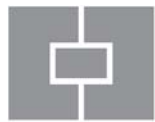


# SOPHOS



sophos **nac**

ADVANCED

Integration with Wireless  
Access Points



Copyright © 2011 Sophos Limited. All rights reserved. No part of this publication may be reproduced, stored in retrieval system, or transmitted, in any form or by any means electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the licence terms or you otherwise have the prior permission in writing of the copyright owner.

Sophos and Sophos Anti-Virus are registered trademarks of Sophos Limited. All other product and company names are trademarks or registered trademarks of their respective owners.

Document version 3.2  
Published January 2011

## Table of Contents

Sophos NAC Integration with Wireless Access Points .....	4
Configuring the WAP for Sophos NAC Integration through RADIUS Authentication .....	4
Using Wireless Encryption Protocol (WEP) .....	6
Using Wi-Fi Protected Access (WPA) .....	9
Connecting to the AP .....	11
Configuring the WAP for Access with Multiple SSIDs .....	11
Connecting to the AP with Multiple SSIDs.....	15

## Sophos NAC Integration with Wireless Access Points

This document provides information on integrating Sophos NAC Advanced with Wireless Access Points (WAPs) so that authentication includes a Sophos NAC compliance assessment.

This document describes and tests the following two end-to-end scenarios:

- **Scenario One:** A machine is not granted access to the network via the WAP until it passes the Sophos NAC compliance assessment.
- **Scenario Two:** A non-compliant machine associates with a specific SSID which provides limited network access. Upon passing a Sophos NAC compliance assessment, the machine can associate with a different SSID which provides full network access.

This document only tests the Cisco Aironet 1200 WAP with Sophos NAC. This WAP supports authentication through RADIUS, a feature which is required for any access point (AP) that integrates with Sophos NAC. Additionally, this WAP supports the creation of multiple SSIDs, which is required for scenario two. WAPs from other manufacturers are also supported by Sophos NAC, but they must support RADIUS authentication and multiple SSIDs.

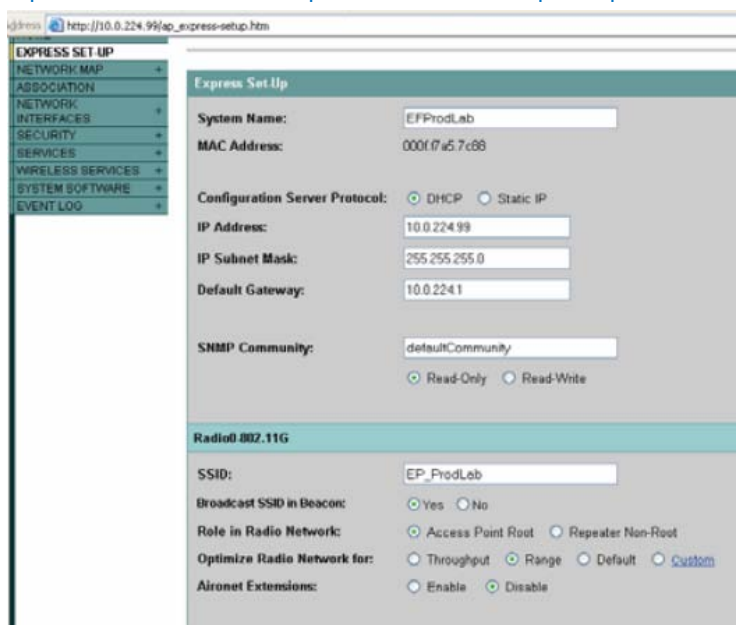
## Configuring the WAP for Sophos NAC Integration through RADIUS Authentication

To integrate Sophos NAC with a WAP, the AP must first be configured on the network and set up to accept RADIUS authentication. Complete the following steps to enable Sophos NAC support in a wireless AP environment.

1. Follow the steps in Chapter 3, “Configuring the Access Point for the First Time” in the document *Cisco Aironet 1200 Series Access Point Hardware Installation Guide*. Minimally, the AP should be configured with a system name, IP address, and SSID like the example that follows.

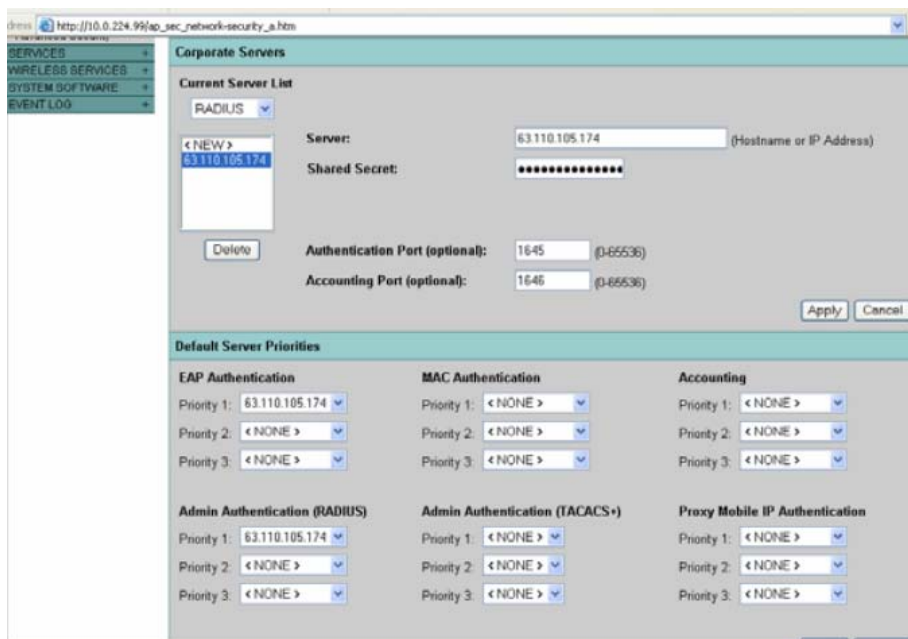
**Note:** This chapter is available online.

[http://www.cisco.com/en/US/products/hw/wireless/ps430/products\\_installation\\_guide\\_chapter09186a00801cfb3e.html](http://www.cisco.com/en/US/products/hw/wireless/ps430/products_installation_guide_chapter09186a00801cfb3e.html)

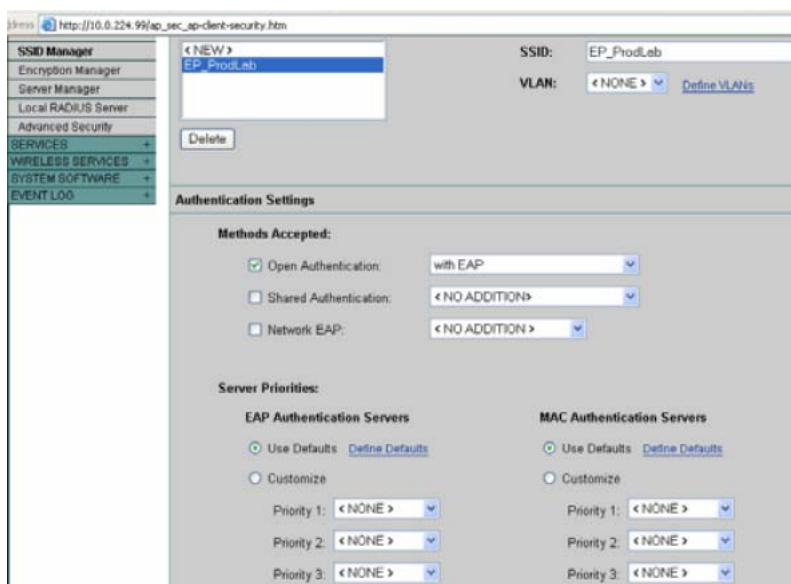


2. From the **Security** menu, select **Server Manager** to open the Security: Server Manager page.
3. From the **Corporate Servers** area, select **RADIUS** from the **Current Server List** box, type the IP address and shared secret for the Sophos Compliance Application Server, and click **Apply** in this area.

4. From the **Default Server Priorities** area for **EAP Authentication** and **Admin Authentication (RADIUS)**, select the **RADIUS server IP address** you added in step 3 above.
5. Click **Apply** in this area. The following is a sample page.

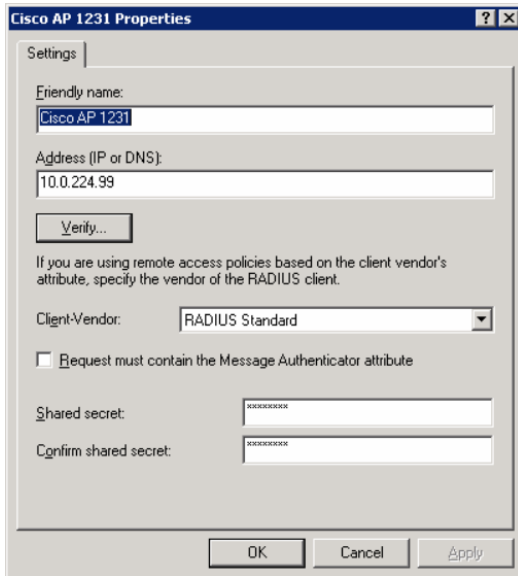


6. From the **Security** menu, select **SSID Manager** to open the Security: SSID Manager page.
7. Select the **SSID** from the **Current SSID List**.
8. In the **Methods Accepted** area, select the **Open Authentication** check box, and then select **with EAP** from the list box.
9. In the **EAP Authentication Servers** area, verify that the **Use Defaults** option button is selected to use the RADIUS Servers set up in steps 2 through 5.



10. Click **Apply** in the **General Settings** area to save the changes.

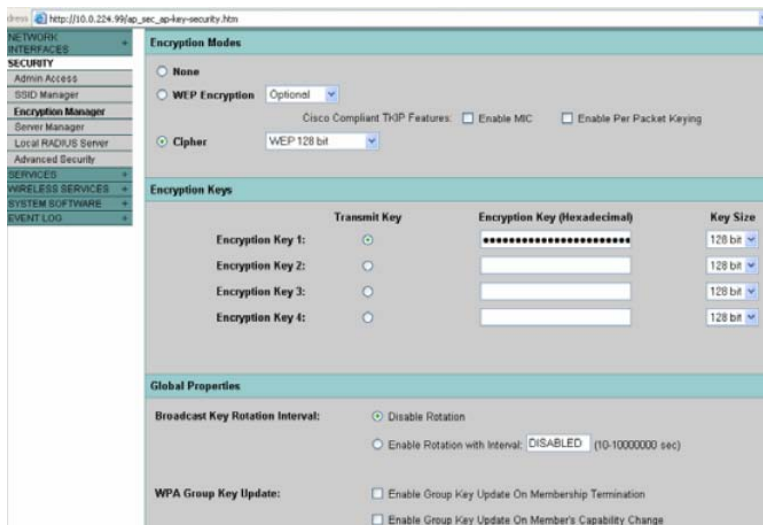
11. Set up Sophos NAC as a RADIUS proxy so that RADIUS requests from the AP are sent through Sophos NAC on their way to IAS. For more information, see the *Sophos NAC Advanced Installation Guide*. The IAS entry should be configured as follows. The shared secret must be the same as the shared secret specified in step 3 above.



## Using Wireless Encryption Protocol (WEP)

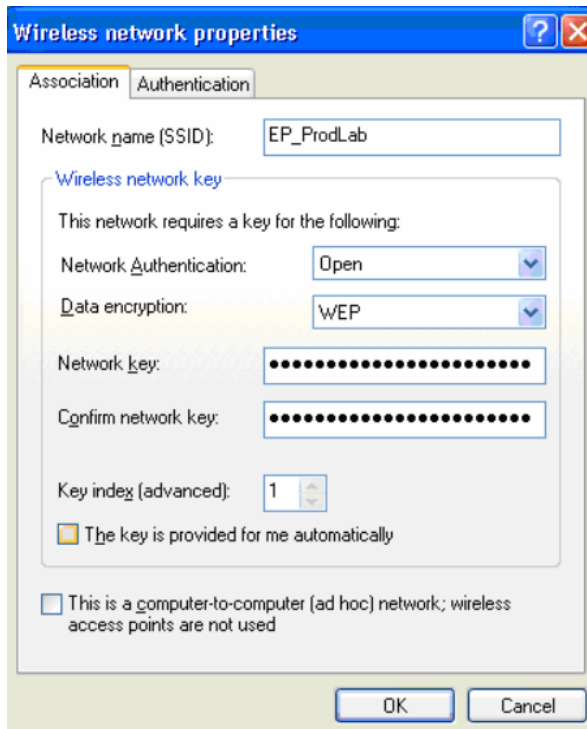
To enable WEP encryption on the AP:

1. From the **Security** menu, select **Encryption Manager** to open the Security: Encryption Manager page.
2. Select the **Cipher** option button, and then select **WEP 128 bit** from the list box.
3. Select the **Encryption Key 1 Transmit Key** option button, and then type a hexadecimal key of the appropriate length.
4. Click **Apply** to save these changes.

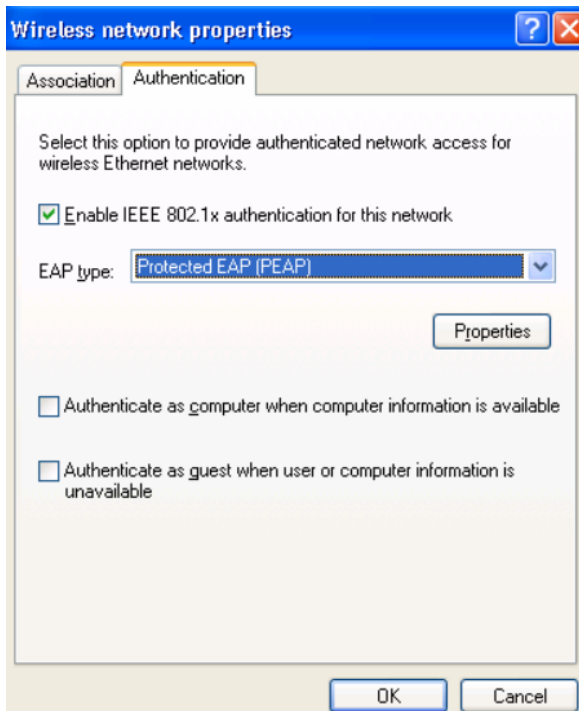


5. Configure the properties for the wireless network on the client to connect to the AP using WEP authentication.

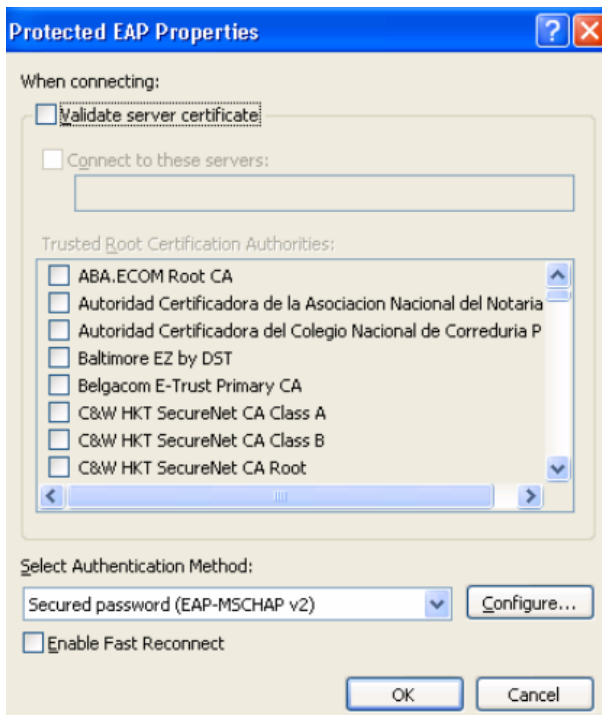
6. On the **Association** tab, select **Open** from the **Network Authentication** list box and **WEP** from the **Data encryption** list box. Type the network key that was entered in step 3 above.



7. On the **Authentication** tab, verify that the **Enable IEEE 802.1x authentication for this network** check box is selected, and then select **Protected EAP (PEAP)** from the **EAP type** list box.



8. Click **Properties** to set up the Protected EAP Properties. Select **Secured password (EAP-MSCHAP v2)** from the **Select Authentication Method** list box.  
**Note:** The **Validate server certificate** check box may be checked if the network is using certificates.



9. Click **Configure** to display the MSCHAPv2 properties. This window determines whether or not the Windows logon is automatically used as the userid and password for RADIUS authentication. If the check box is not selected, the user is prompted for a logon and password. Otherwise, the Windows logon is passed to the RADIUS server for authentication.

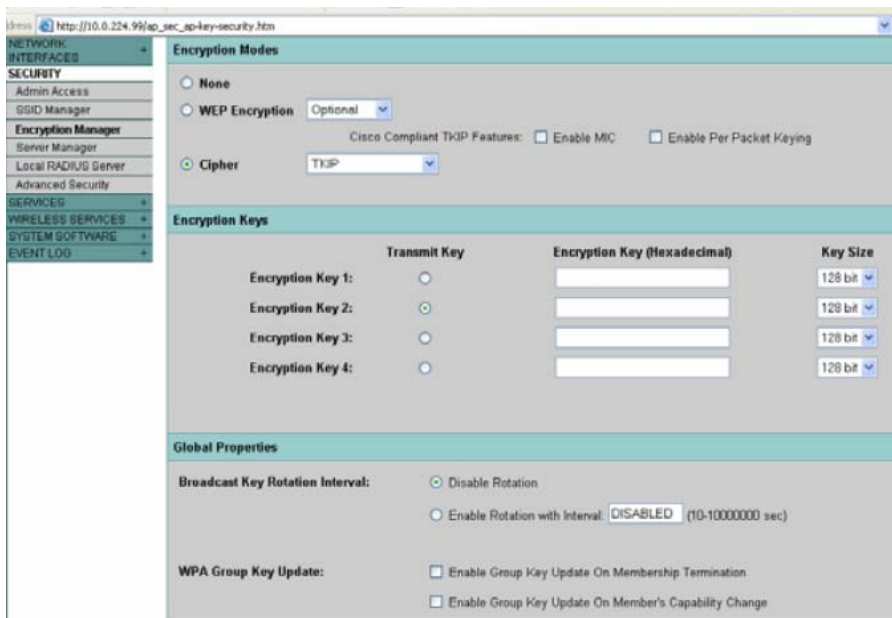


10. Click **OK** three times, once on each **Properties** window, to save the wireless network settings on this machine.

## Using Wi-Fi Protected Access (WPA)

To enable WPA on the WAP:

1. From the **Security** menu, select **Encryption Manager** to open the Security: Encryption Manager page.
2. Select the **Cipher** option button, and then select **TKIP** from the list box.
3. Clear the value in **Encryption Key 1** field, and then select the **Encryption Key 2** option button.
4. Click **Apply** to save these changes. The following is a sample page.



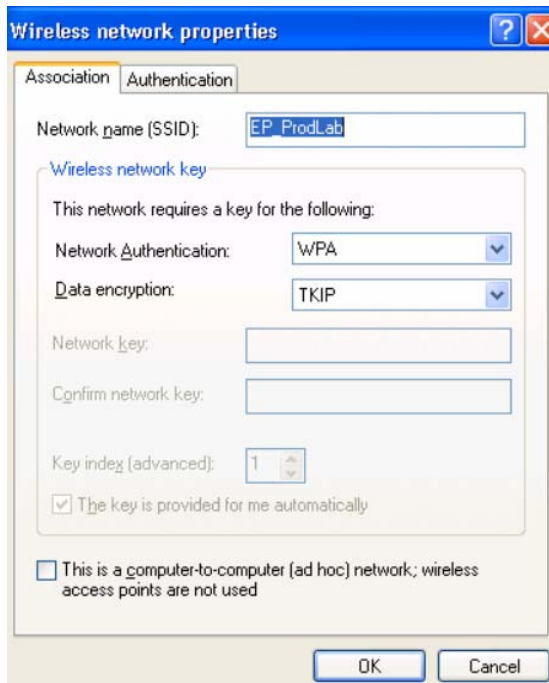
5. From the **Security** menu, select **SSID Manager** to open the Security: SSID Manager page.
6. Select the appropriate **SSID** from the **Current SSID** list.
7. In the **Authenticated Key Management** area, select **Mandatory** from the **Key Management** list box, and then click the **WPA** check box.



8. Click **Apply** to save the changes.

9. Configure the properties for the wireless network on the client to connect to the AP using WPA authentication. The following windows are from Windows XP SP2.

**Note:** On Windows XP SP1, the update Q815485 must be installed to support WPA. This update is available from <http://www.microsoft.com/downloads/details.aspx?FamilyID=009d8425-ce2b-47a4-abec-274845dc9e91&DisplayLang=en>



## Connecting to the AP

The user must first connect to the physical (wired) LAN and authenticate through Sophos NAC. If the compliance assessment passes, the user can disable and re-enable the wireless NIC, connect through the WAP, using RADIUS configured as described above, and disconnect from the wired network.

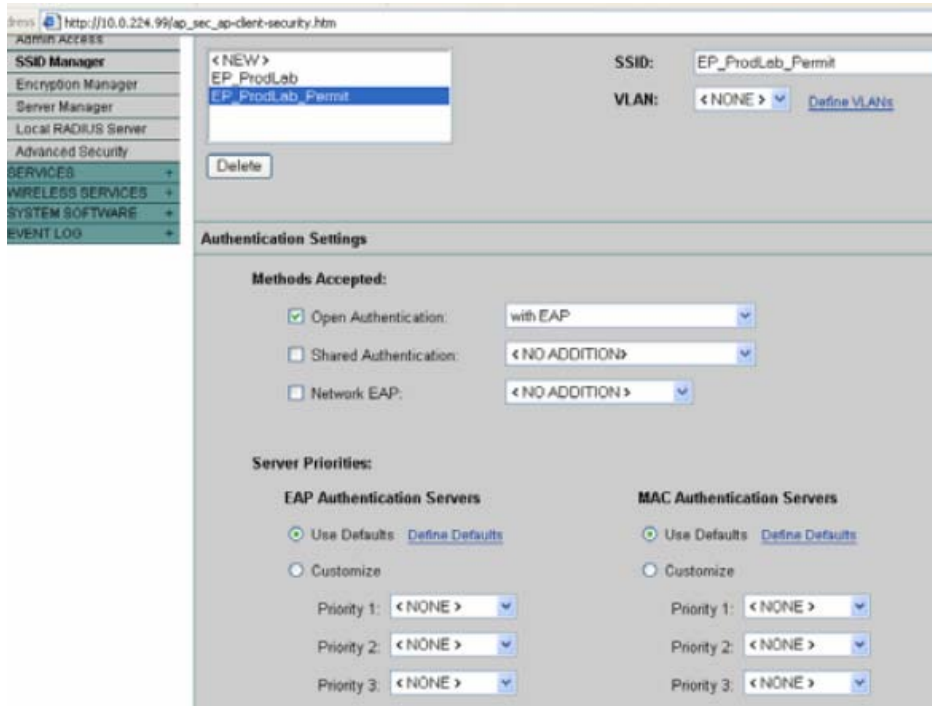
## Configuring the WAP for Access with Multiple SSIDs

The Cisco Aironet offers a feature that enables WAP to support multiple SSIDs. Each SSID can be assigned to a separate VLAN. Additionally, Cisco supports a vendor-specific attribute where the SSID is sent with the RADIUS request. Upon authentication through the RADIUS server, the machine associates with the SSID specified in the request.

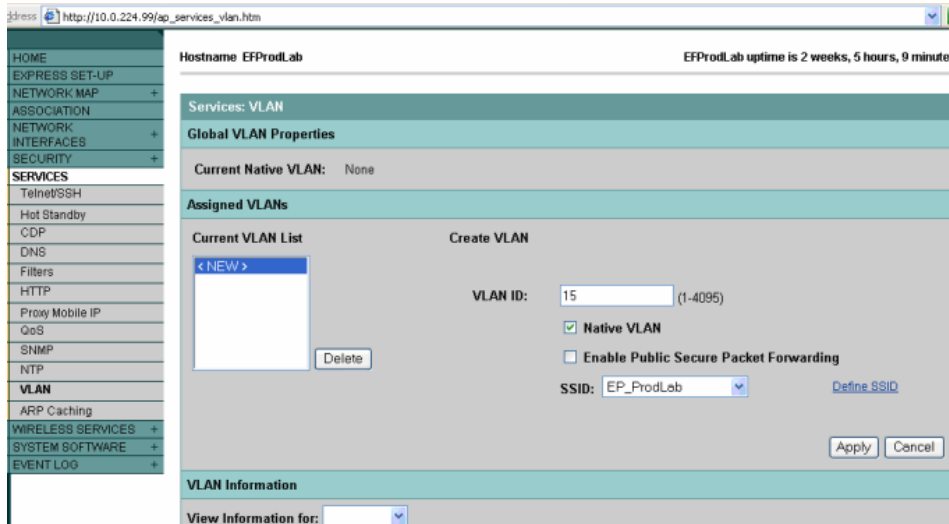
Combining these features enables Sophos NAC to force a non-compliant machine to associate with a certain SSID. This SSID possesses limited network access only to the authentication and remediation servers. Machines that have passed the required assessments are permitted access and associated with a different SSID. This SSID is granted full access to the network.

The following steps describe a method of configuring the WAP to support Sophos NAC enforcement with multiple SSIDs.

1. In the SSID Manager page, create a second SSID that is used to permit access. Use the same authentication settings as described in steps 7-10 on page 5.



2. In the Services: VLAN page, specify a VLAN in the network, and then select the **SSID** from the list box that wireless connections will associate with when the machine is not in policy. Select the **Native VLAN** check box. Click **Apply** to save the changes.



3. Repeat the previous step with the VLAN that is associated with all (permitted) access. Deselect the **Native VLAN** check box. Click **Apply** to save the changes.
4. The Sophos Compliance Application Server must be configured to send the correct RADIUS vendor specific attributes. Create a RADIUS Compliance Setting with the IP Address pointing to the WAP.

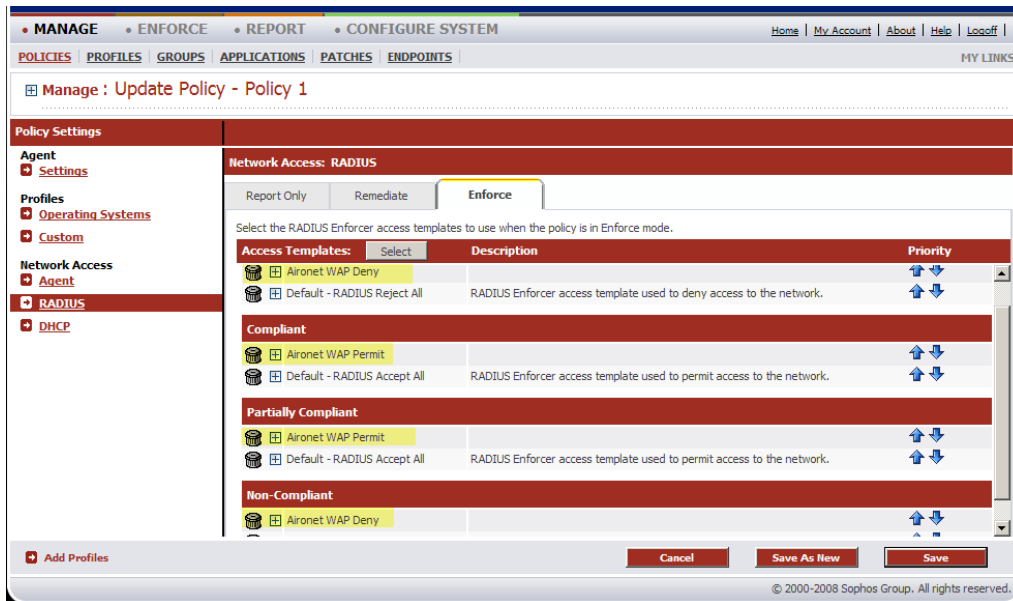
- From the Sophos Compliance Manager RADIUS Enforcer area, create a new RADIUS template, Select **Accept** from the **Network Access** list box, and specify the IP address of the WAP for the RADIUS Client IP Address. Select **Vendor-Specific** from the **Type** list box. The Attribute Number is automatically be set to **26** (the RADIUS standard for vendor-specific attributes). Type an appropriate Attribute Name. Type the Cisco vendor-ID of **9** in the **Vendor Code** field. Type the cisco-avpair of **1** for **Vendor Subattribute** field. Select **Text** from the **Format** list box. Type the **ssid=<name>**, where <name> is the SSID for the permit access exactly as it was specified in the WAP configuration, in the **Value** field, and then click **Save** to save the template.

The screenshot shows the 'Update RADIUS Enforcer Access Template' page in the Sophos Compliance Manager. The 'Name' field is 'Aironet WAP Permit', 'Version' is 5, and 'Network Access' is set to 'Accept'. Under 'RADIUS Client IP Addresses', '10.0.224.99' is listed. In the 'RADIUS Attributes' section, a new attribute 'WAP Permit' is being configured with the following properties: Type: Vendor-Specific, Name: WAP Permit, Number: 26, Vendor Code: 9, Vendor Subattribute: 1, Format: Text, and Value: ssid=EP\_ProdLab\_Permit. The 'Template Compliance States' are set to 'Compliant' and 'Partially Compliant'.

- Repeat the previous step to create an Aironet WAP Deny template for the default SSID, which is used when the machine is not compliant.

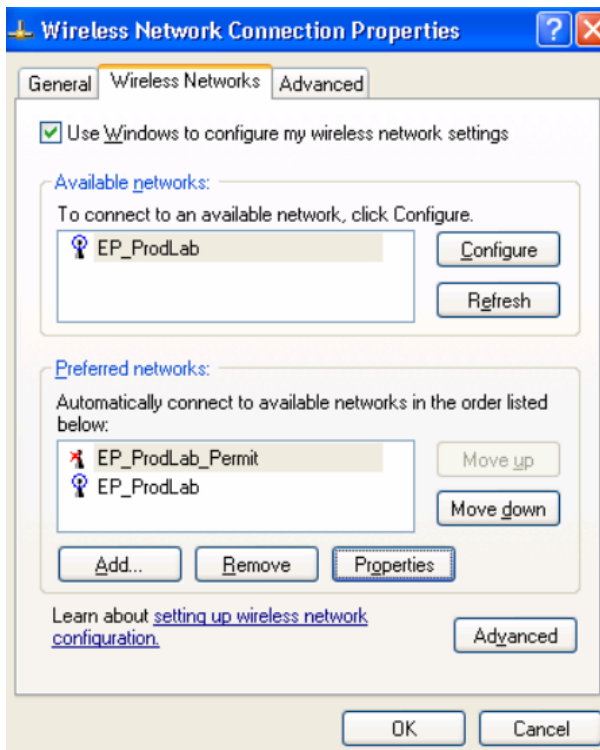
The screenshot shows the 'Update RADIUS Enforcer Access Template' page in the Sophos Compliance Manager. The 'Name' field is 'Aironet WAP Deny', 'Version' is 3, and 'Network Access' is set to 'Reject'. Under 'RADIUS Client IP Addresses', '10.0.224.99' is listed. In the 'RADIUS Attributes' section, a new attribute 'WAP Deny' is being configured with the following properties: Type: Vendor-Specific, Name: WAP Deny, Number: 26, Vendor Code: 9, Vendor Subattribute: 1, Format: Text, and Value: ssid=EP\_ProdLab. The 'Template Compliance States' are set to 'Non-Compliant'.

7. Apply the RADIUS templates to the policy so that they get used in a higher priority than the default templates.



8. Aside from having the Sophos Compliance Agent installed, any machines that need to connect to this wireless network must also add the default and permit SSIDs to the **Wireless Network Connection Properties** dialog box.

**Note:** Verify that the properties for the wireless networks match the configuration of the SSID on the AP.



## **Connecting to the AP with Multiple SSIDs**

When a non-compliant machine first attempts to connect to the WAP, Sophos NAC recognizes that the machine is not compliant and sends the attribute that forces the machine to connect to the default SSID. That SSID must have connectivity to the Sophos Compliance Application Server so that the user can use the Sophos Compliance Agent to establish compliance. After the Compliance Agent verifies compliance, the user can then disable or disconnect the wireless network and re-enable the network to associate with the permitted (all access) SSID.