# TECHNICAL NOTE

## CLEARPASS ONGUARD

### CONFIGURATION GUIDE

<table>
<thead>
<tr>
<th>Revised By</th>
<th>Date</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dennis Boas</td>
<td>July 2015</td>
<td>Version 1 – initial release</td>
</tr>
</tbody>
</table>
TABLE OF CONTENTS

CLEARPASS ONGUARD ....................................................................................................................... 1
INTRODUCTION ................................................................................................................................... 3
CONFIGURATION WORKFLOW ........................................................................................................ 4
CONFIGURE POSTURE POLICIES ..................................................................................................... 4
  Restricting Policies .......................................................................................................................... 5
  Windows OS ..................................................................................................................................... 6
    NAP AGENT .................................................................................................................................. 6
  OnGuard Agent .............................................................................................................................. 8
    Posture Policy Checks .................................................................................................................. 8
  Mac OS X ....................................................................................................................................... 12
CUSTOMIZE AGENT .......................................................................................................................... 15
  Installer Mode ................................................................................................................................ 15
  Agent Customization ...................................................................................................................... 16
    Managed Interfaces ....................................................................................................................... 16
    Agent Mode options ..................................................................................................................... 16
  OnGuard Global Agent Settings .................................................................................................... 17
  Configure Policy Manager Zones .................................................................................................... 19
  Agent Flow Chart ............................................................................................................................ 20
CONFIGURE CLEARPASS SERVICES FOR ONGUARD ................................................................. 21
  Service Configuration ................................................................................................................... 22
  Template Created Services, Policies and Profiles ........................................................................ 24
    Posture Policy ............................................................................................................................. 25
    Enforcement policies .................................................................................................................... 25
    Web Login Page .......................................................................................................................... 31
MONITORING ONGUARD ...................................................................................................................... 32
  OnGuard Agent ............................................................................................................................ 32
  OnGuard Activity .......................................................................................................................... 33
  Access Tracker .............................................................................................................................. 34
  Endpoint Database .......................................................................................................................... 36
ADDITIONAL RESOURCES .................................................................................................................. 36
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
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.

<table>
<thead>
<tr>
<th>Role Name</th>
<th>Description</th>
<th>Select or type role names</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lab User</td>
<td>Posture checks for Macs</td>
<td>(Machine Authenticated) (User Authenticated) (Guest) (TACACS Read-only Admin) (TACACS API Admin) (TACACS Help Desk) (TACACS Receptorist) (TACACS Network Admin) (TACACS Super Admin) (Contractor) (Other) (Employee) (Device Registration) (MAC Caching) (Onboard Android) (Onboard Windows) (Onboard Mac OS X) (Onboard iOS) (BYOD Operator) (AntiGroup v1) (AntiGroup v2) (Aruba TACACS root Admin) (Aruba TACACS read-only Admin) (Onboard Chromebook) (Onboard Linux)</td>
</tr>
</tbody>
</table>
Windows OS

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

NAP AGENT

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.
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.

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.
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.
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.

Then choose the Windows operating system you want to enable checks for. In this example, select Windows 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.

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.

Mac OS X

In the following example we have configured three Policies for Mac OS X.
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 Remediation is checked if the application 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

<table>
<thead>
<tr>
<th>Summary</th>
<th>Policy</th>
<th>Posture Plugins</th>
<th>Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Policy:</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy Name:</td>
<td>Mac Lab access</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Posture Agent:</td>
<td>Web Agent</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Host Operating System:</td>
<td>MACOSX</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Restrict by Roles:</td>
<td>Lab Access</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Posture Plugins:</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The list of selected plugins:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Rules:</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rules Evaluation Algorithm:</td>
<td>First applicable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Conditions</td>
<td>Posture Token</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.</td>
<td>Passes all SHV checks - ClearPass Mac OS X Universal System Health Validator</td>
<td>HEALTHY</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Fails one or more SHV checks - ClearPass Mac OS X Universal System Health Validator</td>
<td>QUARANTINE</td>
<td></td>
</tr>
</tbody>
</table>
Since this policy applies to uses 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.

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

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

Installer Mode

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

- **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 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:** Install and enable Aruba VIA component

  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 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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cache Credentials Interval</td>
<td>15 days</td>
</tr>
<tr>
<td>1. Click to add...</td>
<td></td>
</tr>
</tbody>
</table>
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:

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**
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

<table>
<thead>
<tr>
<th>General</th>
<th>Authentication</th>
<th>Wireless Network Settings</th>
<th>Posture Settings</th>
<th>Enforcement Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Prefix:</td>
<td>basic onguard</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name Prefix*:</td>
<td>basic.onguard</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Description:

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.
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.

Wireless Network Settings tab: Select the wireless controller

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.
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

Template Created Services, Policies and Profiles

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

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

Enforcement policies

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

Radius Enforcement Policy

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

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

**Enforcement Profiles**

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

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

<table>
<thead>
<tr>
<th>Summary</th>
<th>Profile</th>
<th>Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Profile:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name:</td>
<td>basic onguard Aruba 802.1X Wireless Default Profile</td>
<td></td>
</tr>
<tr>
<td>Description:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type:</td>
<td>RADIUS</td>
<td></td>
</tr>
<tr>
<td>Action:</td>
<td>Accept</td>
<td></td>
</tr>
<tr>
<td>Device Group List:</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td><strong>Attributes:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>Name</td>
<td>Value</td>
</tr>
<tr>
<td>1.</td>
<td>Radius:Aruba</td>
<td>Aruba-User-Role = basic_default</td>
</tr>
</tbody>
</table>
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.
OnGuard Related Services

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

<table>
<thead>
<tr>
<th>#</th>
<th>Server</th>
<th>Source</th>
<th>Username</th>
<th>Service</th>
<th>Login Status</th>
<th>Request Timestamp</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>192.168.1.204</td>
<td>RADIUS</td>
<td>exec</td>
<td>basic onguard Aruba 802.1X Wireless</td>
<td>ACCEPT</td>
<td>2015/06/26 15:44:29</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>802.1X Wireless post QPort Authentication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>192.168.1.204</td>
<td>WEBAUTH</td>
<td>58b0356ac83a</td>
<td>basic onguard Aruba 802.1X Wireless Posture Checks</td>
<td>ACCEPT</td>
<td>2015/06/26 15:44:03</td>
</tr>
</tbody>
</table>

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

Your system is healthy. Full network access will be given shortly.
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.

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

### Enforcement tab

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

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

<table>
<thead>
<tr>
<th>Service</th>
<th>Roles</th>
<th>Posture</th>
<th>Enforcement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name: basic onguard Aruba 802.1X Wireless Posture Checks</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description: To authenticate users on an Aruba wireless network via 802.1X.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type: Web-based Health Check Only</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Status: Enabled</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitor Mode: Disabled</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>More Options: Posture Compliance</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Roles:**

- Role Mapping Policy: 

**Posture Policies:**

- Posture Policies: basic onguard Aruba 802.1X Wireless Mac OS X Posture Checks
- Default Posture Token: QUARANTINE (20)
- Remediate End-Hosts: Enabled
- Remediation URL: 
- Posture Servers: 

**Enforcement:**

- Use Cached Results: 
- Enforcement Policy: basic onguard Aruba 802.1X Wireless OnGuard Agent Enforcement

**Enforcement Policy Details**

- Description: 
- Default Profile: [Aruba Terminate Session]
- Rules Evaluation Algorithm: first-applicable

<table>
<thead>
<tr>
<th>Conditions</th>
<th>Enforcement Profiles</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. (Tips: Posture NOT_EQUALS HEALTHY (0))</td>
<td>basic onguard Aruba 802.1X Wireless Quarantined Agent Enforcement, [Aruba Terminate Session]</td>
</tr>
<tr>
<td>2. (Tips: Posture EQUALS HEALTHY (0))</td>
<td>basic onguard Aruba 802.1X Wireless Healthy Agent Enforcement, [Aruba Terminate Session]</td>
</tr>
</tbody>
</table>
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
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.

Login
Log in

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.
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.

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.

<table>
<thead>
<tr>
<th></th>
<th>IP Address</th>
<th>Service</th>
<th>Identity</th>
<th>Type</th>
<th>Status</th>
<th>Date/Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>192.168.1.204</td>
<td>RADIUS</td>
<td>exec</td>
<td>basic onguard Aruba 802.1X Wireless</td>
<td>ACCEPT</td>
<td>2015/07/06 07:17:25</td>
</tr>
<tr>
<td>4</td>
<td>192.168.1.204</td>
<td>WEBAUTH</td>
<td>5ba0356ac83a</td>
<td>basic onguard Aruba 802.1X Wireless Posture Checks</td>
<td>ACCEPT</td>
<td>2015/07/06 07:15:05</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Summary</th>
<th>Input</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enforcement Profiles:</td>
<td>basic onguard Aruba 802.1X Wireless Quarantined Profile</td>
<td></td>
</tr>
<tr>
<td>System Posture Status:</td>
<td>QUARANTINE (20)</td>
<td></td>
</tr>
<tr>
<td>Audit Posture Status:</td>
<td>UNKNOWN (100)</td>
<td></td>
</tr>
</tbody>
</table>

**RADIUS Response**
- Radius:Aruba:Aruba-User-Role: basic_quarantine

**Posture Evaluation Results**
- Posture:OSXUniversal:Firewall: HEALTHY
- Posture:OSXUniversal:USB Devices: UNHEALTHY

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

<table>
<thead>
<tr>
<th>Summary</th>
<th>Input</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Posture Status:</td>
<td>QUARANTINE (20)</td>
<td></td>
</tr>
<tr>
<td>Audit Posture Status:</td>
<td>UNKNOWN (100)</td>
<td></td>
</tr>
</tbody>
</table>

**RADIUS Response**
- Avenda:MacHIV: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.
Endpoint Database

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

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