



Tech Note:

ClearPass

OnGuard in a Cluster

Copyright

Copyright © 2013 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®, Green Island®. All rights reserved. All other trademarks are the property of their respective owners.

Open Source Code

Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other Open Source Licenses. The Open Source code used can be found at this site:

http://www.arubanetworks.com/open_source

<u>Date</u>	<u>Modified By</u>	<u>Comments</u>
September 25th	Danny Jump	Initial Version

Table of Contents

Overview	4
Introduction	4
So firstly what actually is OnGuard, and what can it do for me?	4
THE CLEARPASS ADVANTAGE	5
Persistent and dissolvable agents	5
Automatic remediation	5
IT-managed and BYOD endpoint compliance	5
What's the problem with a Cluster + OnGuard? (Persistent)	6
ZONES	7
OnGuard configuration download	10
Example of configuration downloaded by OnGuard client	10
How OnGuard determines its current Zone	12
How OnGuard selects a CPPM Server to send Web-Auth Request + Client Load Balancing	12
How to configure Client Load Balancing	13
How OnGuard shuffles list of servers:	13
How to restrict a CPPM server to accept/deny OnGuard requests	14
OK, why have Zones?	15
Statement of Health – Who's healthy?	16
Unified Client Nuances	17
Recommendations from the above	17
Appendix A – Global Agent Settings	18
Appendix B – List of OnGuard Modes (Persistent Agent)	20
Appendix C – List of OnGuard Modes (Dissolvable Agent)	21

Appendix D – Random Pieces of Information	23
Error Messages	23
Unattended Installation	23

Table of Figures

Figure 1 - OnGuard information flow	6
Figure 2 - Global Cluster of CPPM	7
Figure 3 - Adding CPPM Zones	8
Figure 4 - Defining SUBNETs in a zone	8
Figure 5 – Defining CPPM Servers to a ZONE - summary	9
Figure 6 - Defining CPPM Servers to a ZONE – detail	9
Figure 7 - Global Agent Settings - Client Load Balancing	13
Figure 8 - Restricting OnGuard access to CPPM.....	14
Figure 9 - Clearing CPPM networks restriction ACL's.....	14
Figure 10 - Example of IP Networks in the Zones	15
Figure 11 - Setting CoA delay	16
Figure 12 - OnGuard configuration for Persistent Agent.....	20
Figure 13 - OnGuard checks for Persistent Agent.....	20
Figure 14 - OnGuard WEB Portal configuration for Dissolvable agent only	21
Figure 15 - OnGuard Health & Auth options.....	21

Overview

The following guidance has been produced to aid field engineering, customers and partners to understand how the OnGuard product can be deployed specifically within a CPPM Cluster environment. A clustered CPPM means that multiple CPPM servers are logically joined together to process more load than what a single instance can process. These CPPM servers can be co-located within the same L2 broadcast network or separated by a L3 boundary. Restrictions do exist and are noted where relevant below.

Introduction

So firstly what actually is OnGuard, and what can it do for me?

ClearPass OnGuard™ agents perform advanced endpoint posture assessments, on leading computer operating systems to ensure compliance is met before devices are granted access.

Running on the ClearPass Policy Manager platform, the advanced network access control (NAC) and network access protection (NAP) framework in ClearPass OnGuard offers exceptional safeguards against vulnerabilities.

The following operating systems and versions are supported:

- *Microsoft – Support for Windows 8 and 7, Vista, XP, 2003 and 2008*
- *Apple – Support for Mac OS X 10.6 and above (64-bit only)*
- *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*

- **Note:** Auto-remediation only supported by the persistent agent.

	OnGuard Persistent Agent	OnGuard Dissolvable Agent	Microsoft's NAP Agent
Microsoft	X	X	X
Apple	X	X	
Linux		X	

Table 1 - OnGuard Supported OS Summary

THE CLEARPASS ADVANTAGE

In addition to anti-virus, anti-spyware and personal firewall audits performed by traditional NAC and NAP products, OnGuard agents can perform additional posture and health checks, to ensure a greater level of endpoint compliance.

Persistent and dissolvable agents

The difference between the two is that the persistent agent provides nonstop monitoring and automatic remediation and control. When running persistent OnGuard agents, ClearPass Policy Manager can centrally send system-wide notifications and alerts, and allow or deny network access. The persistent agent also supports auto and manual remediation.

Alternatively, the web-based dissolvable agent is ideal for personal, non IT-issued devices that connect via a captive portal and do not allow agents to be permanently installed. A one-time check at login ensures policy compliance. Devices not meeting compliance can be redirected to a captive portal for manual remediation. Once the browser page used during authentication is closed, the dissolvable agent is removed leaving no trace.

Automatic remediation

If unhealthy endpoints do 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. ClearPass persistent agents provide the same message and remediation capabilities for 802.1X, non-802.1X, and combined environments.

IT-managed and BYOD endpoint compliance

OnGuard persistent and dissolvable agents can be used together in environments where endpoints are owned by the organization, employees and visitors. This ensures that all devices are assessed and granted proper privileges before accessing the network.

What's the problem with a Cluster + OnGuard? (Persistent)

OnGuard is installed like a most typical client side applications, for windows it's a typical next, next, next, installation. Linux only supports the Java dissolvable agents that installs and runs once. The health status of a client is communicated between the OnGuard agent and CPPM. The outcome of the posture analysis (statement of health) is sent to CPPM via a HTTPS process under a WebAuth session and stored in the multi-master cache (MMC). MMC is a memory only table that holds specific state information. The MMC is replicated across all nodes in the zone to provide zone wide (NOT CLUSTER WIDE) visibility of client health. The MMC also contains other data but it is not relevant for discussion in this document.

The OnGuard typical data flow is shown below.

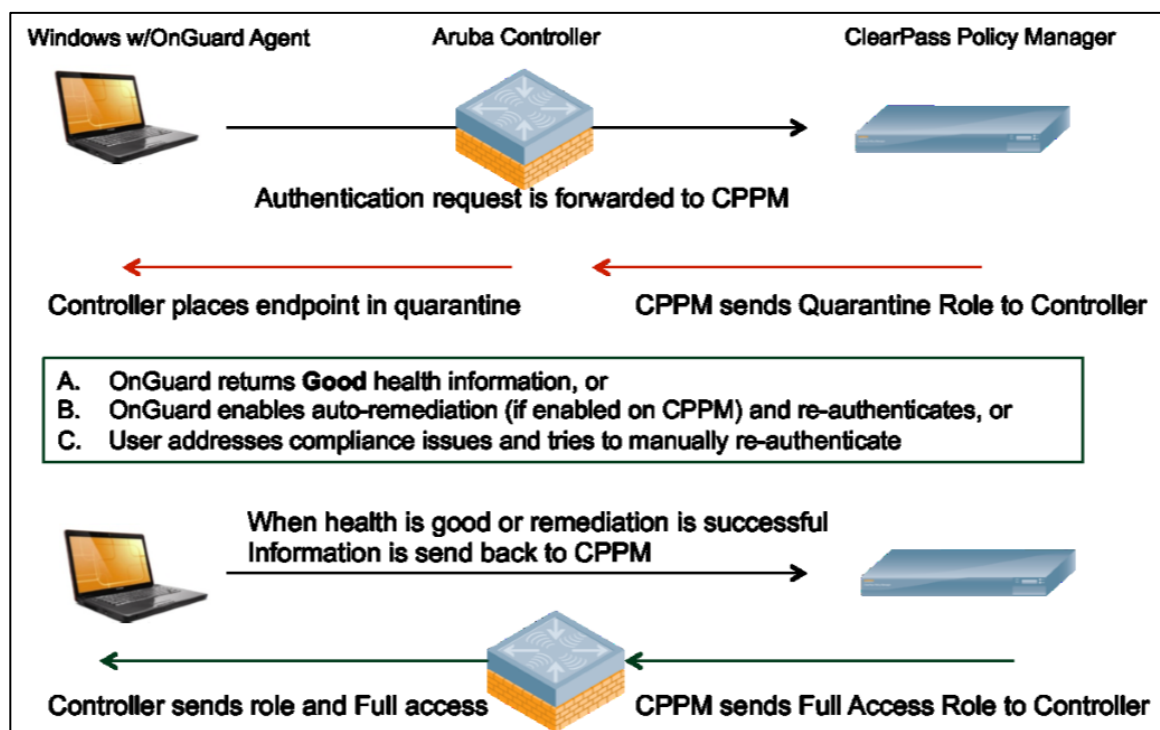


Figure 1 - OnGuard information flow

Taking the above and let us consider a multi-site or global deployment where we have seven CPPM servers spread globally across multiple regions and cities. The replication of the MMC is imperative; delays in this happening can cause problems. We attempt below to describe how we can configure OnGuard and show how to segment the CPPM cluster into Zones to assist in reducing MMC replication across the network.

Note: MMC is only ever replicated within a zone.

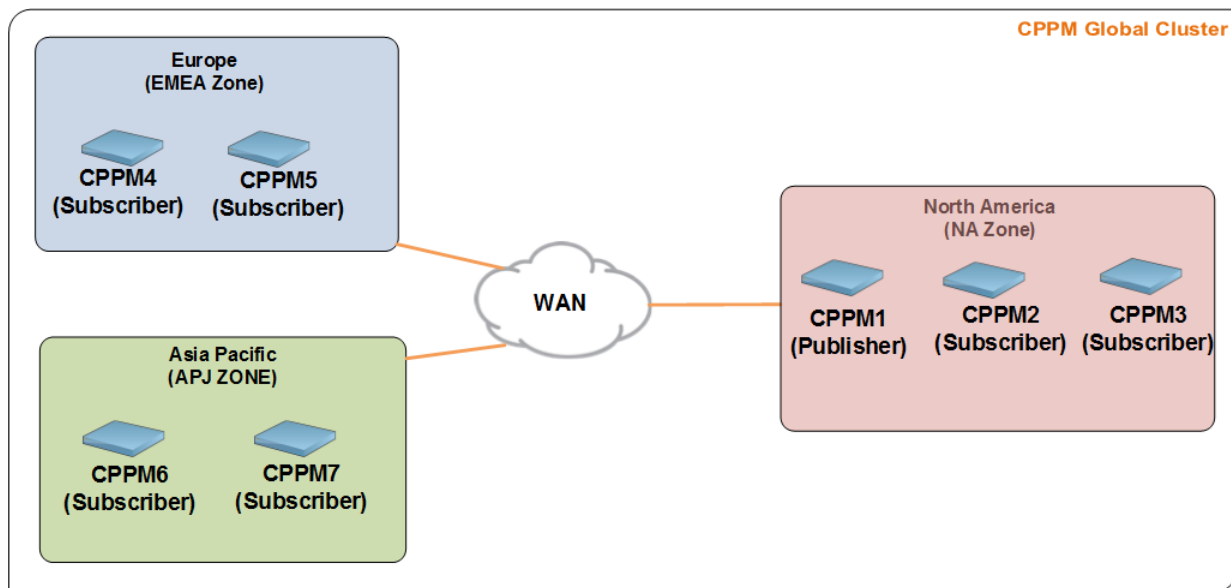


Figure 2 - Global Cluster of CPPM

ZONES

The above diagram shows we have three CPPM's located in North America, two in EMEA and two in APJ.

North America - CPPM1, CPPM2, CPPM3

EMEA – CPPM4, CPPM5

APJ – CPPM6, CPPM7

All boxes are clustered with CPPM1 being the Publisher. We have split the running servers into three zones, NA, EMEA and APJ.

North America – CPPM1, CPPM2, CPPM3

EMEA – CPPM4, CPPM5

APJ – CPPM6, CPPM7

By default when you create the above cluster of CPPM Servers (e: 1 Publisher and 6 Subscriber), the OnGuard agent downloaded will contain the IP addresses of all the CPPM nodes in the cluster, CPPM1 -> CPPM7 after installation and its downloaded its config.

Note: We assume the CPPM's have previously been clustered, its beyond the remit of this TechNote to cover the clustering of multiple CPPM servers, however it is covered in the CPPM User Guide found on our support site at <http://support.arubanetworks.com>

To create the zones use by CPPM, firstly you have to define the zones.... do this under **Administrator -> Server Manager -> Server Configuration -> Manage Policy Manager Zones**

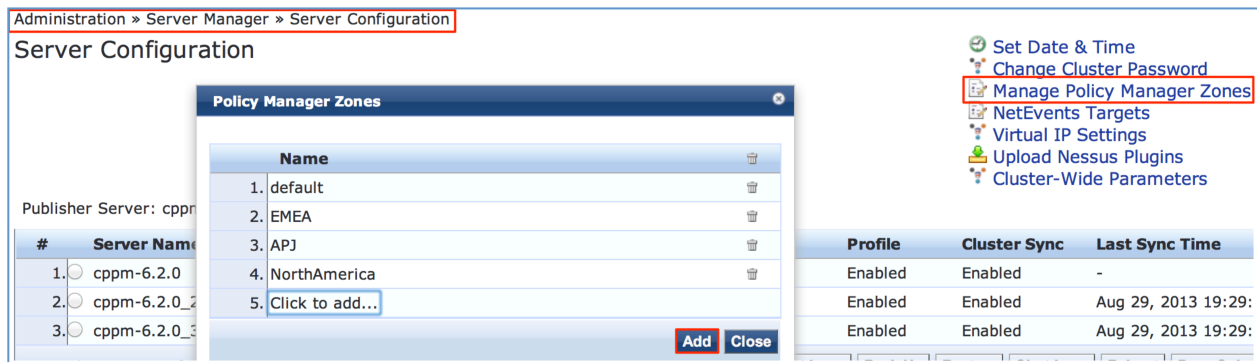


Figure 3 - Adding CPPM Zones

After Configuring the CPPM zones, you then need to define what local subnet's exist in each zone. See below for where to configure this.

Administrator -> Agents and Software Updates -> OnGuard Settings -> Policy Manager Zones

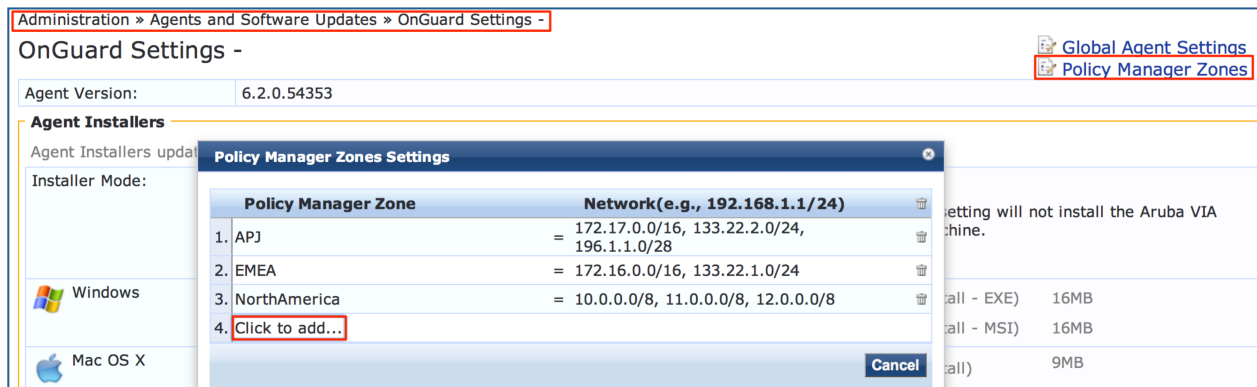


Figure 4 - Defining SUBNETs in a zone

As can be seen above, multiple subnets have been defined across our three zones, add your subnets as they exist in each location and separate them with a comma.

- **NorthAmerica** - 10.0.0.0/8, 11.0.0.0/8, 12.0.0.0/8
- **APJ** - 172.17.0.0/16, 133.22.2.0/24
- **EMEA** - 172.16.0.0/16, 133.22.1.0/24

The final step is to then 'lock' the individual CPPM's into their zone. See below for where to configure this.

Administrator -> Server Manager -> Server Configuration -> <choose each Server>

Administration » Server Manager » Server Configuration

Server Configuration

Publisher Server: cppm-6.2.0 [10.2.100.155]

#	Server Name ▲	Management Port	Data Port	Zone
1.	<input type="radio"/> cppm-6.2.0	10.2.100.155	-	NorthAmerica
2.	<input type="radio"/> cppm-6.2.0_2	10.2.100.156	-	NorthAmerica
3.	<input type="radio"/> cppm-6.2.0_3	10.2.100.157	-	NorthAmerica
4.	<input type="radio"/> cppm-6.2.0_4	172.16.104.158	-	EMEA

Figure 5 - Defining CPPM Servers to a ZONE - summary

Configure each server individually and define the zone it is located in. For our example we have only configured four out of the seven servers. Above you can see that the servers are configured accordingly with the 10.0.0.0 servers in NA and the 172.16.0.0 in EMEA.

Administration » Server Manager » Server Configuration - cppm-6.2.0

Server Configuration - cppm-6.2.0 (10.2.100.155)

System Services Control Service Parameters System Monitoring Network

Hostname:

Policy Manager Zone:

Enable Profile: ☒ Enable to allow this server to perform endpoint classification

Enable Insight: ☐ Enable Insight on this server

Management Port:

IP Address:

Subnet Mask:

Default Gateway:

Figure 6 - Defining CPPM Servers to a ZONE - detail

Under the **System** tab for each server under **Policy Manager Zone**, the drop down box allows you to select the zone per server.

OnGuard configuration download

When the OnGuard agent is downloaded from any of the CPPM servers, at installation time it creates a file named agent.conf. The agent.conf file contains a list of all CPPM Servers IP addresses for the cluster. Then OnGuard downloads its configuration from the first node in the list of IP addresses in agent.conf, typically this is the node it has just been downloaded from. The configuration is downloaded over HTTPS for security. This configuration exists only in memory and tells the OnGuard agent what it has to do and how it will function.....

Note: Every time OnGuard restarts it will download a fresh/updated configuration.

Example of configuration downloaded by OnGuard client

To examine the configuration download by OnGuard, use the following url format to obtain an example.... **http://<IP_address_of_CPPM>\agent\settings**

An example is below.....

```
{ "fieldSubmit": "Submit", "nodeIp": ["10.2.100.155"], "formType": "authApplet", "CacheCredentialsForDays": "15", "EnableClientLoadBalance": "true", "passwordLabel": "Password", "mode": "both", "upgradeAction": "DoNothing", "SupportEmailAddress": "danny@arubanetworks.com", "nodes": { "default": ["10.2.100.155"] }, "interfaces": "wired,wireless,vpn", "domain": "default", "usernameLabel": "Username", "agentVersion": "6.2.0.54353", "UseWindowsCredentials": "true" }
```

In the above returned settings you get an overview of how OnGuard will run. You can see at this time this is a single box cluster, "nodeIp": ["10.2.100.155"]. The Support Email Address "SupportEmailAddress": danny@arubanetworks.com, is clearly visible. Pay special attention to the "nodes" field, for future reference think of this as a list of "zones" and which CPPM servers are in each zone. The "domain", field shows the current zone that the OnGuard agent is using for its configuration, currently "default" in the above example.

Other configuration items exist that can effect how the agent runs, for example the list of interfaces we will manage, how long OnGuard will cache credentials etc.

Note: See [Appendix A](#) for a complete list of 'Global Agent Settings' that can be configured.

The configuration below reflects the changes as we add more CPPM servers.

```
{ "fieldSubmit": "Submit", "nodeIp": ["10.2.100.155", "10.2.100.156", "10.2.100.157", "172.16.104.158"], "formType": "authApplet", "CacheCredentialsForDays": "15", "EnableClientLoadBalance": "true", "passwordLabel": "Password", "mode": "both", "upgradeAction": "DoNothing", "SupportEmailAddress": "danny@arubanetworks.com", "nodes": { "EMEA": ["172.16.104.158"], "NorthAmerica": ["10.2.100.155", "10.2.100.156", "10.2.100.157"] }, "interfaces": "wired,wireless,vpn", "domain": "NorthAmerica", "usernameLabel": "Username", "agentVersion": "6.2.0.54353", "UseWindowsCredentials": "true" }
```

From the above configuration you can see multiple CPPM servers configured and assigned to their zones you now get clarity on the structure of the zones and their associated CPPM's servers. An explanation of some of this configuration follows is below.

- **"nodeIp":["10.2.100.155","10.2.100.156","10.2.100.157","172.16.104.158"]**
 - This is the entire list of CPPM in the cluster
- **"EMEA":["172.16.104.158"]**
 - This is the EMEA zone and its CPPM
- **"NorthAmerica":["10.2.100.155","10.2.100.156","10.2.100.157"]**
 - This is the NorthAmerica zone and its CPPM's
- **"domain":"NorthAmerica"**
 - This is the current zone the client pulled its configuration from

Note: Remember when a CPPM cluster is formed ALL configuration changes should be made on the CPPM server designated as the Publisher.

How OnGuard determines its current Zone

The OnGuard agent opens the Agent Settings URL by binding its http request to the client's network interface i.e. from this request the CPPM Server obtains the client's IP Address.

The CPPM Server uses OnGuard client's IP address to decide its Zone and sets the value of the domain in the agent settings response.

How OnGuard selects a CPPM Server to send Web-Auth Request + Client Load Balancing

Once the OnGuard agent reads the list of CPPM Servers from the Agent Settings, it checks the reachability of each CPPM Server and creates a list of servers that are reachable from each selected Network Interface.

OnGuard knows its current Zone from the '**domain**' parameter of Agent Settings and it also knows list of Zones Servers for that Zone from '**nodes**' parameter.

Note that it is not always the case that first server from list of CPPM Servers is also the first in the list of reachable servers.

Reason being it also depends on which server responds first to the reachability test.

Case 1: Zones not configured and Load Balancing is OFF

OnGuard selects first CPPM Server from the list of reachable servers.

Case 2: Zones not configured and Load Balancing is ON

OnGuard shuffles list of reachable servers and then selects first server from the shuffled list.

Case 3: Zones configured and Load Balancing is OFF

OnGuard creates list of CPPM Server by putting list of Zone Servers first and then Non-Zone Servers.

OnGuard selects first CPPM Server from the combined list.

Since Zones servers are at the beginning, one of the Zone servers will be selected.

Case 4: Zones configured and Load Balancing is ON

OnGuard shuffles list of Zone Servers.

OnGuard shuffles list of Non-Zone Servers.

OnGuard creates list of CPPM Servers by putting list of Zone Servers first and then Non-Zone Servers.

OnGuard selects first CPPM Server from the combined list.

Since Zones servers are at the beginning, one of the Zone servers will be selected.

In any of the above cases, if the first server is not reachable then OnGuard selects the next server from the list.

If Zones are configured, first it tries all the Servers from the 'home' Zone.

If none of these Zone Servers is reachable then it will try 'non-home' Zone servers.

How to configure Client Load Balancing

As discussed above one of the options that can be configured system wide is Client Load Balancing. This is configured under the **Global Agent Settings** as shown below.

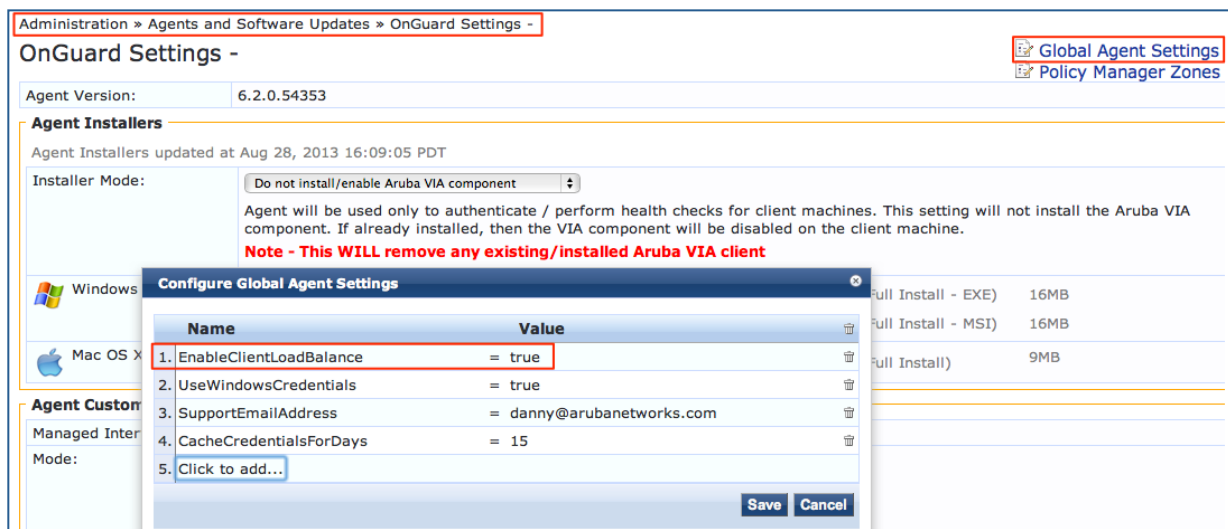


Figure 7 - Global Agent Settings - Client Load Balancing

Configuring the above setting will enable the OnGuard installed agent to load-balance AUTHENTICATIONS across CPPM as explained in [How OnGuard selects a CPPM Server to send Web-Auth Request + LoadBalancing](#).

Note: In essence this is HA for OnGuard. Whilst other service functions can utilize the VIP for communication OnGuard will use its ability to failover to another CPPM via the client-load-balancing option.

How OnGuard shuffles list of servers:

For shuffling list of servers, we use mt19937 as a random generator.

<http://www.cplusplus.com/reference/random/mt19937/>

How to restrict a CPPM server to accept/deny OnGuard requests

On a CPPM Server we can configure Application Access Control for OnGuard
Administration -> Server Manager -> Server Configuration -> Network -> Restrict Access

With this, we can **Allow** or **Deny** OnGuard access for specified Subnets as shown below.

Administration » Server Manager » Server Configuration - cppm-6.2.0

Server Configuration - cppm-6.2.0 (10.2.100.155)

System Services Control Service Parameters System Monitoring **Network**

GRE Tunnel

VLANS:

Application

Restrict Access

Resource Name: OnGuard

Access: Deny

Network: Allow access for all except - 1.0.0.0/8

Note: Enter hostname, IP address or subnet (CIDR) in the Network text box

Create Cancel

Create Tunnel

Create VLAN

Restrict Access

Figure 8 - Restricting OnGuard access to CPPM

If we deny the OnGuard application for a subnet, when the OnGuard Agent tries to check reachability to that Server, CPPM Server returns a HTTP Error 403 (Forbidden).

The OnGuard client treats a CPPM Servers returning HTTP Error 403 as unreachable and tries the next CPPM Server as defined in [How OnGuard selects a CPPM Server to send Web-Auth Request + Client Load Balancing](#).

Note: In CPPM 6.1 we added a CLI command to clear all the network restriction ACL's.

```
[appadmin@cppm-6.2.0]# system apps-access-reset
```

Policy Manager application access is restored

Figure 9 - Clearing CPPM networks restriction ACL's

OK, why have Zones?

In our scenario we have configured several zones. Zones allow us to segment the CPPM servers into smaller more manageable groups, manage OnGuard communications to a 'local' server and to allow better control and reduce the overhead of replication when CPPM's servers are separated by a WAN where bandwidth and/or latency could cause issues related to the replication of the on-box SQL databases and the MMC in-memory table that includes,

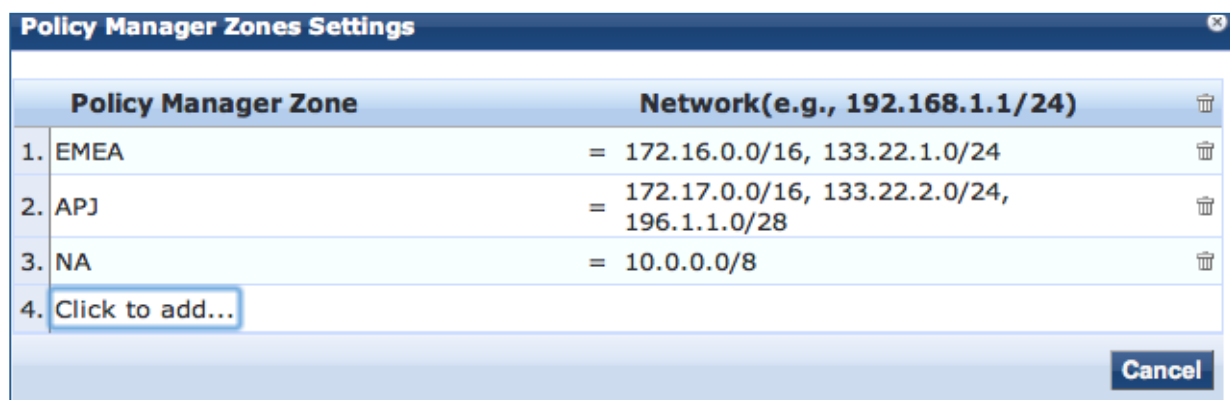
- Roles and Postures of connected entities

The connection status of all endpoints is written to a file in **config-DB**, this file is replicated across the entire cluster, it also contains all the rest of CPPM and guest configuration.

CPPM uses this runtime state information to make policy decisions across multiple transactions.

As mentioned previously, zones provide additional control to allow the network administrator to segment the larger CPPM cluster into mini-clusters (zones). This can be used to control the list of CPPM servers that the OnGuard agent initially tries to communicate with. In the event it cannot communicate with a device in its 'home' zone it will randomly contact one of the other servers as described previously.

Note: When configuring your zones carefully consider the IP Subnets that are in the zones.



Policy Manager Zones Settings	
Policy Manager Zone	Network(e.g., 192.168.1.1/24)
1. EMEA	= 172.16.0.0/16, 133.22.1.0/24
2. APJ	= 172.17.0.0/16, 133.22.2.0/24, 196.1.1.0/28
3. NA	= 10.0.0.0/8
4. Click to add...	

Cancel

Figure 10 - Example of IP Networks in the Zones

Imagine a scenario of a user working in Paris. This user would download the OnGuard agent from the local Paris (possibly CPPM4) server. The OnGuard configuration should then be loaded from the same server. The configuration tells the OnGuard client that there are actually seven CPPM's in the entire network, this would come from the **nodeIp** list, however CPPM4 and CPPM5 are its preferred CPPM's because in the **nodes** list the EMEA zone will be listed first. It would be pointless and possible unworkable for the user to randomly connect to a server in Asia or America when processing resource are available locally.

Statement of Health – Who’s healthy?

Within a cluster where multiple CPPM’s exist and OnGuard is configured to send health and provide authentication, challenges can exist. This typically relates to a clustered deployment where the CPPM servers are distributed over a WAN and with OnGuard we cannot be 100% certain which server it will communicate its Statement-of-Health (SoH)/posture to. Additionally when one CPPM node receives SoH, it updates its MMC that is asynchronously replicated across the cluster.

A NAS can be configured to behave in a deterministically way, sending its RADIUS Access-Request authorization messages to a specific CPPM node. However because of the undeterministic operation of OnGuard this is where the disconnect can occur. When authentication goes to one CPPM server and SoH goes to another, the delay in SoH replicating across all of the nodes in the zone can cause issues. For the user, initially the potential exists that they

In this scenario a user authenticates to CPPM1, this node then writes this data into the MMC and replicates this data across the zone. OnGuard on the client in the mean time is calculating the posture of the device, once the SoH processing is complete it will send this result to CPPM4, this SoH is received by the Web-based health-check service and processed by the node. That node then writes this data into the MMC, this is then replicated across the zone. At this time, the node that has received the SoH will issue a CoA to the NAS that processed the user’s authentication. We need to issue the CoA to get this client’s session re-connected, once they reconnect that authenticating node should have received the SoH via the MMC replication and place the user in the correct VLAN/Role.

One of the solutions that has been engineered to assist with the MMC replication is a delay processing before we send the CoA to the NAS. This is configured by default as 2 seconds but can be adjusted as required.

Administration » Server Manager » Server Configuration - cppm-6.2.0

Server Configuration - cppm-6.2.0 (10.2.100.155)

System Services Control **Service Parameters** System Monitoring Network

Select Service: Async network services

Parameter Name	Parameter Value	Default Value	Allowed Values
Post Auth			
Number of request processing threads	20 threads	20	20-100
Lazy handler polling frequency	5 minutes	5	3-10
Eager handler polling frequency	30 seconds	30	10-300
Command Control			
CoA Delay	2 seconds	2	0-15

Figure 11 - Setting CoA delay

Below we have discussed the Unified Clients main restriction.

Unified Client Nuances

When using the unified client for connectivity/authentication the OnGuard functionality can only work in a Health-only mode. This is because the connection between the client and CPPM is now Layer 3. Previously we had access to the mac address of the device, this allowed us to trigger changes to the NAS (e.g. CoA) using the mac address as the identifier.

Now the client is initially authenticating with IPSEC we do not see the mac address of the client, only the IP address. To overcome this restriction of using the unified client we made additional architecture changes to allow us to utilize the user-name to communicate role/vlan changes back to the NAS.

Recommendations from the above

Ensure that where possible via for large multi site/node deployments, authentication and SoH go to the same node. This can largely be controlled. On the NAS its easy to be deterministic about which CPPM you will send's auths to. We appreciate you may have a fall-through configuration but that's beyond the scope of this document at this time. By planning a deterministic node for your authentication, you can similarly via configuration and use of zones be fairly deterministic where you OnGuard SoH will go to, this then removes the potential issue of SoH being replicated with our MMC function, and certainly where SoH goes to an other node with in your zone, the replication of this data is reduced by reducing the RTT between system.

Appendix A – Global Agent Settings

Below is a list of the options you can add to the Global Agent Settings. These parameters effect how OnGuard will function when the client downloads it configuration from CPPM.

Parameter Name	Description	Supported OS/Agent
CacheCredentialsFor Days	This parameter is used by OnGuard agent if "Settings->Health Settings->Save supplied credentials..." is selected. If Save Credentials option is ON then OnGuard will use the credentials for specified number of days. This duration starts from last successful login so if a user a does not login for 15 days from that machine then on 16th day it will be asked to enter credentials. If user logs in everyday or once within 15 days, OnGuard will use saved credentials. This parameter ensures that saved credentials expire after configurable time and are not used forever.	Windows and Mac OS X - Persistent Agent
WiredAllowedSubnets	Subnets or IP Address to be allowed through Wired Interface. This parameter modifies client machine's routing table to allow only configured Subnets/IP Address through Wired Interface. It also removes default Gateway from routing table for Wired Interface.	Windows - Persistent Agent
WirelessAllowedSubnets	Same as 'WiredAllowedSubnets' but applied to Wireless Interface.	Windows - Persistent Agent
KeepAliveIntervalSeconds	OnGuard Agent periodically sends keep alive message to CPPM Server after connection is established with CPPM Server. CPPM server uses these messages to show status of client in "Monitoring->OnGuard Activity".	Windows and Mac OS X - Both Persistent and Dissolvable Agent
EnableClientLoadBalance	Refer 4th FAQ for detailed description of this parameter - https://arubapedia.arubanetworks.com/arubapedia/index.php/ClearPass_OnGuard	Windows and Mac OS X - Persistent Agent
AllowRemoteDesktopSession	This parameter is used to specify if OnGuard should be allowed to run in RDP Session or not. If this option is OFF (do not allow Remote Desktop Session) and OnGuard is launched in RDP Session then it quits itself.	Windows - Persistent Agent
HideLogoutButton	This option is used to Hide Logout button from OnGuard Agent User Interface. Some customers reported that after clicking Logout button in 'health only' mode, user remains in full access VLAN but its health is not monitored anymore as OnGuard is not connected. This option was added to solve that issue.	Windows and Mac OS X - Persistent Agent
InstallVPNComponent	This parameter is used to specify whether VPN Component should be installed/enabled or not. Some customers may not want to use VPN functionality and others may be interested only in OnGuard functionality so this option lets them decide if they want both or any one of them.	Windows and Mac OS X - Persistent Agent
UseWindowsCredentials	This parameter is to specify if OnGuard should use current user's Windows Credential or not.	Windows - Persistent Agent

SupportEmailAddress	When user clicks on Send Logs button on OnGuard user interface, it composes a new email and attaches logs to it. The email address configured for this parameter is used in the "To" field of that email. If this parameter is not configured then it will show empty "To" field which some customers reported as issue.	Windows and Mac OS X - Persistent Agent
---------------------	---	---

|

Appendix B – List of OnGuard Modes (Persistent Agent)

Below is a list of the available modes for the persistent agent that can be configured for OnGuard under CPPM 6.2.0.. These are configured under the **OnGuard Settings** configuration page as shown below.

Administration » Agents and Software Updates » OnGuard Settings -

OnGuard Settings -

Agent Version: 6.3.0.54751

Agent Installers

Agent Installers updated at Aug 20, 2013 18:05:15 PDT

Installer Mode: Do not install/enable Aruba VIA component

Agent will be used only to authenticate / perform health checks for client machines. This setting will not install the... will be disabled on the client machine.

Note - This WILL remove any existing/installed Aruba VIA client

OS	Installer URL	Installation Type	Size
Windows	http://10.2.100.21/agent/installer/windows/ClearPassOnGuardInstall.exe	(Full Install - EXE)	16MB
	http://10.2.100.21/agent/installer/windows/ClearPassOnGuardInstall.msi	(Full Install - MSI)	16MB
Mac OS X	http://10.2.100.21/agent/installer/mac/ClearPassOnGuardInstall.dmg	(Full Install)	9MB

Agent Customization

Managed Interfaces: ☒ Wired ☒ Wireless ☒ VPN ☐ Other

Mode: Authenticate with health checks

Username Text:

Password Text:

Client Certificate Check: ☐ Enable to use a certificate from User keystore during authentication

Figure 12 - OnGuard configuration for Persistent Agent

Authenticate - no health checks

Check health - no authentication

✓ Authenticate with health checks

Figure 13 - OnGuard checks for Persistent Agent

Authenticate - no health checks.

Check health - no authentication. OnGuard does not collect username/password.

Authenticate with health checks. OnGuard collects username/password and also performs health checks on the endpoint.

Note: Persistent agent supports both OnGuard and VPN+OnGuard functionality.

Appendix C – List of OnGuard Modes (Dissolvable Agent)

Below is a list of the available modes (in figure 12) for the dissolvable agent that can be configured for OnGuard under CPPM 6.2.0. These are configured under the **OnGuard Portal** configuration page as shown below.

Figure 14 - OnGuard WEB Portal configuration for Dissolvable agent only

Authenticate – no health checks (HTML form)
Authenticate – no health checks (Java applet)
✓ Check health – no authentication (Java applet)
Authenticate with health checks (Java applet)
Authenticate with optional health checks (Dual mode)
No Authentication and no health checks (HTML form)

Figure 15 - OnGuard Health & Auth options

Authenticate - no health validation (HTML Form) - Policy Manager presents a simple HTML form with the username and password. Health credentials are not collected from the client.

Authenticate - no health validation (Java Applet) - Policy Manager presents an applet based form with the username and password. Health credentials are not collected from the client. Note that, the Java applet collects the MAC address of all interfaces on the client. In the case of a simple HTML form, Policy Manager would have to perform the extra step of DHCP snooping to collect the MAC address of the client.

Check Health - no authentication (Java applet) - Username/password are not collected. Health is evaluated via a Java applet.

Authenticate with health checks (Java Applet) - Policy Manager prompts the user for username and password, and also collects client health credentials by means of a Java applet downloaded to the page.

Authenticate with optional health checks (Dual mode) - User is presented with a simple HTML form. User can choose to load the Java applet by clicking on a link on this page; the java applet (dissolvable agent) also collects health information.

No Authentication and no health checks (HTML form) - User is presented with a simple HTML form for the username, which is hidden

Appendix D – Random Pieces of Information

Port 6658 is used for OnGuard keep alive exchange (roughly once per minute: but you can change that on CPPM), this heart-beat process consumes approximately 200 bytes.

HTTPS communication is used to send the posture information to CPPM and response.

Error Messages

In respect of error messages between OnGuard and CPPM this is limited specifically to the communication between the client and the WEBAuth that is used by OnGuard to send health. Only two messages can really exist here.....

201 - Authentication failure -> User not found

202 - Authentication failure -> Password mismatch

Unattended Installation

If there is a requirement to perform a silent installation of OnGuard you can create a **bat** file and have it executed by something like MSFT SCCM.:

net stop "clearpass agent controller"

taskkill /f /im clearpassonguard.exe

msiexec /x ClearPassOnGuardInstall.msi /qn

msiexec /i ClearPassOnGuardInstall.msi /qn

Note: /qn flag sets the user interaction to **q=quiet & n=no user interaction**. These flags are specific to using the **.msi**. However if you download from CPPM the **.exe** installer you can use the /S (uppercase) switch to perform a silent installation.