforcement via static route assignment.
- Send notification messages to endpoints or groups of endpoints.
- Devices can be bounced from the network or denied access.

Doshboard       Monitoring & Reporting > Live Monitoring > OnGuard Activity         Monitoring & Reporting       OnGuard Activity Jan 18, 2012 11:12:54 PST         Live Monitoring       Activity Jan 18, 2012 11:12:54 PST         Accounting       Activity         Accounting       Iter:         Monitoring & Reporting       Iter:         Accounting       Iter:         Monitoring & Reporting       Iter:         Accounting       Iter:         Iter:       User A         Host MAC       Host IP         Host OS       Status         Date and Time       Authentication Records         Iter:       User A         Host MAC       Host IP         Host OS       Status       Date and Time         Aution Viewer       On O-17-545-23-89-       10.6.52.42       Microsoft         Jiack       01-75-45-23-89-       10.6.52.45       Microsoft       2012/01/17 11:24:09       View         Jiack       01-175-91-10.6.50.145       Windows 7       2012/01/17 07:34:00       View	APUBA networks	ClearPass Policy Manager admin (Super Administra								
Autoring & Reporting • Activity Jan 18, 2012 11:12:54 PST · Autor Refresh Bounce Client (using SNMP) Activity Accounting Acc	Dashboard 🛛 🔍	Monitoring & Repor	ting » Live Monitoring	» OnGuard Activ	ity					
<ul> <li>Live Monitoring</li> <li>Access Tracker</li> <li>Accounting</li> <li>Conclusion</li> <li>Bounce Client (Using SNMP)</li> <li>Broadcast Message</li> </ul> Filter: User A Host MAC Host IP Host OS Status Date and Time Authentication Records Windows 7 Collaboration Activity Reports Activity Reports Activity Reports Activity Reports Jiphn 00-10-09-01-59- 10.6.52.42 Windows 7 Olicity Origination Windows 7 Collaboration 2012/01/17 10:32:14 View View 3. john 00-1D-08-64-32- 10.6.50.145 Windows 7 Collaboration Collaboration View 4. karen 00-1D-08-64-32- 10.6.52.75 Windows 7 Collaboration Collaboration View 3. john 00-1D-08-64-32- 10.6.52.75 Windows 7 Collaboration Collaboration Collaboration View 4. Karen 00-14-06-21-44- 10.6.52.75 Windows 7 Collaboration Collaboratin <td>And .</td> <td colspan="5"></td> <td></td> <td></td>	And .									
Access Tracker       Accounting       Image: Contains       Concernence       Accounting       Acc										
Image: Solution       User A       Host MAC	- Access Tracker							oudeast message		
#     User A     Host MAC     Host IP     Host OS     Status     Date and Time     Authentication Records       System Monitor     System Monitor     I	-	Filter: User	<ul> <li>contains</li> </ul>		Go Cl	Go Clear Filter Show 10 records				
Image: System Monitor       1.       david       00-87-34-58-75- 99       10.6.52.42       Microsoft Windows 7       2012/01/17 10:32:14       View         Image: System Monitor       1.       david       00-17-34-58-75- 99       10.6.52.42       Windows 7       2012/01/17 10:32:14       View         Image: System Monitor       Image: System Moni		# 🔲 User 🛦	Host MAC	Host IP	Host OS	Status	Date and Time	Authentication Records		
Audit Viewer       2.       jack       90       10.5.2.55       Windows 7       2012/01/17 11:24:09       View         Paudit Viewer       3.       john       00 · 1D · 09 · D1 · 59 · 44       10.6.50.145       Microsoft Wicrosoft Wicrosoft Wicrosoft Wicrosoft Vista       2012/01/17 10:34:13       View         P Data Filters       4.       karen       00 · 1D · 09 · 01 · 69 · 432 · 45       10.6.50.145       Microsoft Vista       2012/01/17 10:34:13       View         5.       trent       00 · 14 · 06 · 21 · 44 · 92       10.6.52.190       Microsoft Vista       2012/01/17 10:34:13       View         6.       venkat       58 · 94 · 68 · 32 · 82 · 40       10.6.52.75       Microsoft Windows 7       2012/01/17 11:28:45       View	, , , , , , , , , , , , , , , , , , , ,	1. 🔲 david		10.6.52.42		•	2012/01/17 10:32:14	View		
Percent Viewer         3.         john         00-10-90-11-39- 44         10.6.50.145         Microsoft Windows 7         2012/01/17 07:34:00         View           P Data Filters         4.         karen         00-10-08-64-32- 45         10.6.50.145         Microsoft Vista 6.0         2012/01/17 07:34:10         View           5.         trent         00-14-06-21-44- 92         10.6.52.190         Microsoft Vista 6.0         2012/01/17 06:34:13         View           6.         venkat         58-94-68-32-82- 40         10.6.52.75         Microsoft Windows 7         2012/01/17 11:28:45         View	Activity Reports	2. 🔲 jjack		10.6.52.55		•	2012/01/17 11:24:09	View		
A     karen     45     10.6.50.18     6.0     2012/01/17     2013/31     View       5.     trent     00-14-06-21-44- 92     10.6.52.190     Microsoft Vista 6.0     2012/01/17     2013/01/17     View       6.     venkat     58-94-68-32-82- 40     10.6.52.75     Microsoft Windows 7     2012/01/17     11:28:45     View		3. 🔲 john		10.6.50.145		9	2012/01/17 07:34:00	View		
5.     Trent     92     10.6.52.190     6.0     2012/01/17 06:34:13     View       6.     venkat     58-94-68-32-82- 40     10.6.52.75     Microsoft Windows 7     9     2012/01/17 11:28:45     View	Data Filters	4. 🔲 karen		10.6.50.18		a 😑	2012/01/17 10:34:13	View		
6. Venkat 40 10.6.52.75 Windows 7 2012/01/17 11:28:45 View		5. 🔲 trent		10.6.52.190		a \varTheta	2012/01/17 06:34:13	View		
Showing 1-6 of 6 Send Message Bounce		6. 🔲 venkat		10.6.52.75		•	2012/01/17 11:28:45	View		
		Showing 1-	5 of 6					Send Message Bounce		
	Configuration O									
, Configuration ●	Administration O									

A centralized view of endpoint using OnGuard from the Aruba ClearPass Policy Manager.



### www.arubanetworks.com

1344 Crossman Avenue. Sunnyvale, CA 94089 1-866-55-ARUBA | Tel. +1 408.227.4500 | Fax. +1 408.227.4550 | info@arubanetworks.com

© 2012 Aruba Networks, Inc. Aruba Networks' trademarks include AirWave®, Aruba Networks®, Aruba Wireless Networks®, the registered Aruba the Mobile Edge Company logo, Aruba Mobility Management System®, Mobile Edge Architecture®, People Move. Networks Must Follow®, RFProtect®, and Green Island®. All rights reserved. All other trademarks are the property of their respective owners. DS\_OnGuard\_120604