



Design and Implementation Guide

Deploying Microsoft's (NAP) Network Access Protection with Aruba's Mobile Network Solutions

Thenu Kittappa

Technical Marketing

Introduction

With an increasing trend of mobility, more and more companies outfit their employees with wireless mobile devices that leave the corporate network and attach to networks at homes, public wireless hotspots, hotels, and partner sites. When these devices return to the corporate network, any malicious software they may be carrying can be spread to other corporate systems. For this reason, ensuring that devices are properly protected from malicious software has become a key interest of IT departments

Aruba Network's user-centric architecture has comprehensive access control capabilities and is built on a standards-based architecture that can easily integrate 3rd party security vendors for functions such as endpoint compliance.

Aruba has partnered with Microsoft® to support Network Access Protection (NAP) for mobile users. Network Access Protection for Windows Vista™ and Windows Server® “Longhorn” (now in beta) is a technology designed to prevent networked assets from connecting to, or communicating with, non-compliant clients. It enforces compliance to network access and health requirement policies by setting access rights based upon validated health state and by coordinating endpoint remediation services to ensure ongoing compliance.

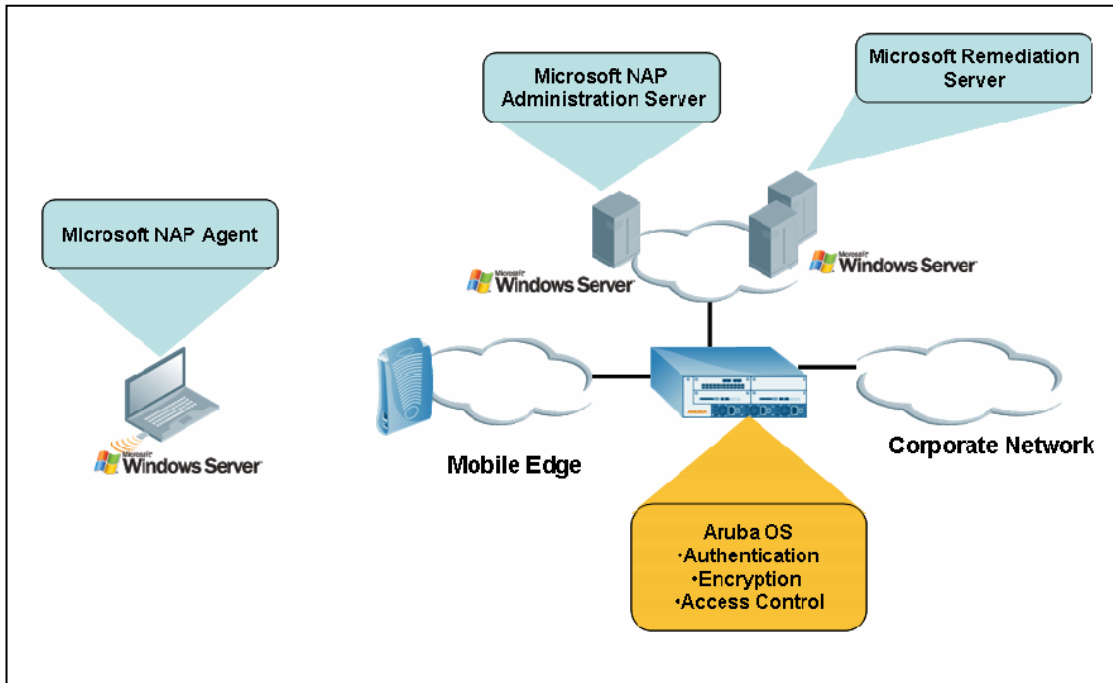
Reference documents

- Tech Brief: Secure and scalable enforcement of Microsoft's Network Access Protection in Mobile Networks -- http://www.arubanetworks.com/pdf/technology/tb_NAPsolution_overview.pdf
- Microsoft NAP documentation – <http://www.microsoft.com/nap>

NAP for Wireless LANs

This document discusses the NAP solution within the scope of the 802.1x and 802.11i wireless security mechanisms.

A Simple NAP Architecture



Aruba and Microsoft Network Access Protection Architecture

Wireless Settings

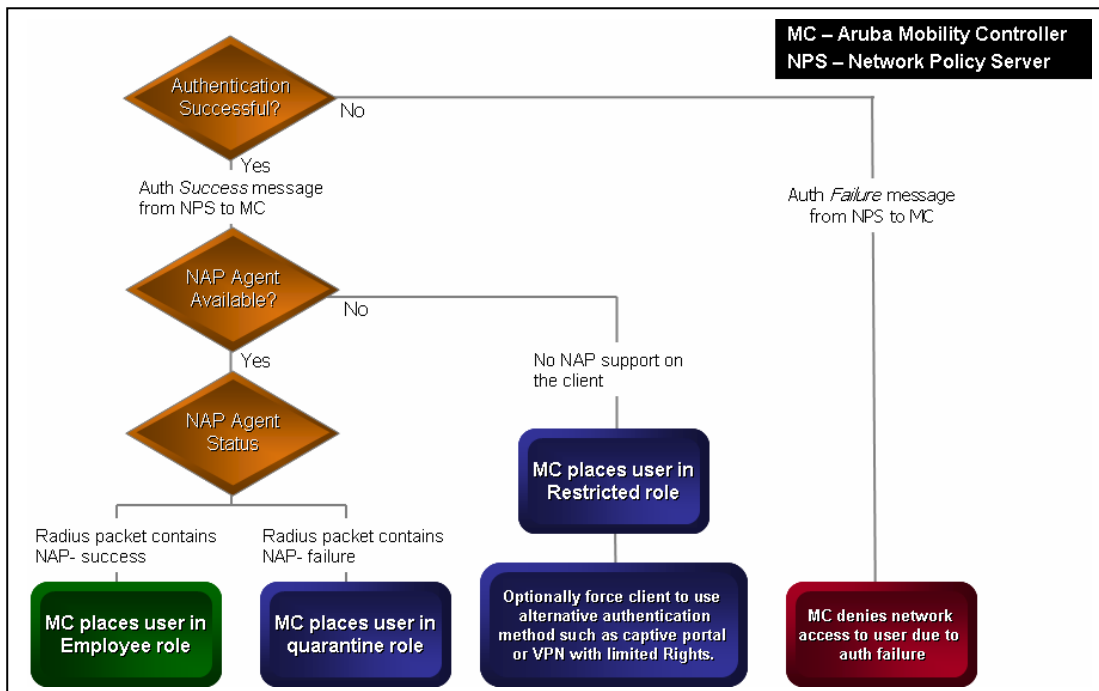
A general recommendation is to implement the highest level of encryption available, which, in the case of an 802.11 network, happens to be 802.11i followed by 802.1x.

The SSID that is used to enable users to connect to the corporate network should support WPA2-AES / WPA-TKIP or dynamic WEP with 802.11i / 802.1x WiFi authentication methods.

NAP operations

The basic Microsoft NAP Solution can be illustrated by the diagram above.

- The managed Microsoft clients tries to connect to the network, and is required to authenticate
- The client provides its login credentials to the sever and during the login process the client's NAP agent (system health agent), if enabled on the client, presents the client's current health status (anti virus signatures, patch levels, firewall settings, applications etc)
- The Aruba mobility controller forwards the authentication credentials and health state information using the RADIUS protocol to the Network Policy Server (a Microsoft RADIUS server). The NPS evaluates the client's health status against a pre-defined set of policies.



- Microsoft NPS validates the client's credentials once received. If the client credentials do not match the entries in Active Directory, the authentication fails, a failed authentication message is passed to the Aruba controller, and the controller denies network access to the client.
- If the authentication succeeds, but the client is not compliant with the predefined health requirement policy, Microsoft NPS sends limited network access configuration information to the Aruba mobility controller, which places the client in a "role" with restrictive firewall policies. The client has limited access to the network or any other clients, and is redirected to get updates from a remediation server. The client requests and receives the updates and starts over by re-authenticating.
- If the client is compliant with the health requirement policy, it is granted access to the network according to its business needs; e.g. a sales user is granted access to sales servers while access to finance networks and servers is blocked.

Advantages of using Aruba

The Aruba solution allows the network manager to further enhance the usability, scalability and manageability of this solution. By using the Aruba system's ability to assign roles and policies to users based on their authentication state and the attributes returned, users can be dynamically classified into different user groups based on the authentication results.

Employee Group	Authentication Mechanism	Authentication Status	Health Check Status	AD User Group	Aruba User Group and Policy
Corporate user	802.11i with WPA2-AES	FAIL	FAIL	- NA -	Deny Access
		PASS	FAIL	- NA -	Quarantine Role with limited access to remediation servers
		PASS	PASS	Employee	Employee
Sales	802.11i with WPA2-AES	FAIL	FAIL	- NA -	Deny Access
		PASS	FAIL	- NA -	Quarantine Role with limited access to remediation servers
		PASS	PASS	Sales	Sales
Guest	Open with Captive Portal	- NA -	- NA -	- NA -	Guest with internet access only
Voice Handsets	Pre-shared key with MAC/SSID Auth	- NA -	- NA -	- NA -	Voice with access limited to the VoIP protocols and /or required servers

SYSTEM REQUIREMENTS

Microsoft

- Windows XP or Windows Vista
- Windows Server "Longhorn"
- Network Policy Server (Microsoft's RADIUS server. A component of Windows Server "Longhorn")
- Active Directory (Microsoft's directory service. A component of Windows Server "Longhorn")

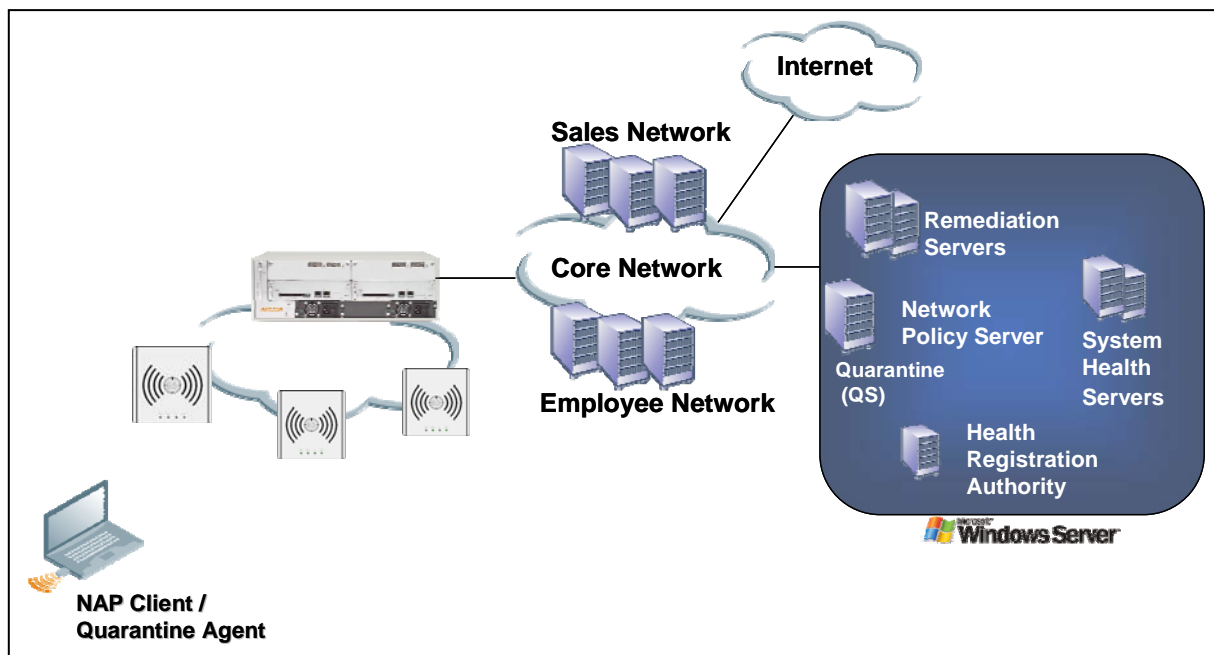
Aruba Networks

- Aruba Mobility Controller (200, 800, 2400, or 6000)
- ArubaOS Policy Enforcement Firewall software module
- ArubaOS External Services Interface software module (optional)
- ArubaOS VPN Server software module (optional)

Configuration

A NAP-ready WLAN has three major components, the Microsoft Network Policy Server (NPS), the Aruba WLAN and the Microsoft Vista / XP client with NAP support. This document details the steps to configure NPS and the Aruba controller and offers some tips on enabling NAP in the client. This document does not discuss the procedures to setup Quarantine servers.

For the purpose of this document, the following topology will be considered.



The order in which the devices will be configured is as follows:

1. Aruba Mobility Controller
 - WiFi Settings
 - Radius Settings
 - Policies
 - Roles
2. NPS Server
 - Radius Client setting
 - Connect Request Policy
 - Security Health Policy
 - Health Policy
 - Network Policy
3. Client
 - Enabling the NAP Client

Configuring the Aruba Controller

Pre-requisites

- Ensure that the firewall licenses has been enabled on the controller
- Refer to the Aruba Setup guides for initial setup. This guide assumes that the network is up and running and discusses the steps required to enable NAP on the network.

Configuring the Authentication Profile

Configuring the RADIUS Server

1. Navigate to the **Configuration** page on the Aruba Controller.
2. Select **Authentication > Server > Radius Server** Option
3. Click on **New** and enter a user friendly name for the Radius server. Ex: NPS_test. Click **Add**.
4. Click on the NPS server name that was just added. This will open the Radius configuration page

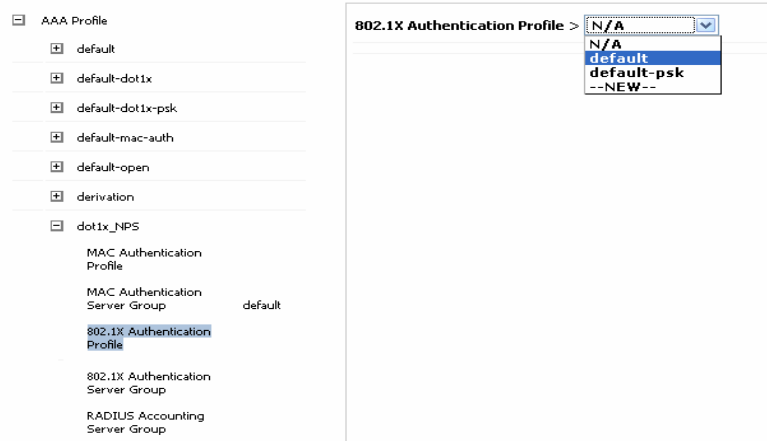
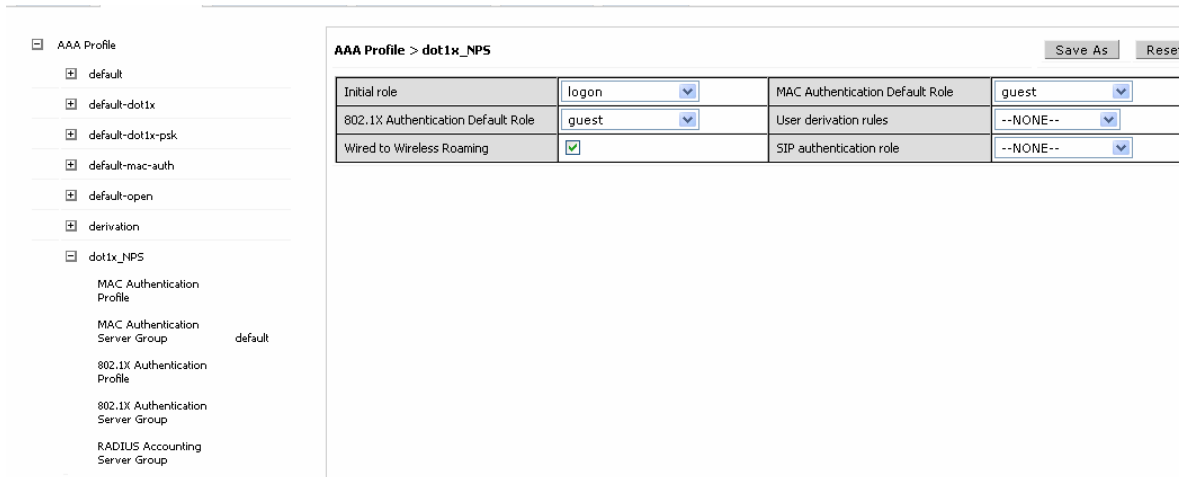
RADIUS Server > NPS		Save As Reset	
Host	10.4.101.150	Key	***** Retype: *****
Auth Port	1812	Acct Port	1813
Retransmits	3	Timeout	5 sec
NAS ID	Aruba Controller 1	NAS IP	10.100.117.250
Use MD5	<input type="checkbox"/>	Mode	<input checked="" type="checkbox"/>

5. Enter the **Host** IP Address which is the RADIUS server address, the key that is shared between the RADIUS server and the Controller, the key used in this example is *aruba123*, and the NAS IP Address which is the controller's IP address.
6. Click **Apply** for the changes to take effect.

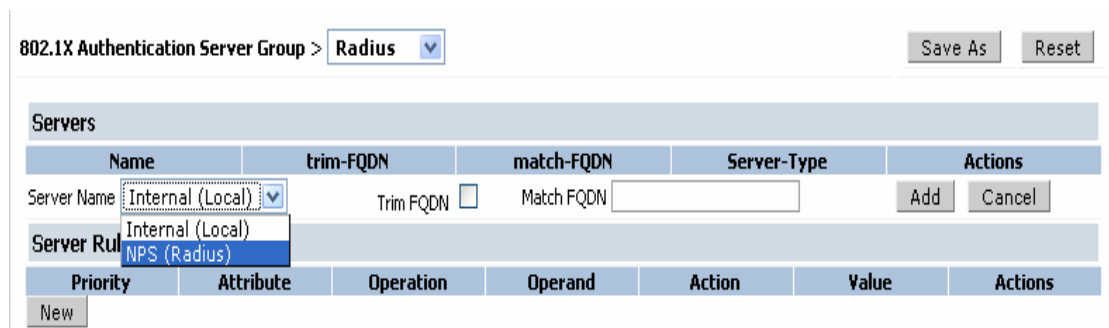
Configuring the Authentication Profile

1. Navigate to the **Configuration > Authentication > Server > AAA Profiles** Option tab.
2. Click on **Add** to add the **Authentication** profile, enter the profile name, *ex dot-1x_NPS* and click on **Apply**.

- Click on the (+) sign next to the configured profile name to change the settings.



- Select the 802.1x Authentication Profile and select the default profile from the pull down menu. Click Apply.
- Click on the 802.1x Authentication Server Group and select Radius from the drop down menu.
- In the resulting page, select New under Servers. Select the configured RADIUS server from the pull down menu and click Add. Click Apply for the changes made to take effect.



Configuring the Policies and Roles

Configure the Policies

1. Navigate to Configuration > Access Policies > Policies
2. Click on **Add** to add a new policy. Enter the policy name **employee_policy**

The screenshot shows the 'Add New Policy' configuration page in the Aruba management console. The breadcrumb navigation is 'Security > Firewall Policies > Add New Policy'. There are tabs for 'User Roles', 'System Roles', 'Policies', 'Time Ranges', and 'Guest Access'. The 'Policies' tab is active. A 'Policy Name' field contains 'employee_policy' and the 'Policy Type' is set to 'Session'. Below this is a 'Rules' section with a table header: Source, Destination, Service, Action, Log, Mirror, Queue, Time Range, BlackList, TOS, 802.1p Priority, Action. An 'Add' button is below the header. The table contains one rule: Source is 'any', Destination is 'network' (with Host IP '10.100.0.0' and Mask '255.255.255.0'), Service is 'any', Action is 'permit', and Log and Mirror are unchecked. Queue is set to 'Low' and 802.1p Priority is 'High'. There are 'Add' and 'Cancel' buttons at the bottom right of the table. An 'Apply' button is at the bottom right of the entire form. A 'Commands' section with a 'View Commands' link is at the very bottom.

3. Click on **Add** under **Rules**.
4. Configure policies that will limit Employee access to the required servers and network devices.
5. Click on **Add**. To add additional rules, click on **Add** and repeat the process.
6. Click **Apply** to apply the changes made.
7. Create the policy **sales_policy**.
8. Add the access rules as explained above and limit access to only those devices that users assigned to the sales role can access.
9. Click **Apply** for the changes to take effect.
10. Create the **Quarantine_policy** and limit access to the quarantine servers and if required internet access. For this policy, limit peer-to-peer traffic.
11. Click **Apply** for the changes to take effect.

Configure the Roles

1. Navigate to **Configuration > Access Control > User Roles**
2. Click **Add** to add a new role
3. Enter the role name as **Employee**.
4. Click **Add** under **Firewall Policies**, select the **Choose from Configured Policies** radio button.
5. From the pull down menu select the **control** policy. Click **Done**.
6. Click **Add** and select the **employee_policy**.
7. Click **Apply** for the changes to take effect.
8. Repeat to create the **Sales** and **Quarantine** role.
9. Assign the **control** and **sales_policy** to the **Sales** role, the **Quarantine_policy** and **control_policy** to the **Quarantine** role.

Configuring RF on the controller

1. Navigate to **Configuration > AP Configuration > AP Group**.
2. Create a new group **dot1xAPs** by selecting the **Add** button. Click **Add** to add the group.
3. Edit the created group to add the required SSID. Click the **Edit** tab next to the group name.
4. Click on the **Wireless LAN** option.
5. Click on **Virtual AP**, under **Add a profile**, select **New** from the pull down menu, enter the Virtual AP profile name **aruba-dot1x** and click **Add**.
6. Click **Apply**.

Configuring the NPS

Pre-requisites

- Ensure that the server is configured as a Domain controller and a DNS server
- Ensure that CA authority has been installed and started on the server.
- Ensure that NPS is installed on the server.
- Ensure that the NPS server is configured to be a member of the same domain.

Create a user account in Active Directory

1. Click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. In the console tree, double-click **contoso.com**, right-click **Users**, point to **New**, and then click **User**.
3. In the **New Object - User** dialog box, next to **Full name**, type **User1 User**, and in **User logon name**, type **User1**.
4. Click **Next**.
5. In **Password**, type the password that you want to use for this account, and in **Confirm password**, type the password again.
6. Clear the **User must change password at next logon** check box, and select the **Password never expires** check box.
7. Click **Next**, and then click **Finish**.
8. Right Click on the user / **Properties**. Select the **Dial-in** tab and select the **Allow access** radio tab.

Add a user to the Right Work Group in Active Directory

Next, add the newly created user to the user group that best reflects the user's logical access rights group. This group will be used to derive the right roles on the Aruba controller.

1. Click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. In the console tree, double-click **contoso.com**, and then click **Users**.
3. In the details pane, double-click **Domain Admins**.
4. In the **Domain Admins Properties** dialog box, click the **Members** tab, and then click **Add**.
5. Under **Enter the object names to select (examples)**, type **User1**, the user name that you created in the preceding procedure, and then click **OK** twice.
6. Close the **Active Directory Users and Computers** window.

Configuring the RADIUS Clients on the NPS server

1. Open the Network Policy Server Program, **Start > Administrative Tools > Network Policy Server**.
2. Double-click **RADIUS Clients and Servers**.
3. Right-click **RADIUS Clients**, and then click **New RADIUS Client**.

New RADIUS Client

Enable this RADIUS client

Name and Address

Friendly name:
Aruba Controller

Address (IP or DNS):
10.100.117.250

Vendor

Specify RADIUS Standard for most RADIUS clients, or select the RADIUS client vendor from the list.

Vendor name:
RADIUS Standard

Shared Secret

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

Manual Generate

Shared secret:
.....

Confirm shared secret:
.....

Additional Options

Access-Request messages must contain the Message-Authenticator attribute

RADIUS client is NAP-capable

4. In the **New RADIUS Client** dialog box, enter the following information
 1. **Friendly name** - type a user friendly name for the controller, *Aruba Controller*.
 2. **Address (IP or DNS)** - type the controller's address, *10.100.117.250*
 3. **Shared secret** - type a secret password. This will also be configured on the aruba controller, *aruba*.
 4. **Confirm shared secret** – re-type the **secret**, *aruba*.
5. Select the **Access-Request must contain the Message Authenticator attribute** check box, and then click **Finish**.
6. Verify that the **RADIUS client is NAP-capable** checkbox is cleared.
7. Check the **Enable this Radius Client** check box.
8. In the left pane, click **RADIUS Clients**. Your new RADIUS client should be displayed in the middle pane.

When using multiple controllers, a unique entry needs to be made for each controller.

Configure connection request policy

The Connection Request Policy is used to indicate if the requests from the controller would be processed locally or remotely. To configure the connection request policy

1. In the same Network Policy Server Window, double-click **Policies**, and then click **Connection Request Policies**.
2. Disable the default CRP found under **Policy Name** by right-clicking the **policy**, and then clicking **Disable**.
3. Right-click **Connection Request Policies**, and then click **New**.
4. In the **Specify Connection Request Policy Name and Connection Type** window, under **Policy name**, type *Aruba_PEAP_Policy*

The screenshot shows the 'New Connection Request Policy' dialog box with the title 'Specify Connection Request Policy Name and Connection Type'. It includes a sub-header 'Specify Connection Request Policy Name and Connection Type' and a description: 'You can specify a name for your connection request policy and the type of connections to which the policy is applied.' The 'Policy name' field contains 'Aruba_PEAP_Policy'. Under 'Network connection method', the 'Type of network access server' radio button is selected, and the dropdown menu shows 'Unspecified'. The 'Vendor specific' radio button is unselected, and its dropdown menu shows '10'.

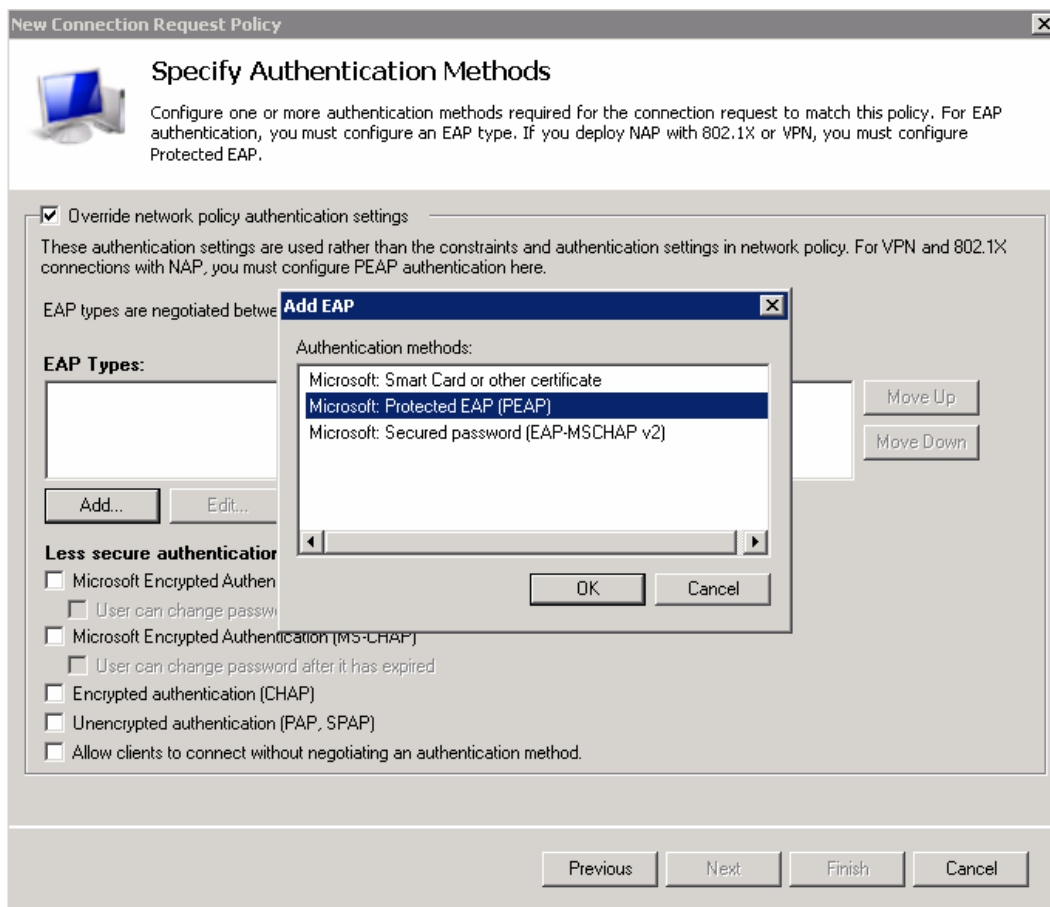
5. Click **Next**, on the next page click **Add** to add the Condition
6. Double click on the **NAS IPv4 Address** option and add the Aruba controller's IP Address , 10.100.117.250

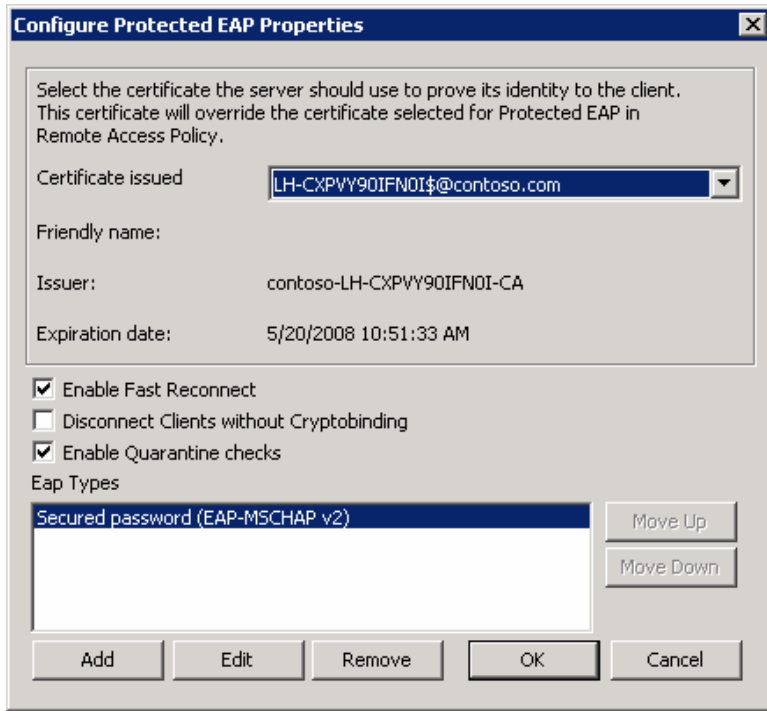
The screenshot shows the 'New Connection Request Policy' dialog box with the title 'Specify Conditions'. It includes a sub-header 'Specify Conditions' and a description: 'Specify the conditions. A minimum of one condition is required.' The 'Conditions' table is empty. The 'Condition description' field is empty. The 'Select condition' dialog box is open, showing a list of conditions: 'Called Station ID', 'NAS Identifier', 'NAS IPv4 Address', 'NAS IPv6 Address', and 'NAS IPv4 Address'. The 'NAS IPv4 Address' condition is selected. The 'NAS IPv4 Address' dialog box is also open, showing the text 'Specify the IPv4 address of the network access server sending the access request message. You can use pattern matching syntax.' and the IP address '10.100.117.250' entered in the text field. The 'Add...' button is highlighted.

7. Click **OK** , **Next**
8. Verify that the Authentication requests on this server checkbox is selected and click **Next**.
9. In the **Specify Authentication Methods**, select **Override network policy authentication settings**.
10. Click **Add** under the EAP dialog and select the **PEAP** option.

Note: Additional inner authentication methods (such as TLS) can be enabled by clicking Add, and then selecting additional EAP types. For this test lab, we will use the default inner authentication method for PEAP, which is EAP-MSCHAPv2.

11. Click **OK**
12. Select **PEAP** in the EAP dialog box and click **Edit**.
13. Verify that **Enable Quarantine checks** is selected, and the right CA authority appears next to Certificate issued.
14. Click **OK**, **Next** , **Next** and **Finish**

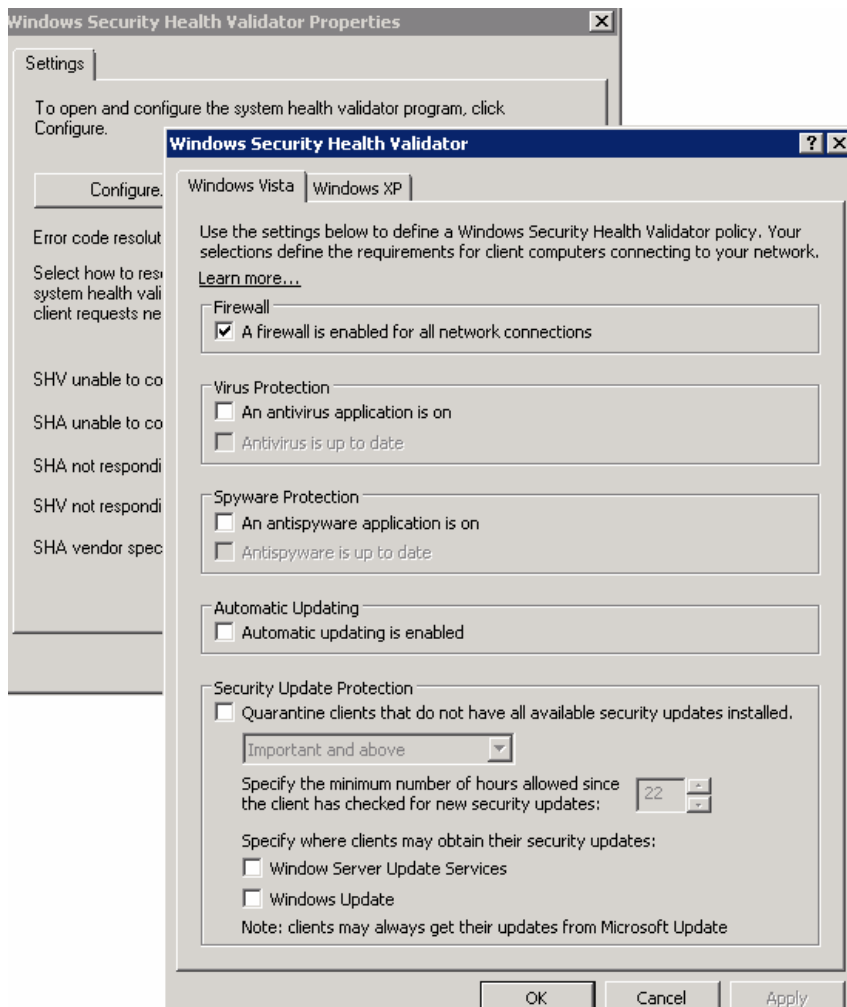




Configure SHVs on the NPS

SHVs define configuration requirements for computers that attempt to connect to your network. For the test lab, Windows Security Health Validator will be configured to require only that Windows Firewall is enabled. The SHVs are also configured in the NPS window.

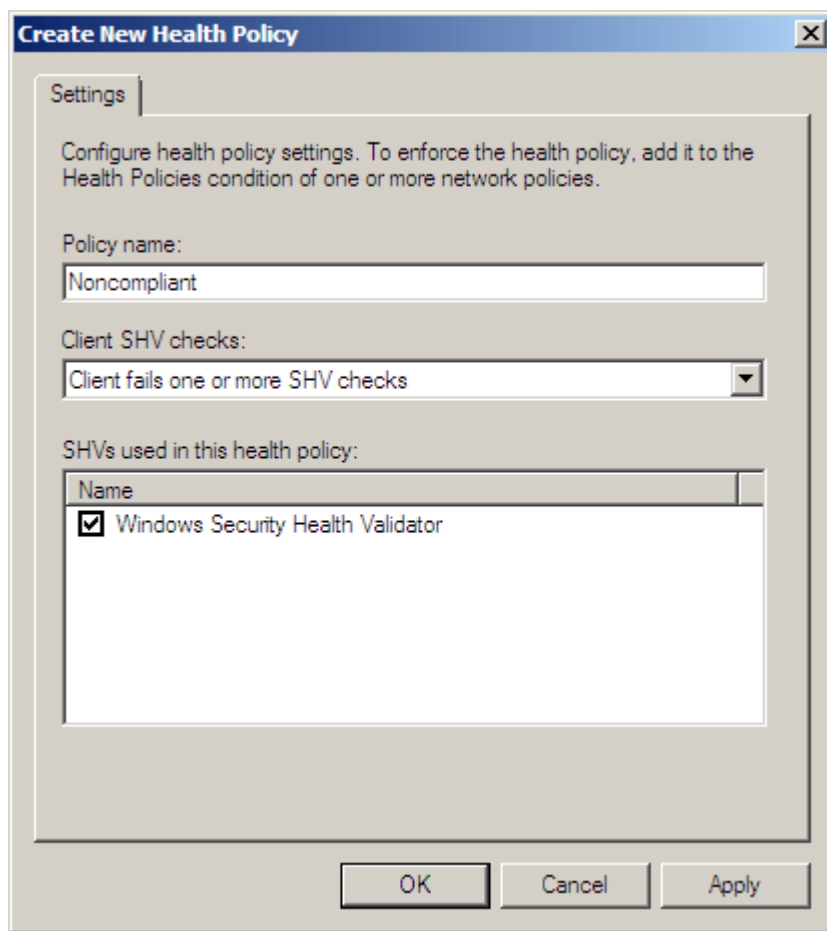
1. Double-click **Network Access Protection**, and then click **System Health Validators**.
2. In the middle pane under **Name**, double-click **Windows Security Health Validator**.
3. In the **Windows Security Health Validator** Properties dialog box, click **Configure**.
4. On this page, configure the Health Checks required. For the purpose of this example only the **Firewall** option is chosen. Clear all check boxes *except A firewall is enabled for all network connections*. You do not need to clear the **Windows Update** check box. See the following example
5. Click **OK** to close the **Windows Security Health Validator** dialog box, and then click **OK** to close the **Windows Security Health Validator Properties** dialog box.



Configure the Health Policies

Health policies define which SHVs are evaluated, and how they are used in validating the configuration of computers that attempt to connect to your network. Based on the results of SHV checks, health policies classify client health status. This test lab defines two health policies, one that corresponds to a compliant health state and one that corresponds to a noncompliant health state.

1. Double-click **Polices**, right-click **Health Policies**, and then click **New**.
2. In the **Create New Health Policy** dialog box, under **Policy Name**, type **NAP_Compliant**.
3. Under **Client SHV checks**, verify that **Client passes all SHV checks** is chosen.
4. Under **SHVs used in this health policy**, select the **Windows Security Health Validator** check box, as shown in the following example, and then click **OK**.
5. Right-click **Health Policies**, and then click **New**.
6. In the **Create New Health Policy** dialog box, under **Policy name**, type **NAP_Noncompliant**.
7. Under **Client SHV checks**, choose **Client fails one or more SHV checks**.
8. Under **SHVs used in this health policy**, select the **Windows Security Health Validator** check box, as shown in the following example, and then click **OK**.

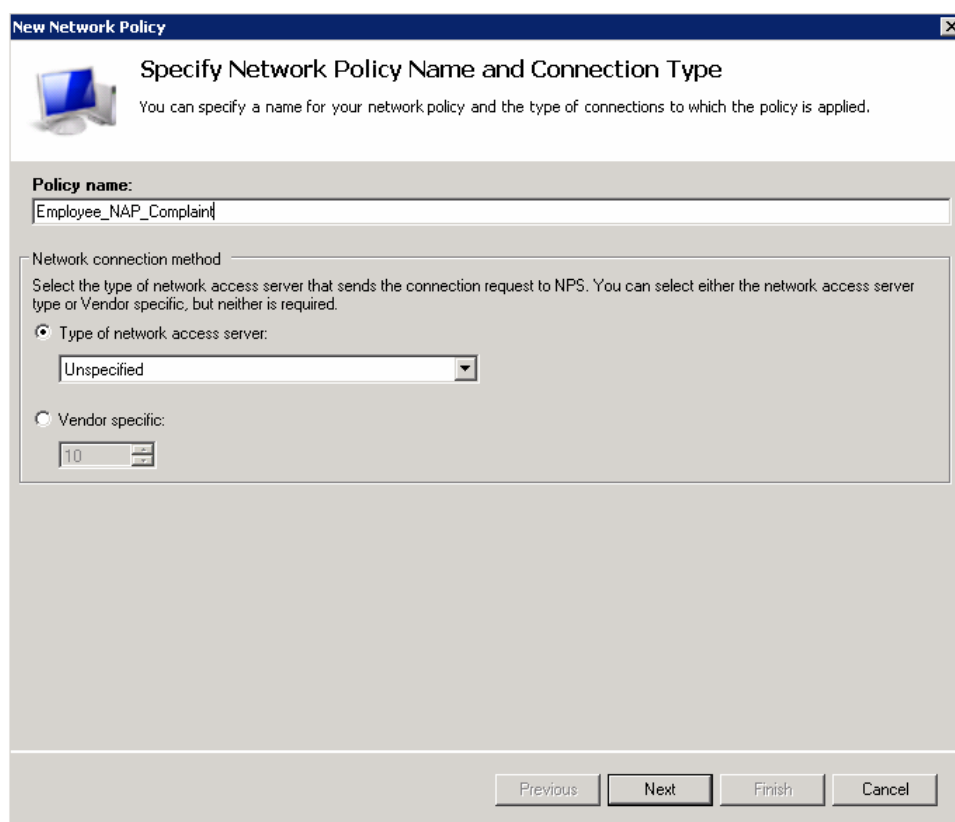


Configure network policies

Network policies evaluate information contained in client authorization requests and grant network access based on the results. Depending on the AD group of the users, the network policies will inform the Aruba Mobility controller to place the corporate users under the **Employee** role and the sales users under the **Sales** role on successful NAP Compliance check. If the client fails compliance check, the client will be placed in the **Quarantine** role and granted limited access to the remediation servers alone. Vendor Specific Attributes will be returned from the NPS to the Aruba Controller which will help the Controller determine the user's role.

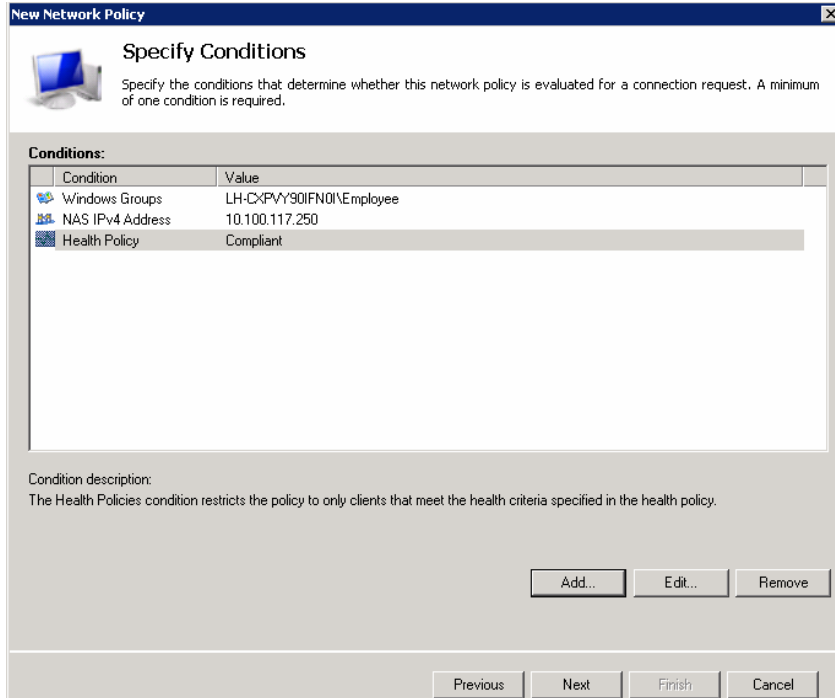
Configuring the network policy for NAP compliant devices for Employees

1. Right click on **Network Policies** and click **New**
2. Enter the Policy Name **Employee_NAP_Compliant** and the click **Next**.



3. In the **Specify Conditions** window, click **Add**
4. Add the **Windows Group** and assign the Windows AD Group corresponding to the Employee user group.
5. Add **NAS IPv4 Address** and enter the Aruba Mobility Controller's Address.

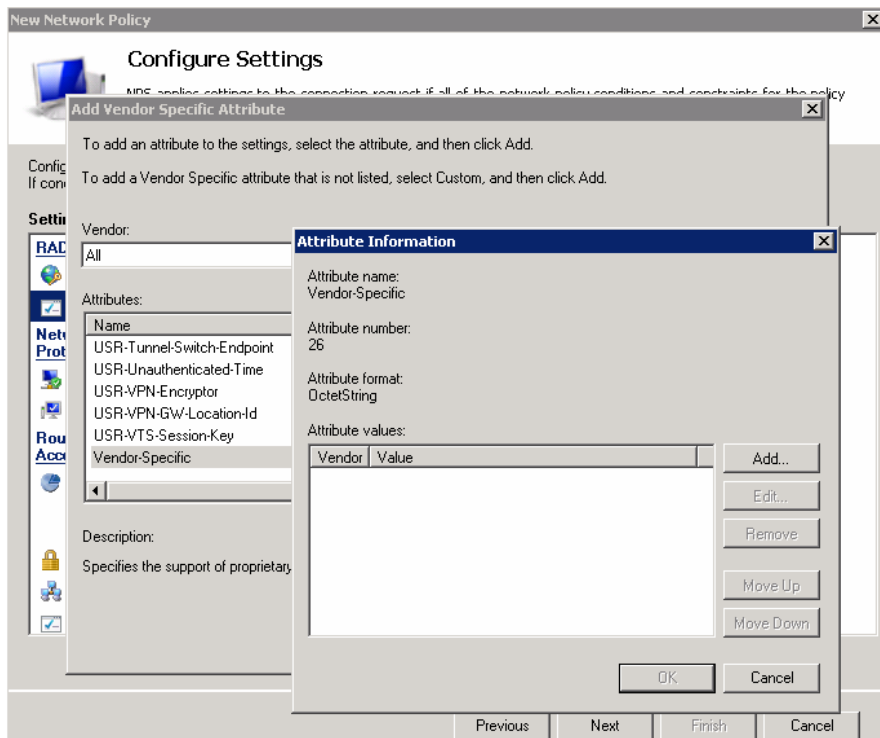
6. Add **Health Policies** and select **Compliant Policy** from the pull down menu.



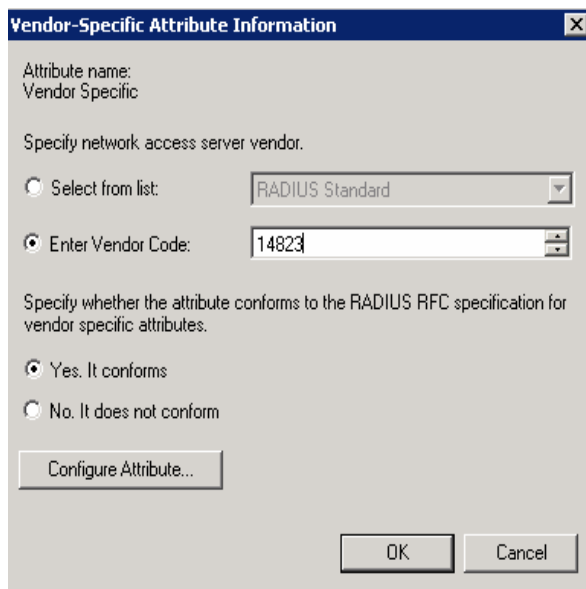
7. Click **Next**.
8. In the **Specify Access Permission** window, verify that **Access granted** is selected.
Note: A setting of *Access granted* does not mean that noncompliant clients are granted full network access. It specifies that clients matching these conditions should continue to be evaluated by the policy
9. Click **Next** three times.

(Continued on next page)

10. In the **Configure Settings** window, click **Vendor Specific**.
11. In the **Add Vendor Specific Attributes** select **Vendor Specific** and click **Add**

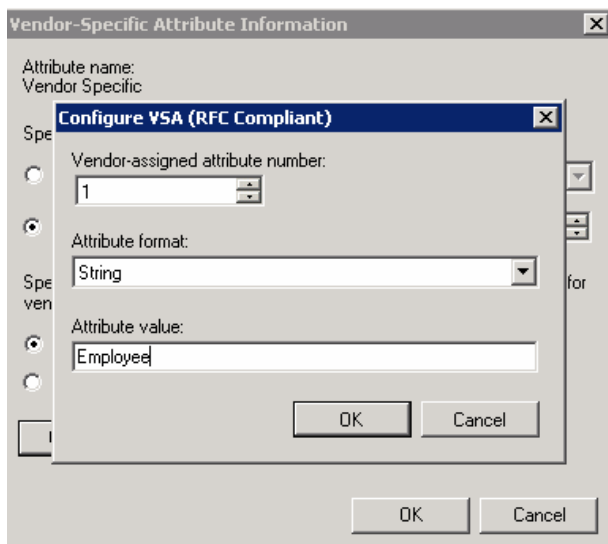


12. Click **Add** , Select the **Enter Vendor Code** option and enter the value **14823** and click on **Configure Attribute**
13. Select the **Yes, It Conforms** radio button.



- Enter **1** for the **Vendor-assigned attribute number**, Select **String** for the Attribute format, enter **Employee** for the **Attribute Value**.

Note: The Attribute Value entered should correspond to a valid role on the Aruba Mobility Controller. The Attribute 14823 corresponds to the user-role setting on the controller.



- Click **OK** three times.
- In the **Configure Settings** window, click **NAP Enforcement**. Choose **Allow limited access** and select **Enable auto-remediation of client computers**. See the following example.
- Click **Finish** to complete configuration of the Employee Compliant network Policy

Configuring the network policy for NAP compliant devices for Sales

- Right click on **Network Policies** and click **New**
- Enter the Policy Name **Employee_NAP_Compliant** and the click **Next**.
- In the **Specify Conditions** window, click **Add**
- Add the **Windows Group** and assign the Windows AD Group corresponding to the Sales user group.
- Add **NAS IPv4 Address** and enter the Aruba Mobility Controller's Address.
- Add **Health Policies** and select **Compliant Policy** from the pull down menu.
- Click **Next**.
- In the **Specify Access Permission** window, verify that **Access granted** is selected.
- Click **Next** three times.
- In the **Configure Settings** window, click **Vendor Specific**.
- In the **Add Vendor Specific Attributes** select **Vendor Specific** and click **Add**
- Click **Add**, select **Enter Vendor Code** and enter the value 14823 and click on **Configure Attribute**.
- Select the **Yes, It Conforms** radio button.
- Enter 1 for the **Vendor-assigned attribute number**, Select **String** for the **Attribute format**, enter Sales for the **Attribute Value**.

Note: The Attribute Value entered should correspond to a valid role on the Aruba Mobility Controller. The Attribute 14823 corresponds to the user-role setting on the controller.

- Click **OK** three times and Close
- In the Configure Settings window, click **NAP Enforcement**. Choose **Allow limited access** and select **Enable auto-remediation of client computers**. See the following example.
- Click **Finish** to complete configuration of the Employee Compliant network Policy

Configuring the network policy for NAP Non compliant devices which would be assigned the Quarantine role on the Aruba controller

1. Right click on **Network Policies** and click **New**
2. Enter the Policy Name **NAP_Non_Compliant** and the click **Next**.
3. In the **Specify Conditions** window, click **Add**
4. Since this applies to all groups, we will not add a group for the Quarantine Policy
5. Add **NAS IPv4 Address** and enter the Aruba Mobility Controller's Address.
6. Add **Health Policies** and select **NAP_Noncompliant Policy** from the pull down menu.
7. Click **Next**.
8. In the **Specify Access Permission** window, verify that **Access granted** is selected.
9. Click **Next** three times.
10. In the **Configure Settings** window, click **Vendor Specific**.
11. In the **Add Vendor Specific Attributes** select **Vendor Specific** and click **Add**
12. Click **Add**, Select the **Enter Vendor Code** option and enter the value 14823 and click on **Configure Attribute**.
13. Enter 1 for the **Vendor-assigned attribute number**, select String for the **Attribute format**, enter **Quarantine** for the **Attribute Value**.
Note: The Attribute Value entered should correspond to a valid role on the Aruba Mobility Controller. The Attribute 14823 corresponds to the user-role setting on the controller.
14. Click **OK** three times.
15. In the **Configure Settings** window, click **NAP Enforcement**. Choose **Allow limited access** and select **Enable auto-remediation of client computers**. See the following example.
16. Click **Next** and then **Finish** to complete configuration of the Employee Compliant network Policy

Configuring NPS on the Client Device

Pre-requisites

The client should support Vista or XP.

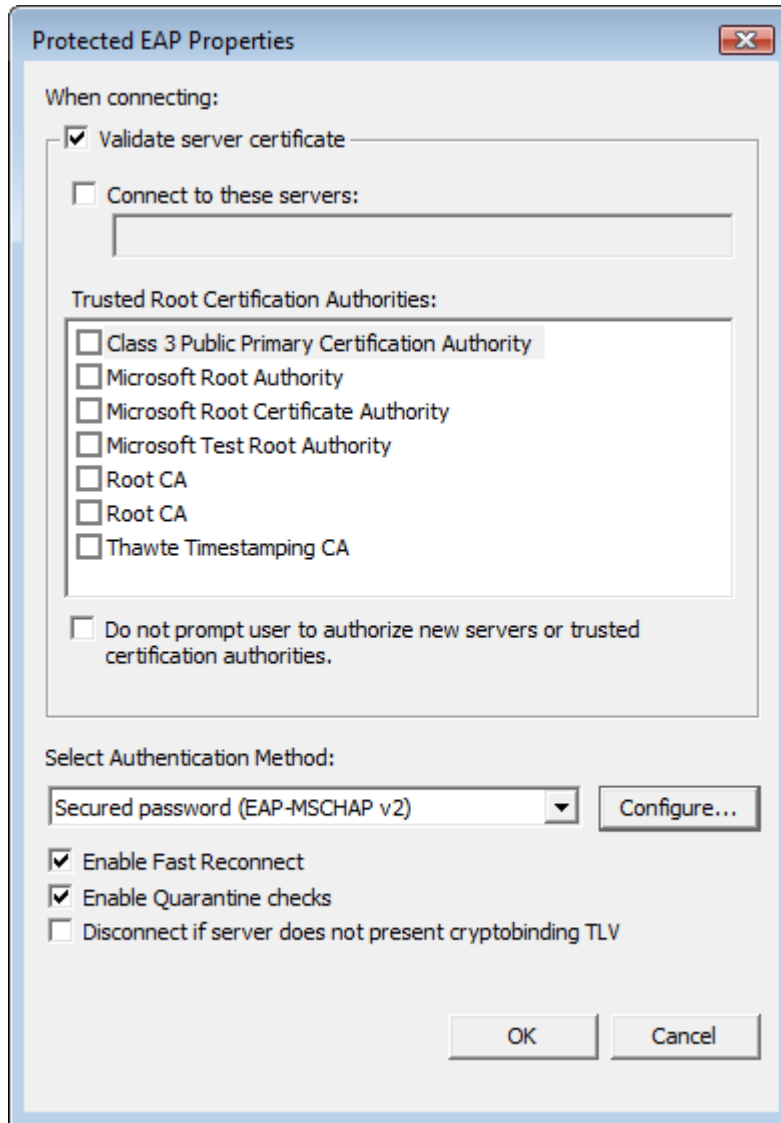
Configuration Procedure

1. Join the client to the right domain.
2. Enable Network Access Protection Agent
 - a. Click **Start**, click **All Programs**, click **Accessories**, and then click **Run**.
 - b. Next to **Open**, type **services.msc**, and then press ENTER.
 - c. In the list of services, right-click **Network Access Protection Agent**, and then click **Properties**.
 - d. Next to **Startup type**, choose **Automatic**.
 - e. Under **Service status**, click **Start**, wait for the service to start, and then click **OK**.
3. Enable the EAP enforcement client and Security Center
 - a. Click **Start**, click **All Programs**, click **Accessories**, and then click **Run**.
 - b. Next to **Open**, type **mmc**, and then press ENTER.
 - c. On the **File** menu, click **Add/Remove Snap-in**.
 - d. Click **NAP Client Configuration**, and then click **Add**.
 - e. In the **NAP Client Configuration** dialog box, click **OK** to accept the default selection, **Local computer (the computer on which this console is running)**.
 - f. Click **OK** to go back to the previous page.
 - g. Double click on **NAP Client Configuration** under **Console Root**.
 - h. Click on **Enforcement Clients**.
 - i. In the middle pane, right-click **EAP Quarantine Enforcement Client**, and then click **Enable**.
 - j. Close the console window
 - k. Click **No** when prompted to save the console settings
 - l. Navigate to the **control panel** and double click on **Security**.
 - m. Ensure that **Windows Firewall** is **enabled**.
4. Configure the Authentication Methods
 - a. Click **Start**, right-click **Network**, and then click **Properties**.
 - b. Click **Manage network connections**.
 - c. Right-click **Local Area Connection** and then click **Properties**.
 - d. Click the **Authentication** tab, and verify that **Enable IEEE 802.1X authentication** is selected.

- e. Click **Settings**.

In the **Protected EAP Properties** dialog box, verify that the following check boxes are selected, as shown in the following example:

- Validate server certificate
- Enable Fast Reconnect
- Enable Quarantine checks



- Click **Configure**, verify that **Automatically use my Windows logon name and password (and domain if any)** is selected, and then click **OK**.
- Click **OK**, and then click **OK** again.
- Restart the computer.

Summary

The joint solution from Microsoft and Aruba offers customers a defense solution that acts at multiple layers and focuses on the health and policies of end devices. This ensures that only healthy endpoints connect to the network, effectively reducing unwanted health risks to networks assets.

About Aruba Networks, Inc.

Aruba securely delivers the enterprise network to users, wherever they work or roam, with user-centric networks that significantly expand the reach of traditional port-centric networks. User-centric networks integrate adaptive WLANs, identity-based security, and application continuity services into a cohesive, high-performance system that can be easily deployed as an overlay on top of existing network infrastructure. Adaptive WLANs deliver high-performance, follow-me connectivity so users are always within reach of mission-critical information. Identity-based security associates access policies with users, not ports, to enable follow-me security that is enforced regardless of access method or location. Application continuity services enable follow-me applications that can be seamlessly accessed across WLAN and cellular networks. The cost, convenience, and security benefits of user-centric networks are fundamentally changing how and where we work. Listed on the NASDAQ and Russell 2000® Index, Aruba is based in Sunnyvale, California, and has operations throughout the Americas, Europe, Middle East, and Asia Pacific regions. To learn more, visit <http://www.arubanetworks.com>.

Guide to Abbreviations

Abbreviation	Meaning
AM	Air Monitor
AP	Access Point
WLAN	LAN
NAP	Network Access Protection
NPS	Network Policy Server
SHV	System Health Validators
VSA	Vendor Specific Attributes

© 2007 Aruba Networks, Inc. All rights reserved. Aruba Networks and Aruba Mobile Edge Architecture are trademarks of Aruba Networks, Inc. All other trademarks or registered trademarks are the property of their respective holders. Specifications are subject to change without notice.

DIG_MSFNAP_US_070813