

---

TECHNICAL NOTE

# CLEARPASS ONGUARD

## CONFIGURATION GUIDE



### REVISION HISTORY

Revised By	Date	Changes
Dennis Boas	July 2015	Version 1 – initial release

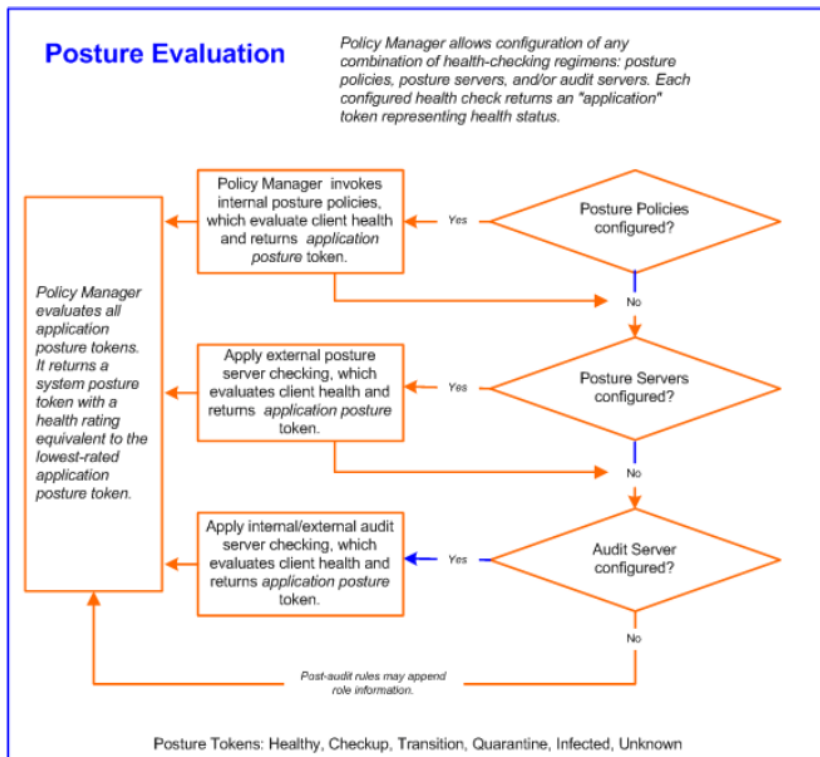
# TABLE OF CONTENTS

<b>CLEARPASS ONGUARD .....</b>	<b>1</b>
<b>INTRODUCTION .....</b>	<b>3</b>
<b>CONFIGURATION WORKFLOW.....</b>	<b>4</b>
<b>CONFIGURE POSTURE POLICIES .....</b>	<b>4</b>
RESTRICTING POLICIES .....	5
WINDOWS OS .....	6
<i>NAP AGENT</i> .....	6
ONGUARD AGENT .....	8
<i>Posture Policy Checks</i> .....	8
MAC OS X .....	12
<b>CUSTOMIZE AGENT .....</b>	<b>15</b>
INSTALLER MODE .....	15
AGENT CUSTOMIZATION .....	16
<i>Managed Interfaces</i> .....	16
<i>Agent Mode options</i> .....	16
ONGUARD GLOBAL AGENT SETTINGS .....	17
CONFIGURE POLICY MANAGER ZONES:.....	19
AGENT FLOW CHART.....	20
<b>CONFIGURE CLEARPASS SERVICES FOR ONGUARD.....</b>	<b>21</b>
SERVICE CONFIGURATION .....	22
TEMPLATE CREATED SERVICES, POLICIES AND PROFILES .....	24
<i>Posture Policy</i> .....	25
<i>Enforcement policies</i> .....	25
<i>Web Login Page</i> .....	31
<b>MONITORING ONGUARD .....</b>	<b>32</b>
ONGUARD AGENT .....	32
ONGUARD ACTIVITY .....	33
ACCESS TRACKER.....	34
ENDPOINT DATABASE.....	36
<b>ADDITIONAL RESOURCES .....</b>	<b>36</b>

## Introduction

This technical note is intended to help field engineers, customers, and partners configure and deploy a basic OnGuard solution. ClearPass OnGuard agents perform advanced endpoint posture assessments to ensure that endpoints meet enterprise security requirements before they are allowed access to the network.

Policy Manager provides several methods for assessing the health posture of clients requesting access; OnGuard Agents, NAP Agents and NESSUS or NMAP Scans. All of these methods return Posture Tokens (E.g., Healthy, Quarantine) that Policy Manager uses for input into Enforcement Policies. One or more of these posture methods can be associated with a Service.



**Note:** This Tech Note will only cover the OnGuard and NAP Agents.

## Configuration Workflow

There are six steps required to configure OnGuard

- Configure Posture Policies
- Configure OnGuard Agent Customization
- Configure Global Agent Settings
- Configure OnGuard Policy Manger Zone mapping
- Configure Policy Manager Service
- Configure ClearPass Web Authorization Page

The first step is to decide which end systems the OnGuard agents will be installed on, what tests will be run and what results will be required to return a Healthy Token.

## Configure Posture Policies

Posture policies can be associated with ClearPass services to verify the security posture of end systems prior to granting network access. The policy defines the end system operating system and the type of agent to deploy. It also tells the agent which tests to run and defines the rules that determine what is required to return a Healthy Token to the ClearPass service. For Windows end systems the Microsoft NAP agent and the OnGuard agent are both available. For Linux and Mac OS X only the OnGuard agent is available.

To configure a new policy navigate to the **Policy** tab on the **Configuration > Posture > Posture Policies > Add** page

The screenshot shows the ClearPass Policy Manager web interface. The top navigation bar includes the Aruba Networks logo, the title 'ClearPass Policy Manager', and links for 'Support', 'Help', and 'Logout'. The user is logged in as 'admin (Super Administrator)'. The left sidebar shows a navigation menu with 'Configuration' selected. The main content area shows the 'Posture Policies' page with tabs for 'Policy', 'Posture Plugins', 'Rules', and 'Summary'. The 'Policy' tab is active, displaying a form for adding a new policy. The form fields are: 'Policy Name' (Lab Mac), 'Description' (Lab OSX computers), 'Posture Agent' (OnGuard Agent (Persistent or Dissolvable) selected), 'Host Operating System' (Mac OS X selected), and 'Restrict by Roles' (empty). There are 'Remove' and 'Add' buttons for the roles section.

## Restricting Policies

The Restrict by Roles section allows the administrator to apply the posture policy only to end systems that authenticate with selected roles. Typically users with access to sensitive information would authenticate with roles associated with more restrictive posture policies. For example users with access to research data might have a posture policy that does not permit the mounting of USB Storage devices. Or users with access to employee or customer personal or health data might have a policy that requires full disk encryption.

### Posture Policies

Policy	Posture Plugins	Rules	Summary
Policy Name:	Lab Mac		
Description:	Posture checks for Macs		
Posture Agent:	<input type="radio"/> NAP Agent <input checked="" type="radio"/> OnGuard Agent (Persistent or Dissolvable)		
Host Operating System:	<input checked="" type="radio"/> Windows <input type="radio"/> Linux <input type="radio"/> Mac OS X		
Restrict by Roles:	<div> <input type="text" value="[Contractor]"/> <input type="button" value="Remove"/> </div> <div>           Select or type role names           <input type="button" value="Add"/> </div> <div> <ul style="list-style-type: none"> <li>[Machine Authenticated]</li> <li>[User Authenticated]</li> <li>[Guest]</li> <li>[TACACS Read-only Admin]</li> <li>[TACACS API Admin]</li> <li>[TACACS Help Desk]</li> <li>[TACACS Receptionist]</li> <li>[TACACS Network Admin]</li> <li>[TACACS Super Admin]</li> <li>[Contractor]</li> <li>[Other]</li> <li>[Employee]</li> <li>[Device Registration]</li> <li>[MAC Caching]</li> <li>[Onboard Android]</li> <li>[Onboard Windows]</li> <li>[Onboard Mac OS X]</li> <li>[Onboard iOS]</li> <li>[BYOD Operator]</li> <li>[AirGroup v1]</li> <li>[AirGroup v2]</li> <li>[Aruba TACACS root Admin]</li> <li>[Aruba TACACS read-only Admin]</li> <li>[Onboard Chromebook]</li> <li>[Onboard Linux]</li> </ul> </div>		

## Windows OS

The Posture agents supported for Windows operating systems are the Microsoft NAP Agent and the ClearPass OnGuard agent.

## NAP AGENT

Configuration » Posture » Posture Policies » Add

### Posture Policies

Policy	Posture Plugins	Rules	Summary
Policy Name:	<input type="text"/>		
Description:	<input type="text"/>		
Posture Agent:	<input checked="" type="radio"/> NAP Agent <input type="radio"/> OnGuard Agent (Persistent or Dissolvable)		
Host Operating System:	<input checked="" type="radio"/> Windows <input type="radio"/> Linux <input type="radio"/> Mac OS X		
Restrict by Roles:	<div> <input type="text"/> <input type="button" value="Remove"/> </div> <div>           Select or type role names           <input type="text"/> <input type="button" value="Add"/> </div>		

The Windows NAP agent includes the System Health Validator and Security Health Validator. Both have limited predefined checklists to enable the tests. The NAP agents send the health information to ClearPass along with the 802.1X authentication information.

Note: Use of the NAP agent is discouraged. NAP was marked deprecated in Server 2012 R2, and NAP is not supported in the Technology Preview of Windows 10 and Windows Server 2016.

To configure the NAP agent Select the Posture Plugin Tab.

Configuration » Posture » Posture Policies » Add

### Posture Policies

Policy Posture Plugins Rules Summary

Select one/more plugins:

Plugin Name	Plugin Configuration	Status
<input type="checkbox"/> Windows System Health Validator	<a href="#">Configure</a> <a href="#">View</a>	-
<input type="checkbox"/> Windows Security Health Validator	<a href="#">Configure</a> <a href="#">View</a>	-

The Windows System Health Validator Plugin allows you to restrict access based on the Windows OS version and Service Pack level of the end system.

#### Windows System Health Validator

Client computers can connect to your network, subject to the following checks -

- ☒ **Windows 8**  
Windows 8 clients are allowed  
☐ Restrict clients which have Service Pack less than
- ☒ **Windows 7**  
Windows 7 clients are allowed  
☐ Restrict clients which have Service Pack less than
- ☒ **Windows Vista**  
Windows Vista clients are allowed  
☐ Restrict clients which have Service Pack less than
- ☒ **Windows XP**  
Windows XP clients are allowed  
☐ Restrict clients which have Service Pack less than
- ☒ **Windows Server 2008**  
Windows Server 2008 clients are allowed  
☐ Restrict clients which have Service Pack less than
- ☒ **Windows Server 2008 R2**  
Windows Server 2008 R2 clients are allowed  
☐ Restrict clients which have Service Pack less than

[Reset](#) [Save](#) [Cancel](#)

The Windows Security Health Validator Plugin verifies that a firewall is enabled, security applications are installed and security updates are current. Unlike the OnGuard Agent the NAP agent does not allow you to restrict access based on specific Firewall, Virus protection and Spyware protection products.

**Windows Security Health Validator**

**Windows 8** ☒ Enable checks for Windows 8  
Client computers can connect to your network, subject to the following checks -

☒ **Firewall**  
Client must have firewall enabled on the client

☒ **Virus Protection**  
Client must have an antivirus application. ☒ Check if Antivirus is up to date

☒ **Spyware Protection**  
Client must have an antispware application. ☒ Check if Antispyware is up to date

☒ **Automatic Updates**  
Check if Automatic Updates is enabled on the client

☒ **Security Updates**  
Client must have all available security updates installed:   
Client must have checked for new security updates within last:  hours  
Additional sources required in your deployment:  
☐ Window Server Update Services  
☐ Windows Update

**Configuration**

**Windows 7**

**Windows Vista**

**Windows XP**

**Reset** **Save** **Cancel**

## OnGuard Agent

The OnGuard Agent enables more extensive health checks than those available in the NAP Agent. Both persistent and dissolvable agents are available for Windows, Mac OS X and Linux operating systems. The persistent agent is installed on the end system and runs in the background. It requires network connectivity and regularly reports health information to a ClearPass Webauth posture check service. The dissolvable agent does not permanently install anything on the end system. The user is redirected to the ClearPass agent page and the agent is run on demand in the Web Browser. Both the persistent and dissolvable agents cache the health results in the Endpoint Database and the latest health posture token can be used by ClearPass services. The persistent and dissolvable agents perform the same tests but auto remediation is only available with the persistent agent.

## Posture Policy Checks

**Services** – specify services to be explicitly running or stopped.

**Processes** - specify processes to be explicitly present or absent on the system.

**Registry Keys** - specify registry keys to be explicitly present or absent. **(Windows only)**

**Antivirus** - specify that an Antivirus application must be on and allows drill-down to choose a specific Antivirus application.

**AntiSpyware** - specify that an AntiSpyware application must be on and allows drill-down to choose a specific AntiSpyware application.



**Firewall** - specify that a Firewall application must be on and allows drill-down to choose a specific Firewall application.

**Peer To Peer** - specify specific peer-to-peer applications or networks to be explicitly stopped. When you select a peer-to-peer network, all applications that make use of that network are stopped.

**Patch Management** - specify that a patch management application must be on and allows drill-down to specify information about the patch management application.

**Windows Hotfixes** - check if specific Windows hotfixes are installed on the endpoint.  
(Windows only)

**USB Devices** - provides configuration to control USB devices attached to an endpoint.

**Virtual Machines** - provides configuration to control Virtual Machines installed on the end system.

**Network Connections** - provides configuration to control network connections based on connection type.

**Disk Encryption** - tests for any encryption product or a specific encryption product. Root Drive, all drives or a specific location can be specified.

**Installed Application** - specifies allowed mandatory, allowed optional, and not allowed applications. Can be set for monitor mode.

**File Check** - tests for the presence or absence of specific file groups. Success can be set to all files present or any file present.

**Note:** The Linux Universal System Health Validator only supports Services and AntiVirus checks

To configure the OnGuard Agent select **Configuration » Posture » Posture Policies » Add**

Configuration » Posture » Posture Policies » Add

### Posture Policies

Policy	Posture Plugins	Rules	Summary
Policy Name:	<input type="text"/>		
Description:	<input type="text"/>		
Posture Agent:	<input type="radio"/> NAP Agent <input checked="" type="radio"/> OnGuard Agent (Persistent or Dissolvable)		
Host Operating System:	<input checked="" type="radio"/> Windows <input type="radio"/> Linux <input type="radio"/> Mac OS X		
Restrict by Roles:	<div> <input type="text"/> <input type="button" value="Remove"/> </div> <div>           Select or type role names           <input type="text"/> <input type="button" value="Add"/> </div>		

The ClearPass Windows Universal System Health Validator leverages the Microsoft NAP Agent and Microsoft's API and performs more advanced health checks than the Microsoft-provided NAP Agent

To configure the ClearPass Windows Universal System Health Validator Select **Configure** under the Plugin Configuration heading

Configuration » Posture » Posture Policies » Add

### Posture Policies

Policy Posture Plugins Rules Summary

Select one/more plugins:

Plugin Name	Plugin Configuration	Status
<input checked="" type="checkbox"/> ClearPass Windows Universal System Health Validator	<a href="#">Configure</a> <a href="#">View</a>	Not Configured
<input type="checkbox"/> Windows System Health Validator	<a href="#">Configure</a> <a href="#">View</a>	-
<input type="checkbox"/> Windows Security Health Validator	<a href="#">Configure</a> <a href="#">View</a>	-

Then choose the Windows operating system you want to enable checks for. In this example; Select Widows 8 then check the Enable checks for Windows 8 checkbox. Next select Firewall on the left hand window. If the desired behavior is to simply test to see if any firewall is running then uncheck the (Uncheck to allow any product) checkbox. To specify the required firewall check the (Uncheck to allow any product) checkbox and click the add button

ClearPass Windows Universal System Health Validator

Windows Server 2003 ☒ Enable checks for Windows 8

Windows XP ☒ A firewall application is on

Windows Vista ☒ Remediation checks ☒ Auto Remediation ☒ User Notification

Windows 7 ☒ Product-specific checks ☒ (Uncheck to allow any product)

Windows Server 2008

Windows 8

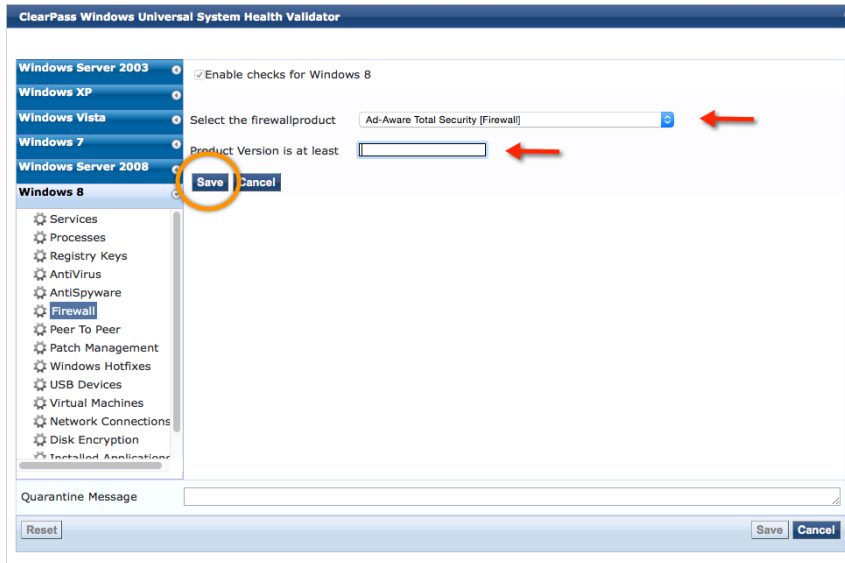
Services  
Processes  
Registry Keys  
AntiVirus  
AntiSpyware  
**Firewall**  
Peer To Peer  
Patch Management  
Windows Hotfixes  
USB Devices  
Virtual Machines  
Network Connections  
Disk Encryption  
Trusted Applications

Firewall Product Name Product Version

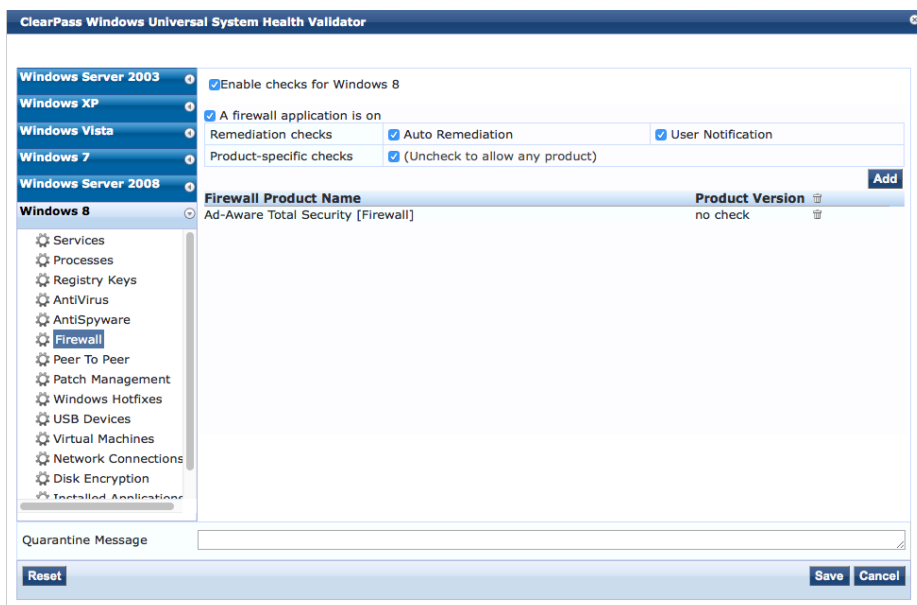
Quarantine Message

Reset Save Cancel

Next select the firewall product from the pull-down window and optionally specify the minimum version



After selecting the Firewall product from the pull down menu set the remediation behavior, Auto Remediation will turn on the firewall if it is not running, User notification will notify the user to turn it on. After the configuration is complete click **Save**.



After all of the Posture Plugins have been configured click on the Rules tab and add the rules that define which Posture Token will be sent to ClearPass. Rules can apply to all configured Plugins or be specific to one Plugin

Plugin rules can be

And Tokens can be

In this example all checks from all plugins must pass before a Healthy Token is sent to ClearPass; if any check fails a Quarantine Token will be sent to ClearPass.

Policy	Posture Plugins	Rules	Summary
Rules Evaluation Algorithm: First applicable			
Conditions			Posture Token
1.	Passes all SHV checks - ClearPass Windows Universal System Health Validator Windows System Health Validator Windows Security Health Validator		HEALTHY
2.	Fails one or more SHV checks - ClearPass Windows Universal System Health Validator Windows System Health Validator Windows Security Health Validator		QUARANTINE
<a href="#">Add Rule</a> <a href="#">Move Up</a> <a href="#">Move Down</a>			<a href="#">Edit Rule</a> <a href="#">Remove Rule</a>

## Mac OS X

In the following example we have configured three Policies for Mac OS X.

Filter:  contains  [Go](#) [Clear Filter](#) Show 10 records

#	<input type="checkbox"/> Name ▲	Description
1.	<input type="checkbox"/> basic mac	firewall test
2.	<input type="checkbox"/> Mac General	
3.	<input type="checkbox"/> Mac Lab access	

Showing 1-3 of 3 [Copy](#) [Export](#) [Delete](#)

The basic mac policy only tests for supported firewall and applies to all roles

The Mac General policy applies to users authenticating with the Employee Role and requires a supported Antivirus application, a supported AntiSpyware application and a supported Firewall application.

The Mac Lab access applies to users with access to sensitive research information. It is much more restrictive then the other policies

## Mac Lab Access Policy

This Posture policy applies only to end systems that authenticate with the Lab Access role. End systems that pass all SHV tests receive a Healthy Posture Token, if they fail a single test they receive a Quarantine Posture Token

This policy will require the latest version of ESET Cybersecurity Pro Antivirus software. Since Auto Remediaton is checked if the applciacation is stopped the agent will restart it.

The policy will also specify auto remediation for MacKeeper Antispyware and ESET Cybersecurity Firewall.

## Posture Policies - Mac Lab access

**ClearPass Mac OS X Universal System Health Validator**

**Antispyware**

**Mac OS X:**

Enable Auto Remediation: true

Enable User Notification: true

Enable Display Update URL: true

List of selected antispyware applications

Product	Product Version	Engine Version	Data File Version	Data File Update	Last Scan	Rtp Status Check
1. MacKeeper	is latest	is latest	is latest	1 Day(s) old	no check	on

**Firewall**

**Mac OS X:**

Enable Auto Remediation: true

Enable User Notification: true

List of selected firewall applications

Product	Product Version
1. ESET Cybersecurity Pro	no check

Since this policy applies to users with access to critical information it will also enforce checks on mounting USB devices and hosting virtual machines. Auto Remediation will eject any mounted USB devices and stop any virtual machines running on the host.

**ClearPass Mac OS X Universal System Health Validator**

**USB Devices**

**Mac OS X:**

Enable Auto Remediation: true

Enable User Notification: true

USB Mass Storage Remediation Action: Eject USB Devices

**Virtual Machines**

**Mac OS X:**

Enable Auto Remediation: true

Enable User Notification: true

Allow Host Virtual Machine: true

Allow Guest Virtual Machines: false

Guest Virtual Machine Remediation Action: Stop Guest VMs

Information on this machine is considered classified so then policy will require full disk encryption. Auto remediation is not available for Encryption checks

**Disk Encryption**

**Mac OS X:**

Enable Auto Remediation: false

Enable User Notification: true

List of selected disk encryption applications

Product	Product Version	Locations to Check
1. FileVault	no check	AllDrives

## Customize Agent

The OnGuard settings page provides links to the Persistent and Dissolvable agent files, installer mode selection, and the agent customization parameters.

aruba NETWORKS ClearPass Policy Manager Support | Help | Logout  
admin (Super Administrator)

Administration » Agents and Software Updates » OnGuard Settings -

OnGuard Settings - Global Agent Settings Policy Manager Zones

Agent Version: 6.5.1.72346

**Agent Installers**  
Agent Installers updated at Jun 23, 2015 04:29:47 EDT

Installer Mode:

Agent will be used only to authenticate/perform health checks for client machines. This setting will not install the Aruba VIA component. If already installed, then the VIA component will be disabled on the client machine.  
**Note - This WILL remove any existing/installed Aruba VIA client**

OS	Installer	Format	Size
Windows	<a href="http://192.168.1.204/agent/installer/windows/ClearPassOnGuardInstall.exe">http://192.168.1.204/agent/installer/windows/ClearPassOnGuardInstall.exe</a>	(Full Install - EXE)	17MB
Mac OS X	<a href="http://192.168.1.204/agent/installer/windows/ClearPassOnGuardInstall.msi">http://192.168.1.204/agent/installer/windows/ClearPassOnGuardInstall.msi</a>	(Full Install - MSI)	17MB
Mac OS X	<a href="http://192.168.1.204/agent/installer/mac/ClearPassOnGuardInstall.dmg">http://192.168.1.204/agent/installer/mac/ClearPassOnGuardInstall.dmg</a>	(Full Install)	12MB
Ubuntu	<a href="http://192.168.1.204/agent/installer/ubuntu/ClearPassOnGuardInstall.tar.gz">http://192.168.1.204/agent/installer/ubuntu/ClearPassOnGuardInstall.tar.gz</a>	(Full Install)	18MB

**Native Dissolvable Agent Apps**

OS	App	Size
Windows	<a href="http://192.168.1.204/agent/webagent/windows/OnGuard_Windows_Health_Checker.exe">http://192.168.1.204/agent/webagent/windows/OnGuard_Windows_Health_Checker.exe</a>	11MB
Mac OS X	<a href="http://192.168.1.204/agent/webagent/mac/OnGuard_Mac_Health_Checker.dmg">http://192.168.1.204/agent/webagent/mac/OnGuard_Mac_Health_Checker.dmg</a>	7MB
Ubuntu	<a href="http://192.168.1.204/agent/webagent/ubuntu/OnGuard_Ubuntu_Health_Checker-x86.tar.gz">http://192.168.1.204/agent/webagent/ubuntu/OnGuard_Ubuntu_Health_Checker-x86.tar.gz</a>	4MB
Ubuntu	<a href="http://192.168.1.204/agent/webagent/ubuntu/OnGuard_Ubuntu_Health_Checker.tar.gz">http://192.168.1.204/agent/webagent/ubuntu/OnGuard_Ubuntu_Health_Checker.tar.gz</a>	4MB

**Agent Customization**

Managed Interfaces: ☒ Wired ☒ Wireless ☒ VPN ☐ Other

Mode:

Username Text:

Password Text:

Agent action when an update is available:

Save Cancel

## Installer Mode

Installer Mode specifies the action to be taken when the Aruba VIA component is used to provide VPN-based access.

Installer Mode:

Agent will be used only to authenticate/perform health checks for client machines. This setting will not install the Aruba VIA component. If already installed, then the VIA component will be disabled on the client machine.  
**Note - This WILL remove any existing/installed Aruba VIA client**

Installer Mode:

Agent will include the Aruba VIA component that allows VPN-based access using the same agent that allows to authenticate/perform health checks for client machines.  
**Note - This WILL upgrade any existing/installed Aruba VIA client**

## Agent Customization

### Managed Interfaces

Select the end system network interfaces that the agent will be applied to

Note: Virtual Interfaces are categorized as “Other”

Agent Customization	
Managed Interfaces:	<input checked="" type="checkbox"/> Wired <input checked="" type="checkbox"/> Wireless <input checked="" type="checkbox"/> VPN <input type="checkbox"/> Other
Mode:	<div>Authenticate with health checks</div> <div> <div>Username Text: Username</div> <div>Password Text: Password</div> </div>
Agent action when an update is available:	Ignore

### Agent Mode options

- Authentication-no health checks: OnGuard will only authenticate users without performing any type of Health checks.
- Check health-no authentication: OnGuard agent will only perform Health checks for clients PCs, no Authentication will be performed.
- Authentication with health checks: OnGuard agent will be used for both health checks and Authenticating users.

Username/Password Text:

This is the label for the username/password fields presented to the user by the OnGuard agent if the mode requires Authentication.

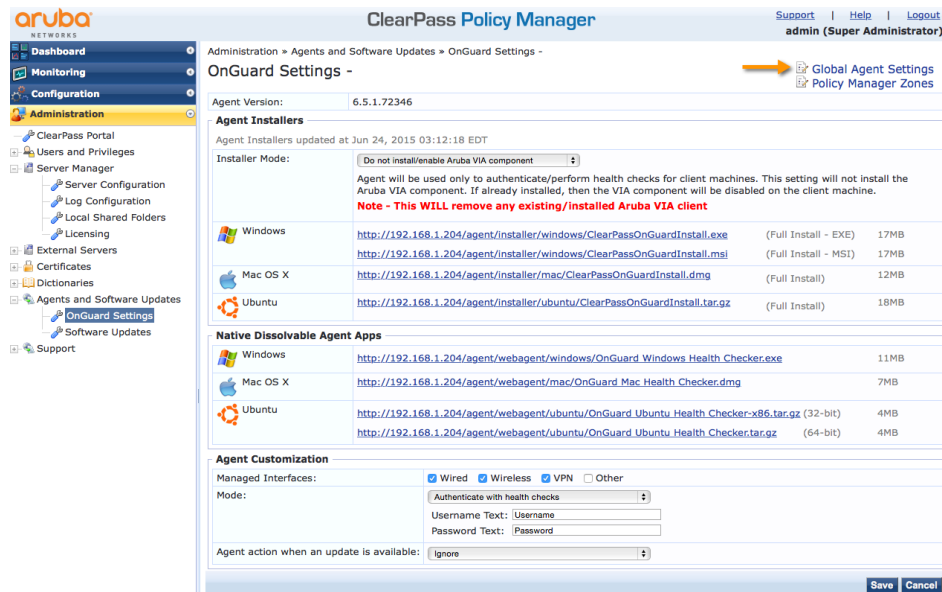
Agent action when an update is available:

- Ignore
- Notify User
- Download and Install



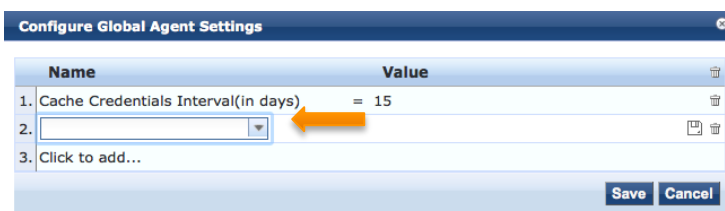
## OnGuard Global Agent Settings

The Global Agents Settings page is used to configure settings that apply to all agents.



### Global Agent Settings

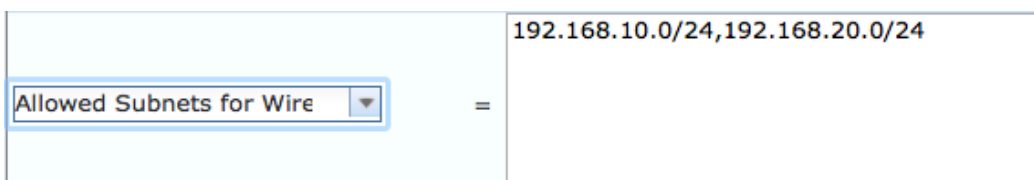
Configure the amount of time to cache OnGuard credentials.



Additional Global Agents setting include:

**Allowed Subnets for Wired access:** Add comma-separated list of IP or subnet addresses

**Allowed Subnets for Wireless access:** Add comma-separated list of IP or subnet addresses.



**Cache Credentials Interval (in days):** Select the number of days the user credentials should be cached on OnGuard agents.

**Delay to bounce after Logout (in minutes):** Specify the number of minutes that should elapse before OnGuard bounces the interface if OnGuard remains disconnected.

**Enable OnGuard requests load-balancing:** Enable this option to load balance OnGuard authentication requests across ClearPass Policy Manager servers in a cluster.

**Enable access over Remote Desktop Session:** Enable this option to allow OnGuard access through a Remote Desktop session.

**Enable to hide Logout button:** Enable this option to hide the Logout button on OnGuard agent.

**Install VPN component:** Enable this option to install the OnGuard VPN component. This will be automatically set based on what was selected for Installer Mode.

**Enable to use Windows Single-Sign On:** Enable this option to allow use of a user's Windows credentials for authentication.

**Keep-alive Interval (in seconds):** Add a keep-alive interval for OnGuard agents. After the connection is established agents periodically send keep alive messages to the ClearPass server. The server uses these messages to show the online status of client in "Monitoring->OnGuard Activity"

**OnGuard Health Check Interval (in hours):** Specify the number of hours that OnGuard will skip health checks for healthy clients.

NOTE: Note the following information when you set the OnGuard Health Check Interval parameter:

- You can set this parameter if OnGuard mode is set to health only.
- This parameter is valid only for wired and wireless interface types.
- This parameter is not applicable for the OnGuard Dissolvable Agent, VPN, and other interface types.

**Support Team Email Address:** Enter an email address that automatically populates the To field in the user's email client when they send logs.

## Configure Policy Manager Zones:

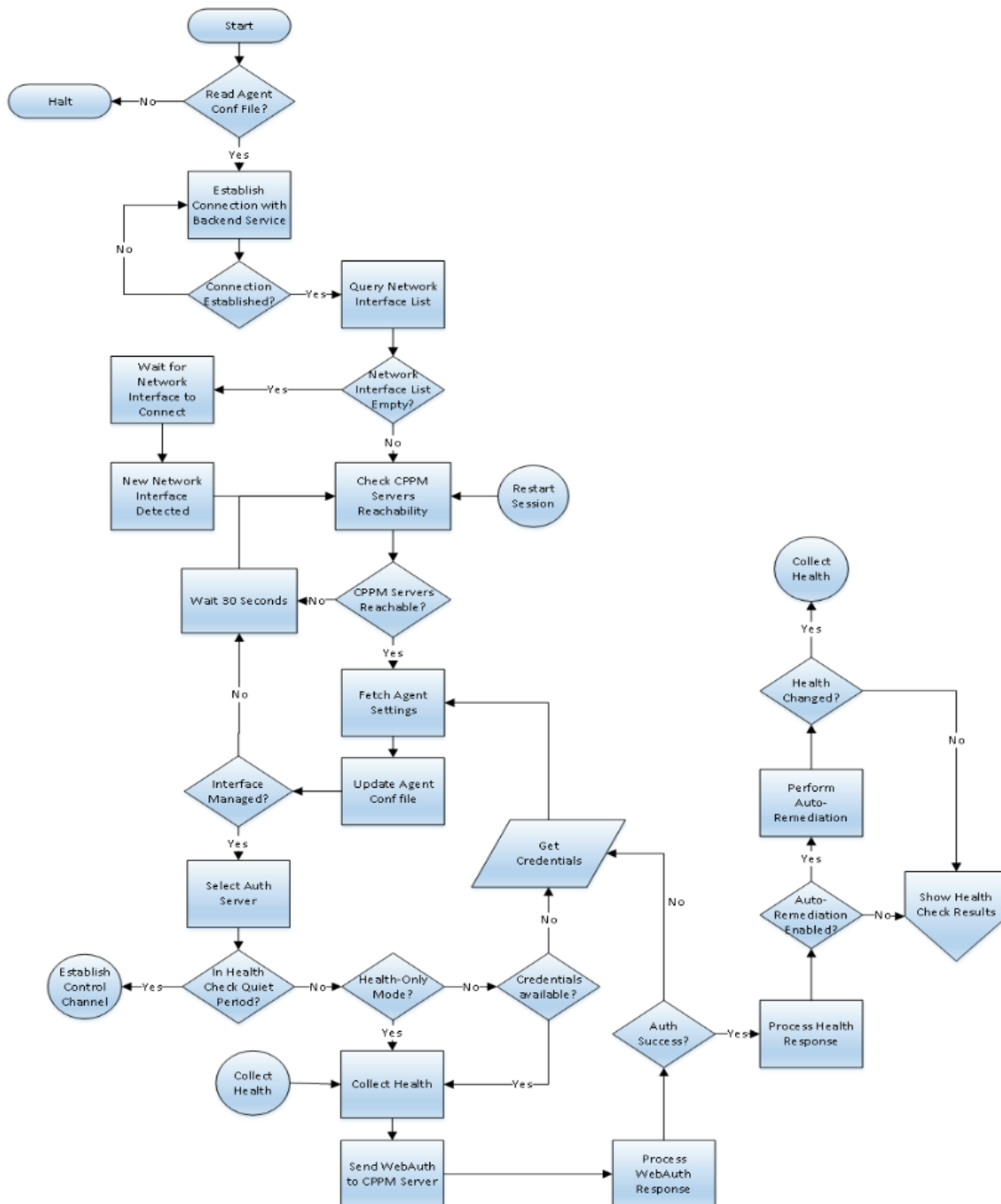
Policy Manager Zone	Client Subnets	Server IPs
No Policy Manager Zone settings configured		
<b>Zone Network Details -</b>		
Policy Manager Zone:	lab	
Client Subnets (e.g., 192.168.1.1/24):		
Default ClearPass Server IPs:	192.168.1.204	
Override Server IPs (optional):		
<span>Reset</span> <span>Delete</span> <span>Save</span> <span>Close</span>		

Optionally override the default IP address used by the Agent to communicate with ClearPass. If the Data Port is configured the agent will use it for communication by default.

Use cases include

- VIP setup: Customer wants OnGuard agents to contact VIP IP for redundancy
- External load balancer: Customer wants OnGuard connections to go through an external load balancer like F5
- Customer wants OnGuard to use management port, instead of data port, because of their network setup
- Customer wants explicit control over the order in which servers should be contacted on failover

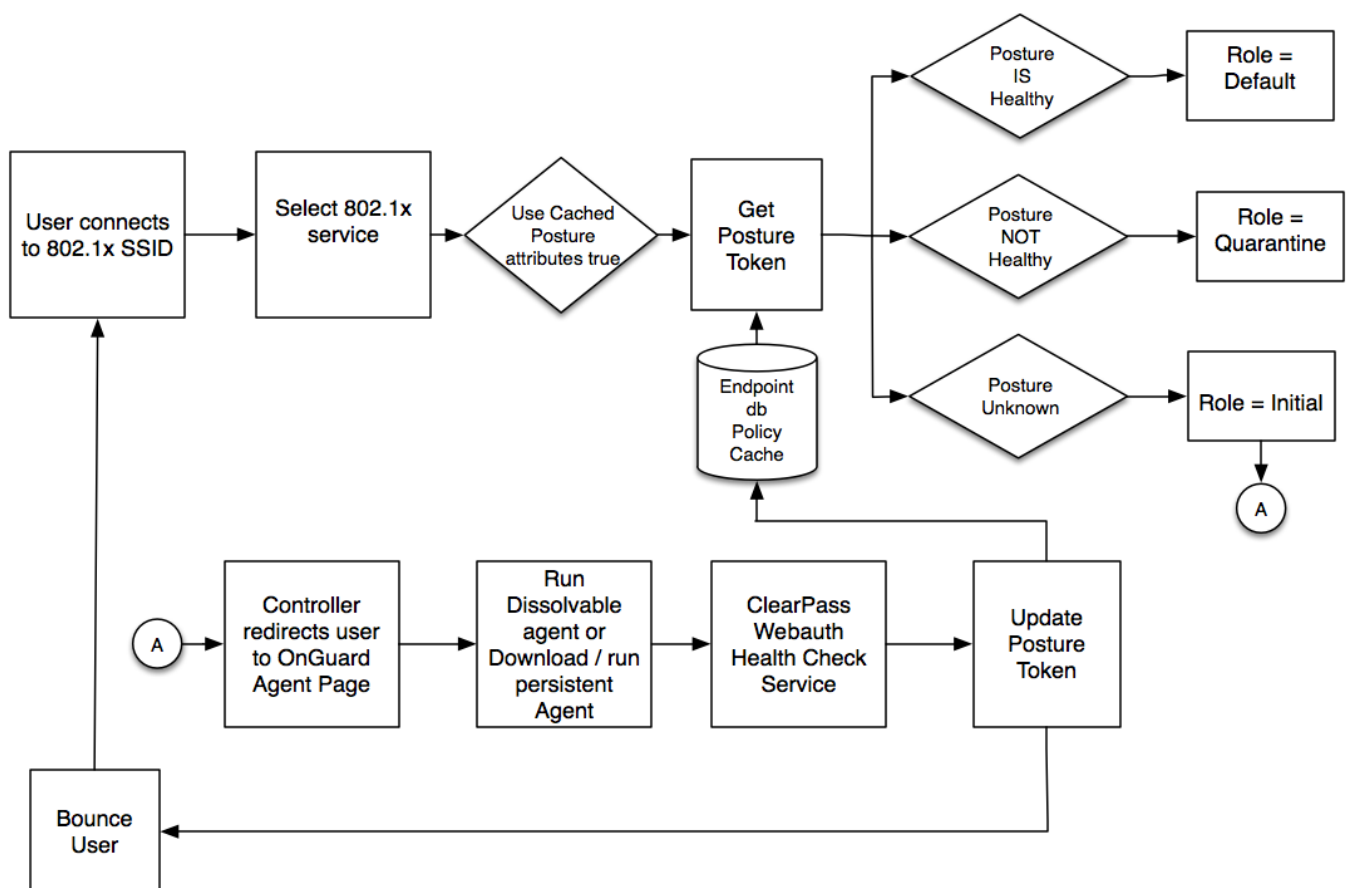
## Agent Flow Chart



## Configure ClearPass Services for OnGuard

There are two ClearPass services used by OnGuard.

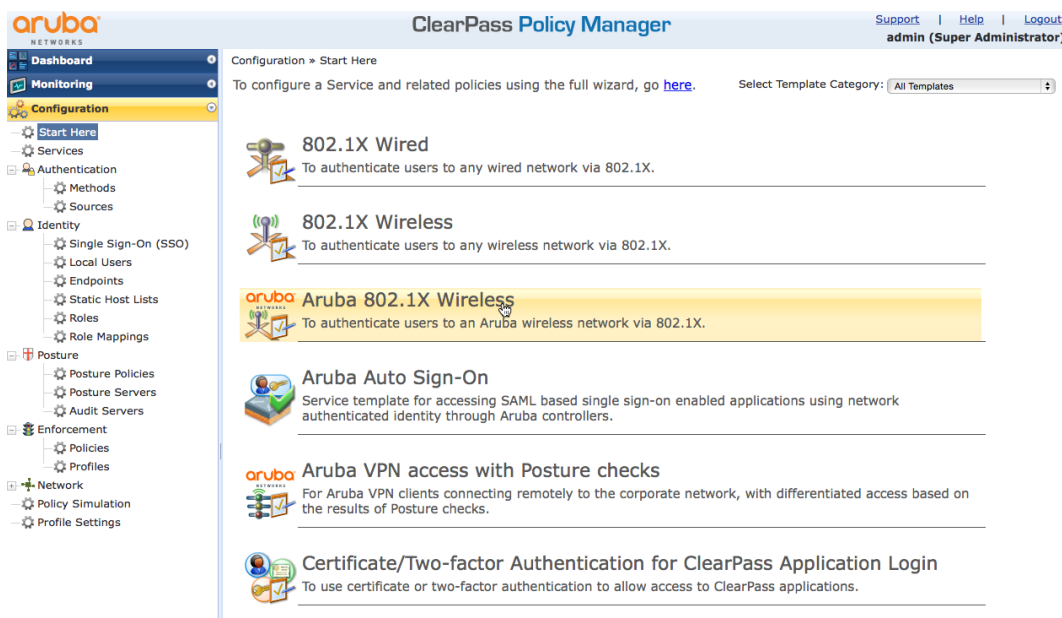
- The first is a Webauth service that communicates with the OnGuard agents. This service collects end system health tokens and updates the Endpoint policy cache.
- The second is an 802.1X service that has posture checks enabled. This service tests the cached health tokens and applies the correct enforcement profiles.



When the user connects to the 802.1x SSID for the first time the Posture token will be Unknown, the initial role will be returned to the controller and the user will be redirected to OnGuard Agent page. The user will download and run the dissolvable or persistent agent and the agent will send the health results to the Webauth Health Check service, which will update the posture token in the Endpoint database and send a Bounce User request to the controller. That will cause the user to re-authenticate and this time the posture token will be known.

## Service Configuration

The simplest way to deploy OnGuard is to first deploy a basic configuration to verify that the services and workflows are correct. After verifying the basic configuration go back and add the required level of complexity to the configuration.



Use the Aruba 802.1X wizard for your basic configuration. Selecting posture checks will cause the wizard to configure two services, an 802.1X service with posture checks enabled and a Webauth health check service.

## Service Wizard

In the example below, “basic onguard” is used as the prefix for the service names. All services, enforcement profiles, enforcement policies and posture policies created by the wizard will be prefixed with “basic onguard”.

### Service Templates - Aruba 802.1X Wireless

General	Authentication	Wireless Network Settings	Posture Settings	Enforcement Details
Select Prefix: <input type="text" value="basic onguard"/>				
Name Prefix*: <input type="text" value="basic onguard"/>				
<b>Description</b> For wireless end-hosts connecting through an Aruba 802.11 wireless access device or controller, with authentication via IEEE 802.1X (Service rules customized for Aruba WLAN Mobility Controllers). This template configures an AD Authentication Source; joins this node to the AD Domain; creates Enforcement Policy for AD based attributes; and creates an Aruba Network Access Device.				
<a href="#">Back to Start Here</a> <span>Delete</span> <span>Next &gt;</span> <span>Update Service</span> <span>Cancel</span>				

Authentication tab: For simplicity, this example uses the Local User Repository as an authentication source. In a typical enterprise environment the authentication source would most likely be Active Directory.

Configuration » Start Here

### Service Templates - Aruba 802.1X Wireless

General Authentication Wireless Network Settings Posture Settings Enforcement Details

Select Authentication Source: [Local User Repository]

[Back to Start Here](#) [Delete](#) [Next >](#) [Update Service](#) [Cancel](#)

Wireless Network Settings tab: Select the wireless controller

Configuration » Start Here

### Service Templates - Aruba 802.1X Wireless

General Authentication Wireless Network Settings Posture Settings Enforcement Details

Select a wireless controller from the list, or create a new one

Select Wireless Controller: [620]

Wireless Controller Name: [620]

Controller IP Address: [192.168.1.203]

Vendor Name: [Aruba]

RADIUS Shared Secret: [.....]

Enable RADIUS CoA: ☒

RADIUS CoA Port: [3799]

[Back to Start Here](#) [Delete](#) [Next >](#) [Update Service](#) [Cancel](#)

Under the Posture Settings tab: Enable Posture Checks, select the host operating systems to be tested and define the message to be sent to the user if the end system is quarantined.

Configuration » Start Here

### Service Templates - Aruba 802.1X Wireless

General Authentication Wireless Network Settings Posture Settings Enforcement Details

Enable Posture Checks to perform health checks after authentication.

Enable Posture Checks: ☒

Host Operating System\*: ☐ Windows ☐ Linux ☒ Mac OS X

Quarantine Message: [please contact the help desk]

[Back to Start Here](#) [Delete](#) [Next >](#) [Update Service](#) [Cancel](#)

## Enforcement Details tab:

The enforcement details will be used by the wizard to create the enforcement policies and profiles that will be attached to the services. At least one attribute to role mapping rule must be specified. In this example, if Role Name equals exec then we will assign the cxo role. This can be edited later.

The Default role is the 802.1X service default role for a HEALTHY posture token

The Initial Role is the role returned to the controller when the Radius:Tips posture equals UNKNOWN

The Quarantine Role is the role that will be sent to the controller if the posture token is not equal to HEALTHY

Configuration » Start Here

### Service Templates - Aruba 802.1X Wireless

General Authentication Wireless Network Settings Posture Settings **Enforcement Details**

Create a new Enforcement Policy

Attribute Name	Attribute Value	Aruba Role
If Role_Name	equals exec	then assign Role cxo
If Enabled	equals	then assign Role
If Enabled	equals	then assign Role
Default Role*:		basic_default
Initial Role*:		basic_initial
Quarantine Role*:		basic_quarantine

[Back to Start Here](#) [Delete](#) [Next >](#) [Update Service](#) [Cancel](#)

## Template Created Services, Policies and Profiles

The Wizard creates two services, seven enforcement profiles, two enforcement policies, and one posture policy.

### Services

[Add](#)  
[Import](#)  
[Export All](#)

- Updated 7 Enforcement Profile(s)
- Updated 2 Enforcement Policies
- Updated 1 Posture Policies
- Updated 2 service(s)

Filter: Name contains Go Clear Filter Show 10 records

#	Order	Name	Type	Template	Status
1.	1	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	●
2.	2	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement ( Generic )	●
3.	3	[Aruba Device Access Service]	TACACS	TACACS+ Enforcement	●
4.	4	[Guest Operator Logins]	Application	Aruba Application Authentication	●
5.	7	lab Onboard Provisioning	RADIUS	Aruba 802.1X Wireless	●
6.	8	lab Onboard Authorization	Application	Aruba Application Authorization	●
7.	9	lab Onboard Pre-Auth	Application	Aruba Application Authentication	●
8.	10	lab ClearPass Certificate SSO Login	Application	Aruba Application Authorization	●
9.	11	lab ClearPass Identity Provider	Application	Aruba Application Authentication	●
10.	12	socail Guest Social Media Authentication	RADIUS	RADIUS Enforcement ( Generic )	●

Showing 1-10 of 12 [Reorder](#) [Copy](#) [Export](#) [Delete](#)



## Posture Policy

The default posture policy created by the wizard for Mac OS X tests for any supported Antivirus application and any Firewall application.

**ClearPass Mac OS X Universal System Health Validator**

Mac OS X: true

**Antivirus**

**Mac OS X:**

Enable Auto Remediation: true

Enable User Notification: true

Enable Display Update URL: false

List of selected antivirus applications

Product	Product Version	Engine Version	Data File Version	Data File Update	Last Scan	Rtp Status Check
Any						
1. Supported AntiVirus	no check	no check	is latest	no check	no check	no check

**Firewall**

**Mac OS X:**

Enable Auto Remediation: true

Enable User Notification: true

Allow any product: true

## Enforcement policies

The wizard creates one Radius enforcement policy and one Webauth enforcement policy.

### Radius Enforcement Policy

Configuration » Enforcement » Policies

#### Enforcement Policies

[Add](#)  
[Import](#)  
[Export All](#)

Filter: Name contains onguard Go Clear Filter Show 10 records

#	<input type="checkbox"/>	Name ▲	Type	Description
1.	<input type="checkbox"/>	basic onguard Aruba 802.1X Wireless Enforcement Policy	RADIUS	
2.	<input type="checkbox"/>	basic onguard Aruba 802.1X Wireless OnGuard Agent Enforcement Policy	WEBAUTH	

Showing 1-2 of 2

[Copy](#) [Export](#) [Delete](#)

The Radius enforcement policy applies the Initial enforcement Profile if the posture token is UNKNOWN. This is the initial condition for end systems using the Dissolvable agent or for end systems before the Persistent Agent has been downloaded. If the cached posture token is not HEALTHY, the Quarantine enforcement profile is applied. If the cached posture token is HEALTHY and the authorization role matches the one specified in the enforcement details tab of the wizard, in our example exec, the basic onguard wireless default profile and update endpoint location profiles are applied.

## Enforcement Policies - basic onguard Aruba 802.1X Wireless Enforcement Policy

Note: This Enforcement Policy is created by Service Template

Summary	Enforcement	Rules
<b>Enforcement:</b>		
Name:	basic onguard Aruba 802.1X Wireless Enforcement Policy	
Description:		
Enforcement Type:	RADIUS	
Default Profile:	basic onguard Aruba 802.1X Wireless Default Profile	
<b>Rules:</b>		
Rules Evaluation Algorithm:	First applicable	
Conditions	Actions	
1. (Tips:Posture <b>EQUALS</b> UNKNOWN (100))	basic onguard Aruba 802.1X Wireless Initial Profile	
2. (Tips:Posture <b>NOT_EQUALS</b> HEALTHY (0))	basic onguard Aruba 802.1X Wireless Quarantined Profile	
3. (Authorization:[Local User Repository]:Role_Name <b>CONTAINS</b> exec)	basic onguard Aruba 802.1X Wireless Profile1, basic onguard Aruba 802.1X Wireless Update Endpoint Location	

## Enforcement Profiles

Summary	Profile	Attributes
<b>Profile:</b>		
Name:	basic onguard Aruba 802.1X Wireless Initial Profile	
Description:	Role assigned before health checks are performed	
Type:	RADIUS	
Action:	Accept	
Device Group List:	-	
<b>Attributes:</b>		
Type	Name	Value
1. Radius:Aruba	Aruba-User-Role	= basic_initial

Summary		Profile		Attributes	
<b>Profile:</b>					
Name:		basic onguard Aruba 802.1X Wireless Quarantined Profile			
Description:		Role assigned after health checks are performed for unhealthy users			
Type:		RADIUS			
Action:		Accept			
Device Group List:		-			
<b>Attributes:</b>					
Type		Name		Value	
1.	Radius:Aruba	Aruba-User-Role		=	basic_quarantine

Summary	Profile	Attributes
<b>Profile:</b>		
Name:	basic onguard Aruba 802.1X Wireless Default Profile	
Description:		
Type:	RADIUS	
Action:	Accept	
Device Group List:	-	
<b>Attributes:</b>		
Type	Name	Value
1. Radius:Aruba	Aruba-User-Role	= basic_default

Summary		Profile		Attributes	
<b>Profile:</b>					
Name:		basic onguard Aruba 802.1X Wireless Profile1			
Description:					
Type:		RADIUS			
Action:		Accept			
Device Group List:		-			
<b>Attributes:</b>					
Type		Name		Value	
1.	Radius:Aruba	Aruba-User-Role		=	CX0

## OnGuard Agent Enforcement Policy

The OnGuard Agent enforcement policy retrieves the posture token. If the token is HEALTHY it returns a healthy message to the agent and bounces the session. If the token is UNHEALTHY it returns an unhealthy message to the agent and bounces the session.

Configuration » Enforcement » Policies » Edit - basic onguard Aruba 802.1X Wireless OnGuard Agent Enforcement Policy

### Enforcement Policies - basic onguard Aruba 802.1X Wireless OnGuard Agent Enforcement Policy

**Note: This Enforcement Policy is created by Service Template**

Summary	Enforcement	Rules
<b>Enforcement:</b>		
Name:	basic onguard Aruba 802.1X Wireless OnGuard Agent Enforcement Policy	
Description:		
Enforcement Type:	WEBAUTH	
Default Profile:	[Aruba Terminate Session]	
<b>Rules:</b>		
Rules Evaluation Algorithm: First applicable		
Conditions		Actions
1.	(Tips:Posture <span>NOT_EQUALS</span> HEALTHY (0))	basic onguard Aruba 802.1X Wireless Quarantined Agent Enforcement, [Aruba Terminate Session]
2.	(Tips:Posture <span>EQUALS</span> HEALTHY (0))	basic onguard Aruba 802.1X Wireless Healthy Agent Enforcement, [Aruba Terminate Session]

Summary	Profile	Attributes
<b>Profile:</b>		
Name:	basic onguard Aruba 802.1X Wireless Quarantined Agent Enforcement	
Description:		
Type:	Agent	
Action:	Accept	
Device Group List:	-	
<b>Attributes:</b>		
Attribute Name		Attribute Value
1. Message	=	Your system has not passed all the health checks. Restricted network access will be given.

Summary	Profile	Attributes
<b>Profile:</b>		
Name:	basic onguard Aruba 802.1X Wireless Healthy Agent Enforcement	
Description:		
Type:	Agent	
Action:	Accept	
Device Group List:	-	
<b>Attributes:</b>		
Attribute Name		Attribute Value
1.	Message	= Your system is healthy. Full network access will be given shortly.

## OnGuard Related Services

The service wizard creates a Radius 802.1X service with posture checks enabled and a Webauth health check service

#	Server	Source	Username	Service	Login Status	Request Timestamp ▾
1.	192.168.1.204	RADIUS	exec	basic onguard Aruba 802.1X Wireless	ACCEPT	2015/06/26 15:44:29
2.	192.168.1.204	WEBAUTH	58b0356ac83a	basic onguard Aruba 802.1X Wireless Posture Checks	ACCEPT	2015/06/26 15:44:03

**802.1X service** - This service is usually edited to make it specific to a single SSID. Authentication methods, Authentication source and role mapping may also need to be edited for your environment.

#### Services - basic onguard Aruba 802.1X Wireless

Summary	Service	Authentication	Roles	Enforcement
<b>Service:</b>				
Name:	basic onguard Aruba 802.1X Wireless			
Description:	To authenticate users to an Aruba wireless network via 802.1X.			
Type:	Aruba 802.1X Wireless			
Status:	Enabled			
Monitor Mode:	Disabled			
More Options:	-			
<b>Service Rule</b>				
Match ALL of the following conditions:				
<b>Type</b>	<b>Name</b>	<b>Operator</b>	<b>Value</b>	
1. Radius:IETF	NAS-Port-Type	EQUALS	Wireless-802.11 (19)	
2. Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)	
3. Radius:Aruba	Aruba-Essid-Name	EXISTS		
<b>Authentication:</b>				
Authentication Methods:	1. [EAP PEAP] 2. [EAP FAST] 3. [EAP TLS] 4. [EAP TTLS]			
Authentication Sources:	[Local User Repository] [Local SQL DB]			
Strip Username Rules:	-			
<b>Roles:</b>				
Role Mapping Policy:	-			
<b>Enforcement:</b>				
Use Cached Results:	Enabled			
Enforcement Policy:	basic onguard Aruba 802.1X Wireless Enforcement Policy			

**Note:** Make sure the Use cached Roles and Posture attributes check box is enabled.

#### Services - basic onguard Aruba 802.1X Wireless

Summary	Service	Authentication	Roles	Enforcement
Use Cached Results:	<input checked="" type="checkbox"/> Use cached Roles and Posture attributes from previous sessions			
Enforcement Policy:	basic onguard Aruba 802.1X Wireless Enforcement <a href="#">Modify</a> <a href="#">Add new Enforcement Policy</a>			
<b>Enforcement Policy Details</b>				
Description:				
Default Profile:	basic onguard Aruba 802.1X Wireless Default Profile			
Rules Evaluation Algorithm:	first-applicable			
<b>Conditions</b>	<b>Enforcement Profiles</b>			
1. (Tips:Posture EQUALS UNKNOWN (100))	basic onguard Aruba 802.1X Wireless Initial Profile			
2. (Tips:Posture NOT_EQUALS HEALTHY (0))	basic onguard Aruba 802.1X Wireless Quarantined Profile			
3. (Authorization:[Local User Repository]:Role_Name CONTAINS exec)	basic onguard Aruba 802.1X Wireless Profile1, basic onguard Aruba 802.1X Wireless Update Endpoint Location			

The Webauth health check service applies to all Health Check requests from any Wireless interface. This is based on the Managed Interface type checkboxes on the OnGuard agent configuration page.

#### Services - basic onguard Aruba 802.1X Wireless Posture Checks

Note: This Service is created by Service Template

Summary	Service	Roles	Posture	Enforcement
<b>Service:</b>				
Name:	basic onguard Aruba 802.1X Wireless Posture Checks			
Description:	To authenticate users to an Aruba wireless network via 802.1X.			
Type:	Web-based Health Check Only			
Status:	Enabled			
Monitor Mode:	Disabled			
More Options:	Posture Compliance			
<b>Service Rule</b>				
Match ALL of the following conditions:				
Type	Name	Operator	Value	
1. Host	CheckType	MATCHES_ALL	Health	
2. Host	InterfaceType	EQUALS	WIRELESS	
<b>Roles:</b>				
Role Mapping Policy:	-			
<b>Posture:</b>				
<b>Posture Policies:</b>				
Posture Policies:	basic onguard Aruba 802.1X Wireless Mac OS X Posture Checks			
Default Posture Token:	QUARANTINE (20)			
Remediate End-Hosts:	Enabled			
Remediation URL:				
<b>Posture Servers:</b>				
Posture Servers:	-			
<b>Enforcement:</b>				
Use Cached Results:	Disabled			
Enforcement Policy:	basic onguard Aruba 802.1X Wireless OnGuard Agent Enforcement Policy			

## Enforcement tab

#### Services - basic onguard Aruba 802.1X Wireless Posture Checks

Note: This Service is created by Service Template

Summary	Service	Roles	Posture	Enforcement
Use Cached Results: <input type="checkbox"/> Use cached Roles and Posture attributes from previous sessions				
Enforcement Policy:		basic onguard Aruba 802.1X Wireless OnGuard Agent		<a href="#">Add new Enforcement Policy</a>
<b>Enforcement Policy Details</b>				
Description:				
Default Profile:		[Aruba Terminate Session]		
Rules Evaluation Algorithm:		first-applicable		
Conditions		Enforcement Profiles		
1.	(Tips:Posture NOT_EQUALS HEALTHY (0))	basic onguard Aruba 802.1X Wireless Quarantined Agent Enforcement, [Aruba Terminate Session]		
2.	(Tips:Posture EQUALS HEALTHY (0))	basic onguard Aruba 802.1X Wireless Healthy Agent Enforcement, [Aruba Terminate Session]		

## Web Login Page

In order to allow users to download the dissolvable and persistent OnGuard agents you need to create a Web Login page. The controller will redirect users to this page if the posture token is UNKNOWN.

On the Web Login page configuration check the “Require a successful OnGuard agent health check checkbox

**Guest**

**Onboard**

**Configuration**

- Start Here
- Advertising
- Authentication
- Content Manager
- Guest Manager
- Hotspot Manager
  - Start Here
  - Transaction Processors
- Pages**
  - Start Here
  - Fields
  - Forms & Views
  - Guest Self-Registrations
  - Web Logins**
  - Web Pages
- Receipts
- SMS Services
- Translations
  - Start Here
  - Translation Packs
  - Translation Assistant

**Allowed Access:**

Enter the IP addresses and networks from which logins are permitted.

**Denied Access:**

Enter the IP addresses and networks that are denied login access.

**\* Deny Behavior:** Send HTTP 404 Not Found status

Select the response of the system to a request that is not permitted.

**Post-Authentication**

Actions to perform after a successful pre-authentication.

**Health Check:** ☒ Require a successful OnGuard health check

If selected, the guest will be required to pass a health check prior to accessing the ne

**Client Agents:** Native agents with Java fallback

Select the agent options for client scanning. Native agents are available for Microsoft Windows and Apple OS X. All other OS will f

**Header HTML:**

Insert...

HTML template code displayed before the health check text.

**Footer HTML:**

Insert...

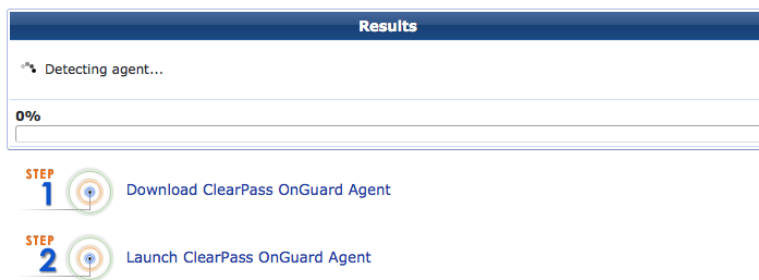
That will link the page to Login Page that will allow the user to download the Dissolvable agent

Please login to the network using your username and password.



Contact a staff member if you are experiencing difficulty logging in.

After clicking Login the user will be redirected to download and run the Dissolvable agent.



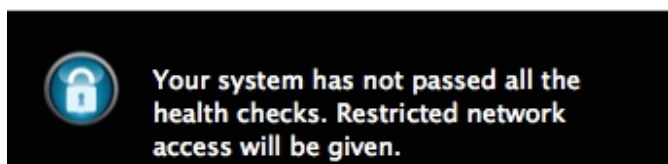
This page can be edited for the desired look and feel. Links can also be added to allow the user to download the persistent agent.

## Monitoring OnGuard

For this example we have used a Posture Policy that checks for an Active Firewall and does not permit mounting USB devices

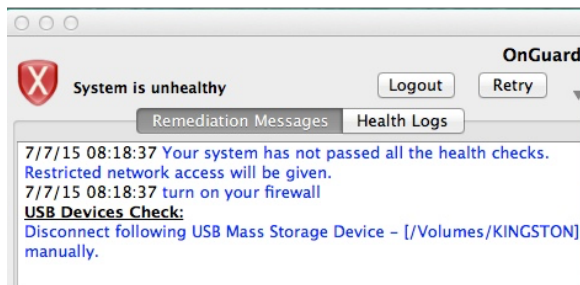
### OnGuard Agent

The OnGuard Agent on the end system informs the user of the health of the system. The Popup reports if the system is HEALTHY or UNHEALTHY. The message in the pop up is coming from the ClearPass Webauth service's enforcement profile.



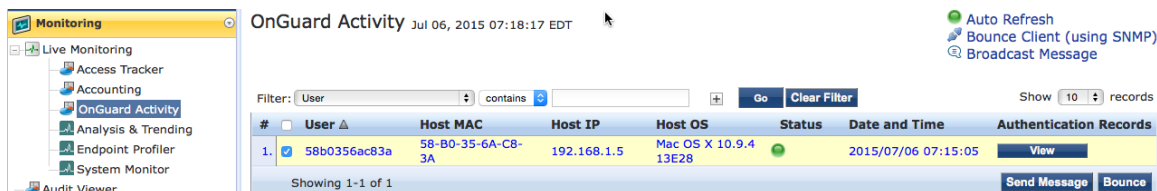


The Agent runs the health tests on the system and reports the results of the tests and any remediation steps required to bring the system into compliance to the user.



## OnGuard Activity

The OnGuard Activity tab provides real time Health status for posture-tested endpoints. The Green status light indicates the online status of the end system based on Agent keep-alive messages. This is NOT the health status of the end system.



Clicking on the entry opens the Agent and Endpoint Details page. In this case the health status is QUARANTINE based on an attached USB Device

Agent and Endpoint details			
Host MAC:	58b0356ac83a	Static IP	FALSE
Description:		Hostname	tests-mbp-2.home
Status:	Unknown	Device Category	Computer
Added by:	Policy Manager	Device OS Family	Apple Mac
MAC Vendor	-	Device Name	Mac OS X
OnGuard Details			
User:	58b0356ac83a		
Host IP:	192.168.1.5		
Status:	Online		
Agent Type:	OnGuard		
Host OS:	Mac OS X 10.9.4 13E28		
Registered Policy Manager Server:	cp.dpblab.net [192.168.1.204]		
Registered at:	2015/07/06 07:15:05		
Last Unregistered at:	2015/07/06 07:15:01		
Last Seen Health Status:	QUARANTINE		
Unhealthy Health Classes:	USBDevices		
<div>Send Message Bounce Close</div>			

The details page also allows you to send a popup message to the agent and to bounce the agent to force a new health check. The bounce option also allows the administrator to change the endpoint status to allow or block network access.

Send Notification to Agents

You have selected 1 Agent to be notified

Display Message:

Web link for more details (Optional):

Send

Cancel

Bounce Agents

You have selected 1 Agent to be bounced

Display Message (Optional):

Web link for more details (Optional):

Endpoint Status:

☒ No change in status  
☐ Allow network access  
☐ Block network access

Bounce

Cancel

## Access Tracker

Access tracker provides a real time look at all authentication requests sent to ClearPass. This example looks at the following Radius and Webauth service requests.

3.	192.168.1.204	RADIUS	exec	basic onguard Aruba 802.1X Wireless	ACCEPT	2015/07/06 07:17:25
4.	192.168.1.204	WEBAUTH	58b0356ac83a	basic onguard Aruba 802.1X Wireless Posture Checks	ACCEPT	2015/07/06 07:15:05

The Output tab from the Radius request shows the Posture status as QUARANTINE. The evaluation results show that the Firewall test returned HEALTHY and the USB test returned UNHEALTHY.

**Request Details**

Summary Input **Output**

Enforcement Profiles: basic onguard Aruba 802.1X Wireless Quarantined Profile

System Posture Status: QUARANTINE (20)

Audit Posture Status: UNKNOWN (100)

**RADIUS Response**

Radius:Aruba:Aruba-User-Role basic\_quarantine

**Posture Evaluation Results**

Posture:OSXUniversal:Firewall	HEALTHY
Posture:OSXUniversal:USB Devices	UNHEALTHY

Showing 3 of 1-10 records

Change Status Show Configuration Export Show Logs Close

The Output tab for the Webauth health check service shows the Agent posture response, Posture evaluation results and Application response

**Request Details**

Summary Input **Output**

System Posture Status: QUARANTINE (20)

Audit Posture Status: UNKNOWN (100)

**RADIUS Response**

**Posture Response**

Avenda:MacSHV:Application-Posture-Token	20
ClientVersion:HealthStatus	Healthy
Firewall:HealthStatus	Healthy
USBDevices:HealthStatus	Not Healthy

**Posture Evaluation Results**

Posture:OSXUniversal:Firewall	HEALTHY
Posture:OSXUniversal:USB Devices	UNHEALTHY

**Application Response**

Agent:Message Your system has not passed all the health checks. Restricted network access will be given.

Showing 4 of 1-10 records

Change Status Show Configuration Export Show Logs Close

## Endpoint Database

Endpoint Posture information is stored in the ClearPass Endpoint Database policy cache.

**Edit Endpoint**

EndPoint Attributes **Policy Cache**

**Policy Evaluation**

Username	58b0356ac83a
Roles	
Posture Status	HEALTHY (0)
Last Updated at	Jul 07, 2015 01:49:46 EDT
Cache Expires at	Jul 07, 2015 01:54:46 EDT

**Posture Evaluation**

Last Updated at	Jul 07, 2015 01:49:46 EDT
Cache Expires at	Jul 07, 2015 01:54:46 EDT
Applied Policy	basic mac
OSXUniversal:Firewall	HEALTHY
OSXUniversal:USB Devices	HEALTHY

Clear Cache Save Cancel

The Clear Cache button allows the administrator to manually clear the Policy Cache.

## Additional Resources

For additional information refer to the following documents available under ClearPass - Policy Manager – Tech Notes on the Aruba Support site:

- ClearPass Users Guide
- OnGuard In a Cluster Tech Note
- ClearPass OnGuard Troubleshooting Tech Note



1344 CROSSMAN AVE | SUNNYVALE, CA 94089  
1.866.55.ARUBA | T: 1.408.227.4500 | FAX: 1.408.227.4550 | [info@arubanetworks.com](mailto:info@arubanetworks.com)

[www.arubanetworks.com](http://www.arubanetworks.com)