

SOPHOS



sophos **nac**

ADVANCED

802.1x Dynamic VLAN Assignment



Copyright © 2010 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 December 2010

Table of Contents

802.1x Dynamic VLAN Configuration	4
Cisco Switch Supported Options	4
Cisco Switch Configuration	5
Server Settings for Network Policy Server (Windows Server 2008)	6
Server Settings for Internet Authentication Service (IAS) (Windows Server 2003)	9
Compliance Manager Settings	12
Microsoft Supplicant Settings (Protected EAP Protocol)	19
Microsoft Supplicant Settings (Protected EAP Protocol) for Windows XP SP3+	21
Microsoft Supplicant Settings (MD5-Challenge Protocol)	23
Juniper Networks Odyssey Access Client Supplicant	25
Cisco Secure Services Client Supplicant	29
Appendix A: Sample Cisco 802.1x Catalyst 2950 Configuration	37

802.1x Dynamic VLAN Configuration

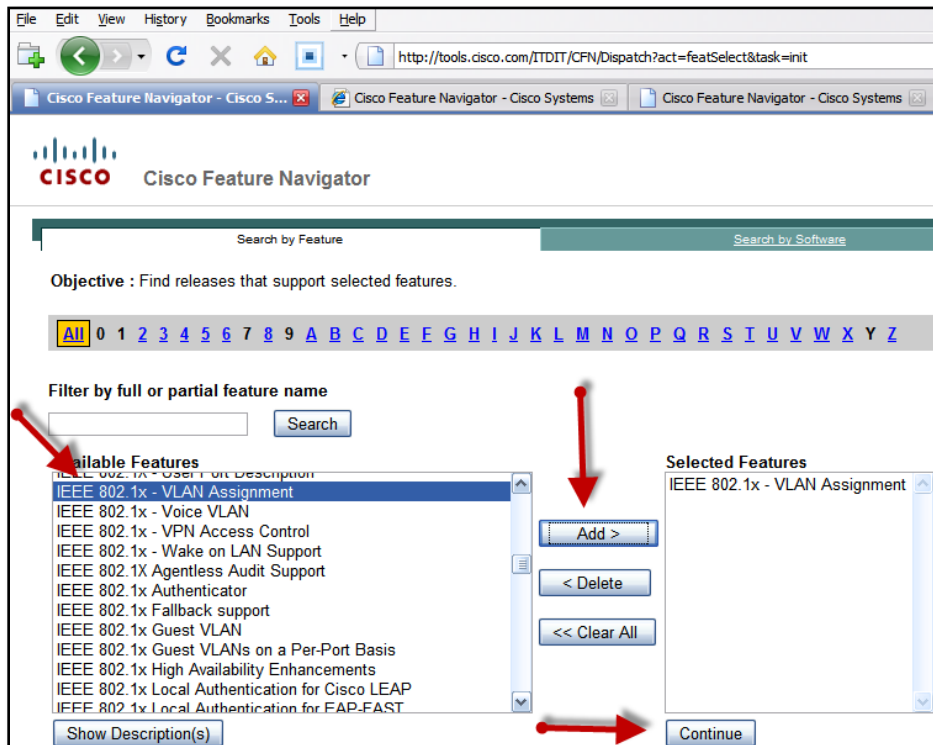
This document provides information on integrating Sophos NAC Advanced in an environment that includes switches set up to support the 802.1x IEEE protocol. The information in this document has been tested in an end-to-end scenario. Sophos testing information concludes at the point where the 802.1x authentication is complete and the client is placed on the correct VLAN.

In this document, three virtual LANs (VLANs) are created: guest, quarantine, and all access. Configurations involving only two VLANs are also possible and supported, but the three VLAN configurations are contained in this document.

Cisco Switch Supported Options

The Cisco® switch must support **IEEE 802.1x – VLAN Assignment** to work correctly with Sophos NAC Advanced. This feature is usually found in the Enhanced versions of the Cisco Catalyst IOSs. Some switches have different hardware to support “enhanced” functionality; so, you should ensure the switch supports this prior to going through the rest of the process. If you do not know if your Cisco switch supports this feature, you can use the Cisco Feature Navigator® to confirm this.

1. Locate the Cisco Feature Navigator tool. The location of the tool as of publication is: <http://tools.cisco.com/ITDIT/CFN/Dispatch?act=featSelect&task=init>.
2. From the Available Features section, select **IEEE 802.1x – VLAN Assignment**, and click **Add**.
3. Click **Continue**.



- Search by any CatOS or IOS version to see if your current image is listed in the Image Name section. If it is, your current Cisco software/hardware should work with Sophos NAC Advanced.

Note: If you have hardware from another vendor, consult their materials to confirm if the hardware supports this feature.

IEEE 802.1x - VLAN Assignment

Software: IOS

Major Release: Select One

Release: All Releases

Platform: CAT2950

Feature Set/License: All Feature Sets/Licenses

Search Results

Cisco IOS quick pick latest Releases

GD Release

LD Release

ED Release: 12.1(22)EA12

MD Release

Release	Feature Set/License	Image Name	DRAM	Flash
12.1(22)EA12	C2950 EI AND SI IOS CRYPTO IMAGE	c2950-i6k2l2q4-mz.121-22.EA12.bin	16	8
12.1(22)EA12	C2950 EI AND SI IOS IMAGE	c2950-i6q4l2-mz.121-22.EA12.bin	16	8
12.1(22)EA11	C2950 EI AND SI IOS CRYPTO IMAGE	c2950-i6k2l2q4-mz.121-22.EA11.bin	16	8
12.1(22)EA11	C2950 EI AND SI IOS IMAGE	c2950-i6q4l2-mz.121-22.EA11.bin	16	8
12.1(22)EA10a	C2950 EI AND SI IOS CRYPTO IMAGE	c2950-i6k2l2q4-mz.121-22.EA10a.bin	16	8
12.1(22)EA10a	C2950 EI AND SI IOS IMAGE	c2950-i6q4l2-mz.121-22.EA10a.bin	16	8
12.1(22)EA10	C2950 EI AND SI IOS CRYPTO IMAGE	c2950-i6k2l2q4-mz.121-22.EA10.bin	16	8
12.1(22)EA10	C2950 EI AND SI IOS IMAGE	c2950-i6q4l2-mz.121-22.EA10.bin	16	8
12.1(22)EA9	C2950 EI AND SI IOS CRYPTO IMAGE	c2950-i6k2l2q4-mz.121-22.EA9.bin	16	8
12.1(22)EA9	C2950 EI AND SI IOS IMAGE	c2950-i6q4l2-mz.121-22.EA9.bin	16	8
12.1(22)EA8a	C2950 EI AND SI IOS CRYPTO IMAGE	c2950-i6k2l2q4-mz.121-22.EA8a.bin	16	8
12.1(22)EA8a	C2950 EI AND SI IOS IMAGE	c2950-i6q4l2-mz.121-22.EA8a.bin	16	8
12.1(22)EA8	C2950 EI AND SI IOS CRYPTO IMAGE	c2950-i6k2l2q4-mz.121-22.EA8.bin	16	8
12.1(22)EA8	C2950 EI AND SI IOS IMAGE	c2950-i6q4l2-mz.121-22.EA8.bin	16	8

Cisco Switch Configuration

The following settings were used to configure the Cisco 802.1x Catalyst 2950 switch. Other switches may use different commands.

- Follow the instructions for the switch to create the three virtual LANs (VLANs). For the purpose of this document, they are referred to as **guest**, **quarantine**, and **all access**.
- The location of the RADIUS server was set to point to the Compliance Application Server. For example: `radius-server host <app server IP> auth-port 1812 acct-port 1813 key <password>`, where `<app server IP>` is the IP address of the Compliance Application Server and `<password>` is the RADIUS server key.

The following is an example of a basic switch configuration on a Cisco 802.1x Catalyst 2950 switch. The switch/router should be working with 802.1x prior to installing Sophos NAC Advanced. The following example is for reference only.

Configuration	Explanation
aaa new-model	Enables AAA/RADIUS.
aaa authentication dot1x default group radius	Creates an 802.1x "method list".
aaa authorization network default group radius	Authorizes RADIUS to change the VLAN dynamically.
radius-server host 10.2.3.1 auth-port 1812 acct-port 1813	Identifies the Compliance Application Server IP address and authentication/accounting ports.
radius-server retransmit 3	Tries 3 times before it times out.
radius-server key MyRadiusKey	Identifies the RADIUS server authorization key.
dot1x system-auth-contro	Turns on 802.1x authentication on the switch and is required as of IOS 12.1(14), not required for previous IOS versions.

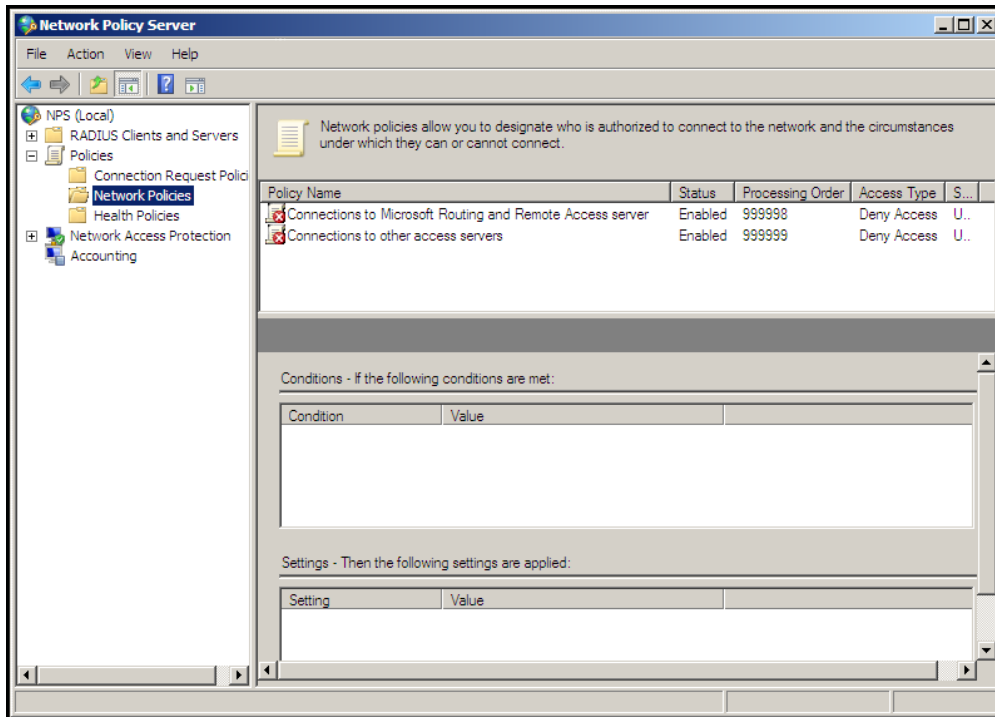
Configuration	Explanation
Interface FastEthernet0/1	
switchport access vlan 5	Defines the VLAN the port belongs to.
switchport mode access	Turns off VLAN “dynamic” mode. No trunking allowed.
dot1x port -control auto	Enables 802.1x on a specific port.
dot1x guest-vlan 66	(Optional setting). Defines what VLAN to assign to clients that fail authentication 3 times. Otherwise, the port closes.
dot1x host-mode multi-host	Allows both a host and a voice device to be authenticated on an IEEE 802.1x-authorized port.

Server Settings for Network Policy Server (Windows Server 2008)

If you are using Windows Server 2008, use Network Policy Server to configure the DHCP server with IP scopes corresponding to the various VLANs. For example, the guest VLAN is 10.0.181.0/24, the all-access VLAN is 10.0.182.0/24, and the quarantine VLAN is 10.0.183.0/24.

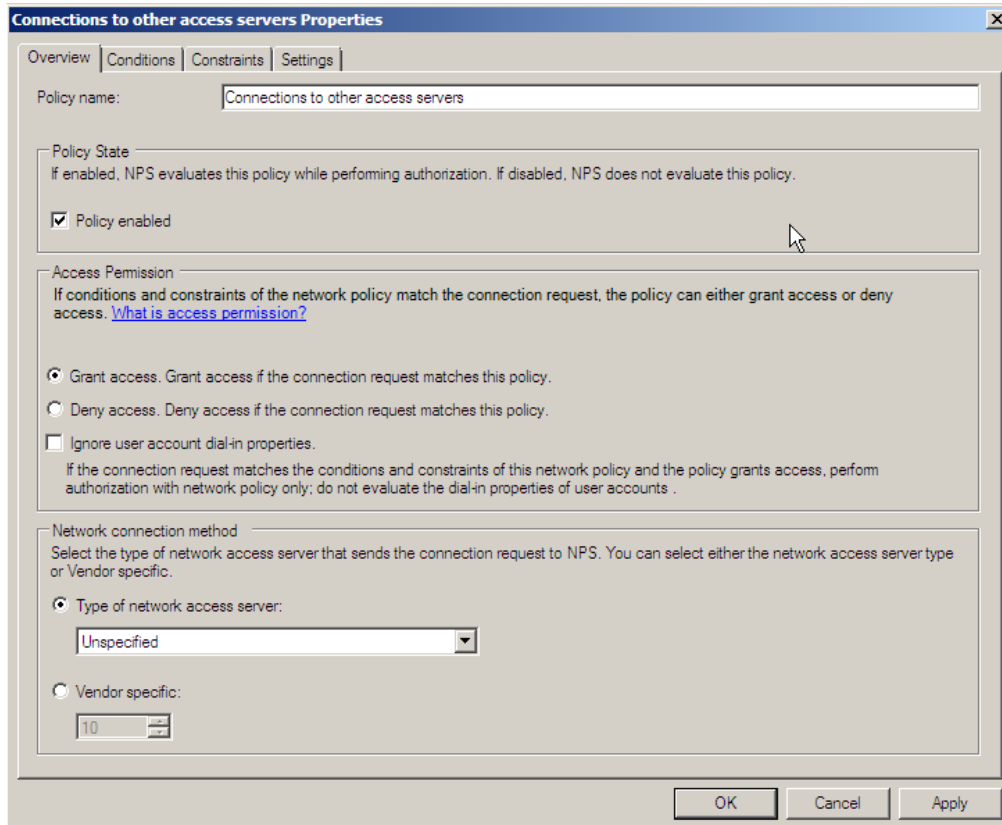
1. On the machine where Network Policy Server is installed, configure the remote access policies. From the Start menu, select **Administrative Tools ► Network Policy Server**.
2. Under Policies, click **Network Policies**.

Note: Either create a new network policy, or use an applicable existing network policy.



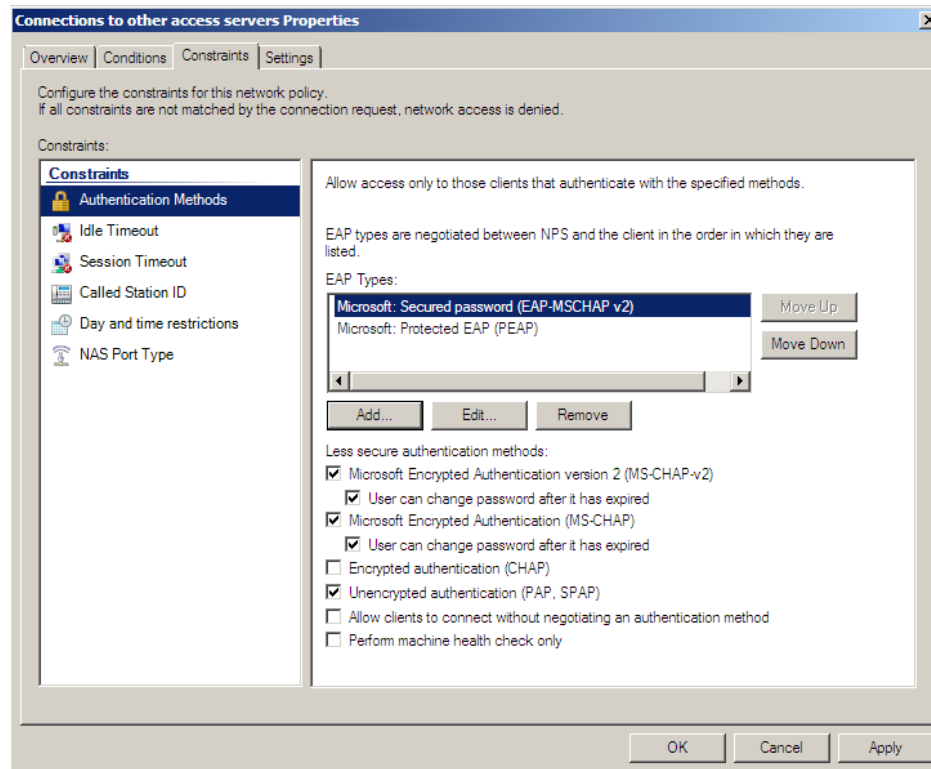
3. Right-click the policy and select **Properties**.

Note: Verify that the **Grant access** option button is selected.



4. Click the **Conditions** tab to specify the appropriate policy conditions.
5. Click the **Constraints** tab.

6. In the **Authentication Methods** section, select the appropriate check boxes for authentication methods for the environment.



7. In the **EAP Types** section, click **Add**.
8. In the **Add EAP** window, select **Microsoft:Secured password (EAP-MSCHAP v2)** or **Microsoft: Protected EAP (PEAP)**, and then click **OK**.

Note: Most implementations will choose just one EAP provider. Both options are included here for illustration purposes.

9. If EAP-MSCHAP v2 is going to be used for authentication, then Active Directory must be set up for 802.1x users to have their passwords stored in a "Reversible Password Encryption" format.

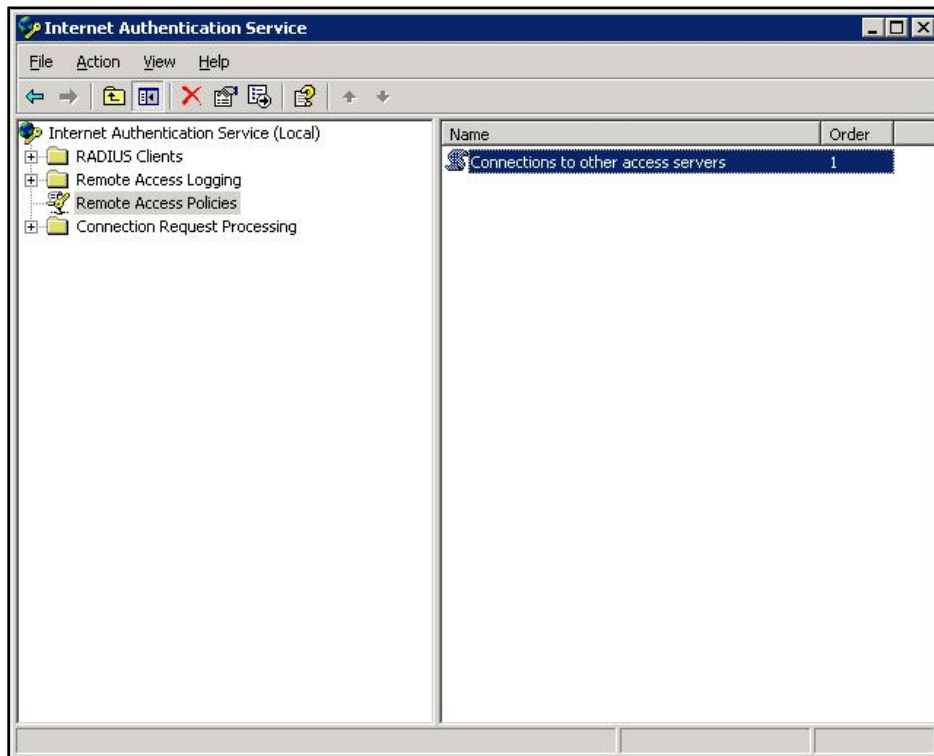
Important: If this is not set, then each user's account will need to be modified to enable it, and each user's password will need to be reset in order for Active Directory to store it in the new format. Enabling the "Reversible Password Encryption" feature within Active Directory without resetting the password will not work.

Server Settings for Internet Authentication Service (IAS) (Windows Server 2003)

If you are using Windows Server 2003, use Internet Authentication Service (IAS) to configure the DHCP server with IP scopes corresponding to the various VLANs. For example, the guest VLAN is 10.0.181.0/24, the all-access VLAN is 10.0.182.0/24, and the quarantine VLAN is 10.0.183.0/24.

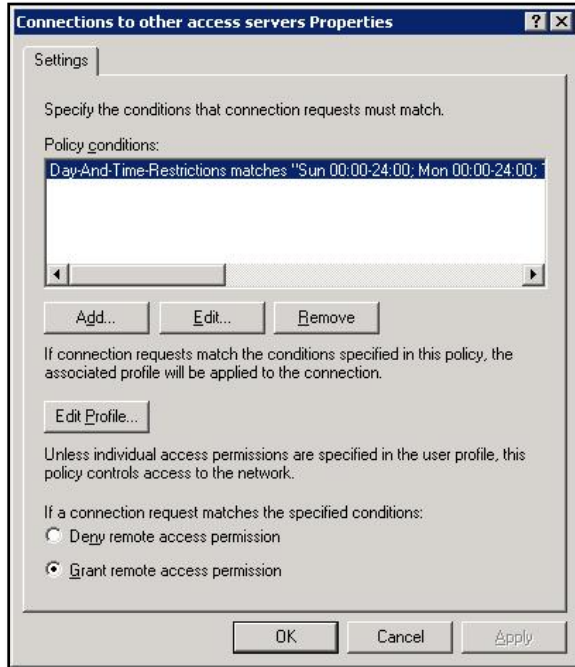
1. On the machine where IAS is installed, configure the remote access policies. From the Start menu, select **Administrative Tools ► Internet Authentication Server**.
2. Select **Remote Access Policies**.

Note: Either create a new remote access policy, or use an applicable existing remote access policy.

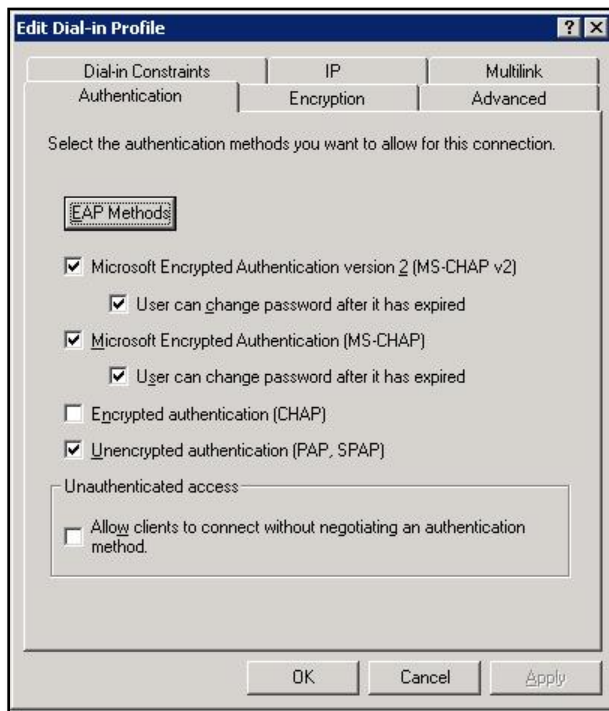


3. Right-click the policy and select **Properties**.

Note: Verify that the **Grant remote access permission** option button is selected.



4. Specify the appropriate policy conditions.
5. Click **Edit Profile...**
6. In the Edit Dial-in Profile window, click the **Authentication** tab.



7. Select the appropriate check boxes for authentication methods for the environment.
8. Click **EAP Methods**.

9. In the Select EAP Providers window, select **Protected EAP (PEAP)** or **MD5-Challenge**, and then click **Add....**

Note: Most implementations will choose just one EAP provider. Both PEAP and MD5 are included here for illustration purposes.

10. If MD5 is going to be used for authentication, then Active Directory must be set up for 802.1x users to have their passwords stored in a “Reversible Password Encryption” format.

Important: If this is not set, then each user’s account will need to be modified to enable it, and each user’s password will need to be reset in order for Active Directory to store it in the new format. Enabling the “Reversible Password Encryption” feature within Active Directory without resetting the password will not work.



Compliance Manager Settings

For more explicit instructions and additional information on using the Sophos NAC Advanced Compliance Manager, see the Compliance Manager online help.

Creating RADIUS Enforcer Access Templates

1. Log on to the Compliance Manager, and access **Enforce > RADIUS Enforcer Access Templates > Create RADIUS Enforcer Access Templates** to create a RADIUS Enforcer access template with an IP Address pointing to the switch. This template will point to the “good” VLAN (all access or guest).
2. In the Template Compliance States section, select the **Compliant** check box.
3. In the RADIUS Client IP Addresses section, type the IP address of the switch, and click **Add** to add the IP address to the template.
4. In the RADIUS Attributes section, select **Accept** as the network access type.
5. Create an accept attribute with the name **Tunnel-Private-Group-ID**. Set its Number to **81**, Format to **Text**, and Value to **VLAN0182**. In this case, NAC Advanced will be pointing to VLAN0182 (the “good” VLAN).

Important: This value must be set to whatever the VLAN NAME is on the switch. This value must be exactly as the switch sees the VLAN or it will not be able to put the user in the VLAN. If you want to know how the switch sees the VLAN, perform a “show vlan” on the switch to display the VLAN name. If the VLAN has not been given a custom name, then the switch will automatically name it something like VLAN00182. Use the output from this process to determine what value to use. For example, you may think the value is VLAN1, but the switch sees the value as VLAN0001.

The screenshot displays the 'Update RADIUS Enforcer Access Template' configuration page. The interface includes a navigation bar with 'MANAGE', 'ENFORCE', 'REPORT', and 'CONFIGURE SYSTEM'. Below the navigation, there are tabs for 'AGENT ENFORCER ACCESS TEMPLATES', 'RADIUS ENFORCER ACCESS TEMPLATES', 'DHCP ENFORCER ACCESS TEMPLATES', 'NETWORK RESOURCES', 'EXEMPTIONS', and 'MY LINKS'. The main content area is titled 'Enforce : Update RADIUS Enforcer Access Template' and contains the following sections:

- Name:** 8021.x: Enforcement Accept
- Version:** 4
- Description:** (empty field)
- Template Compliance States:**
 - Compliant
 - Partially Compliant
 - Non-Compliant
- RADIUS Client IP Addresses:**
 - ANY
 - 172.16.132.11
- RADIUS Attributes:**
 - Network Access: Accept
 - Attributes: Tunnel-Mode-Type 6 (802), Tunnel-Private-Group-ID, Tunnel-Type-13 (VLAN)
 - Properties for Tunnel-Private-Group-ID:
 - Type: Standard
 - Name: Tunnel-Private-Group-ID
 - Number: 81
 - Format: Text
 - Value: VLAN0182

At the bottom of the page, there are buttons for 'View Usage Details', 'Cancel', 'Save As New', and 'Save'. The footer indicates '© 2000-2007 Sophos Group. All rights reserved.'

- Click **New** to create another attribute with the name **Tunnel-Mode-Type 6(802)**. Set its Number to **65**, Format to **Integer**, and Value to **6**.

The screenshot shows the 'Enforce : Update RADIUS Enforcer Access Template' page. The 'Name' field contains '8021.x Enforcement Accept', 'Version' is '4', and 'Description' is empty. 'Template Compliance States' are set to 'Compliant'. Under 'RADIUS Client IP Addresses', '172.16.132.11' is listed. In the 'RADIUS Attributes' section, 'Network Access' is 'Accept'. The 'Attributes' list includes 'Tunnel-Mode-Type 6 (802)', 'Tunnel-Private-Group-ID', and 'Tunnel-Type-13 (VLAN)'. The 'Properties' for the selected attribute are: Type: Standard, Name: Tunnel-Mode-Type 6 (802), Number: 65, Format: Integer, and Value: 6. Buttons for 'View Usage Details', 'Cancel', 'Save As New', and 'Save' are visible at the bottom.

- Click **New** to create another attribute with the name **Tunnel-Type 13(VLAN)**. Set its Number to **64**, Format to **Integer**, and Value to **13**.

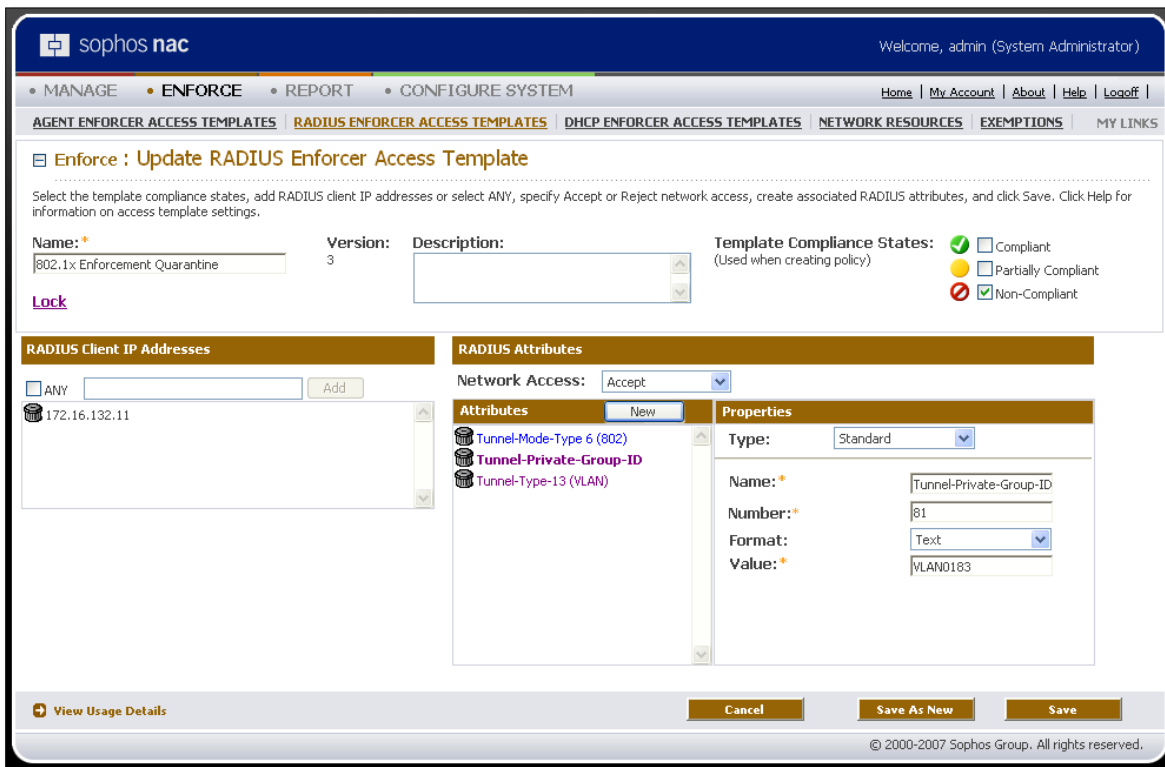
The screenshot shows the same 'Enforce : Update RADIUS Enforcer Access Template' page. The 'Name' field contains '8021.x Enforcement Accept', 'Version' is '4', and 'Description' is empty. 'Template Compliance States' are set to 'Compliant'. Under 'RADIUS Client IP Addresses', '172.16.132.11' is listed. In the 'RADIUS Attributes' section, 'Network Access' is 'Accept'. The 'Attributes' list includes 'Tunnel-Mode-Type 6 (802)', 'Tunnel-Private-Group-ID', and 'Tunnel-Type-13 (VLAN)'. The 'Properties' for the selected attribute are: Type: Standard, Name: Tunnel-Type-13 (VLAN), Number: 64, Format: Integer, and Value: 13. Buttons for 'View Usage Details', 'Cancel', 'Save As New', and 'Save' are visible at the bottom.

- Click **Save** to save the RADIUS Enforcer access template.

Important: Each of these attributes must be set up exactly as it is seen here, or it is very likely that the switch will not properly assign the VLAN to the NAC Advanced user. The following explains the attributes that you defined:

RADIUS Attributes Used	Attribute Description
Tunnel-Mode-Type 6 (802)	This attribute indicates the tunneling protocol(s) to be used. In this instance, the Value is 6, meaning that there is an IP Authentication Header in the Tunnel-mode (AH). (RFC2868)
Tunnel-Private-Group-ID	This attribute indicates the group ID for a particular tunneled session. In this case, the value for this attribute needs to be the exact name as it is labeled on the switch port for the switch to understand which VLAN to place the user in. (RFC2868)
Tunnel-Type-13 (VLAN)	This attribute indicates the tunneling protocol(s) to be used. In this instance, the Value is 13, meaning that the type of tunnel is a VLAN. (RFC3580)

- Create a new RADIUS Enforcer access template with an IP address pointing to the switch. This template will point to the “quarantine” VLAN.
- In the Template Compliance States section, select the **Non-Compliant** check box.
- In the RADIUS Client IP Addresses section, type the IP address of the switch, and click **Add** to add the IP address to the template.
- In the RADIUS Attributes section, select **Accept** as the network access type.
- Create an accept attribute with the name **Tunnel-Private-Group-ID**. Set its Number to **81**, Format to **Text**, and Value to **VLAN0183**. In this case, NAC Advanced will be pointing to VLAN0183 (the “quarantine” VLAN).



14. Repeat steps 6 and 7 to set up the two additional accept attributes.
15. Click **Save** to save the RADIUS Enforcer access template.

Note: You must create a policy and add the two RADIUS Enforcer access templates that were just created. Each template that was created was applied a network access type of “Accept”. If either one of the templates had a network access type of “Reject”, then the switch would deny all access to the port and would not switch the VLAN for the user.

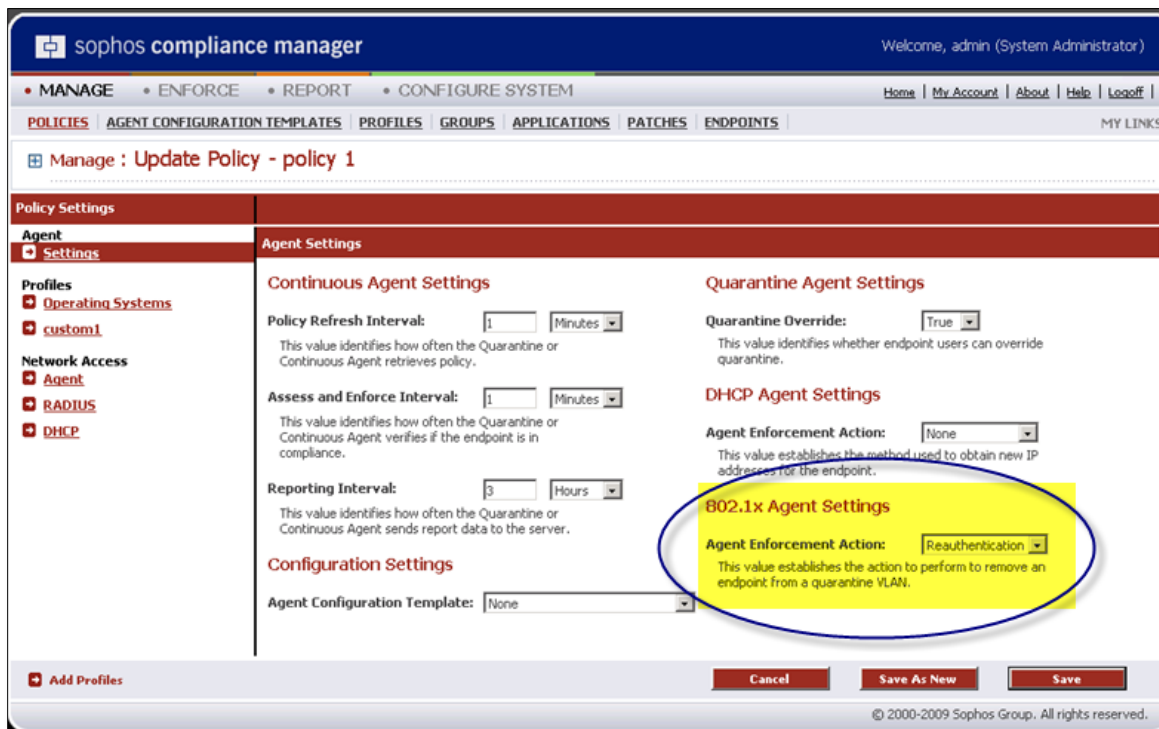
Creating a Policy

To use the access templates you created, you must create a policy and add the two RADIUS Enforcer access templates to it.

1. In the Compliance Manager, access **Manage > Policies > Create Policy**.
2. Type a name and description for the policy.
3. Select the **Default Policy** check box to make this policy the default policy.

Only one policy can be a default policy. The default policy is assigned if an endpoint has the Agent installed but the user or endpoint does not belong to a group in the Compliance Manager, or the user or endpoint belongs to a group and that group is not yet assigned to a policy. If an endpoint does not have an Agent installed and is not using the Dissolvable Agent, then Enforcer settings determine network access.

4. Click the **Policy Mode** list box to select the policy mode. The following policy modes are available:
 - **Report Only:** Endpoints are evaluated against profiles in policy and report information is generated in the Compliance Manager; however, no messages are displayed, no remediation actions are performed on the endpoint, and no enforcement actions are taken. The Report Only mode uses the access templates assigned in step 11.
 - **Remediate:** Endpoints are evaluated against profiles in policy, report information is generated in the Compliance Manager, messages are displayed, and remediation actions are performed on the endpoint; however, no enforcement actions are taken. The Remediate mode uses the access templates assigned in step 11.
 - **Enforce:** Endpoints are evaluated against profiles in policy, report information is generated in the Compliance Manager, messages are displayed and remediation actions are performed on the endpoint, and access templates are applied for the appropriate access or compliance states. The Enforce mode uses the access templates assigned in step 11.
5. In the left navigation Agent area, click **Settings**. Do any of the following, if applicable:
 - Specify the Continuous Agent Settings. These settings apply only to endpoints running the Continuous Agent or the Quarantine Agent:
 - **Policy Refresh Interval:** Identifies how often the Continuous Agent or Quarantine Agent retrieves policy.
 - **Assess and Enforce Interval:** Identifies how often the Continuous Agent or Quarantine Agent verifies if the endpoint is in compliance.
 - **Report Interval:** Identifies how often the Continuous Agent or Quarantine Agent sends report data to the server.
6. In the 802.1x Agent Settings area, click the **Agent Enforcement Action** list box and select **Reauthentication**. By doing this, the Agent forces an 802.1x Reauthentication, which will move the machine in and out of the “good”/“quarantine” VLANs as necessary. If this is not set, the client will be compliant or non-compliant, but the VLAN will not automatically switch. For this reason, it is **highly recommended** that this option be set to Reauthentication in an 802.1x environment.



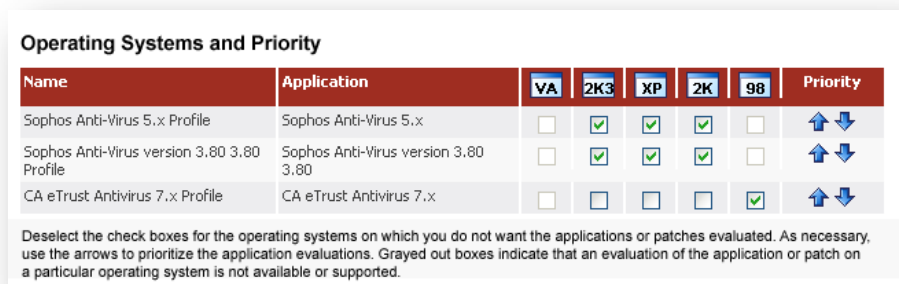
7. Click **Add Profiles**.
8. Select the check boxes beside the operating system profiles you want to add to the policy, and click **OK**. If you selected more than one operating system profile, you can prioritize the operating systems for evaluation.

Important: You must first add an operating system profile to the policy and then add profiles of other types to the policy. Unlimited profiles can be added to a policy. At a minimum, at least one operating system profile must be added to a policy. Policies must contain corresponding operating system profiles for each operating system you want to evaluate on endpoints.

Policy Behavior	Description
Required - Use Best Profile	The operating system profile is required and is evaluated as a best profile. In the case that one of the required operating systems is not installed on the endpoint, then the Else condition compliance state from the highest priority operating system profile is used to determine the compliance state and actions for the operating system profile type, and no additional profiles for that policy are evaluated.
Use Best Profile	Each profile of a particular type within a policy is evaluated on the endpoint, the best match is determined, and only the warranted actions associated with the best match profile are taken. The Best behavior uses the profile that is the most compliant on the endpoint to determine the compliance state for the profile type in policy. Application profiles, unless designated otherwise, are evaluated in this way. If none of the profiles that are evaluated is installed on the endpoint, then the Else condition compliance state from the highest priority profile is used to determine the compliance state and actions for the profile type in policy.
Use All Profiles	All profiles of a particular type within a policy are evaluated on the endpoint, and warranted actions associated with all of the profiles are taken. The All behavior uses the profile that is the least compliant on the endpoint to determine the compliance state for the profile type in policy. Patch profiles

Policy Behavior	Description
	are evaluated in this way. Application profiles that you want to prevent on the endpoint can be evaluated in this way.

- As necessary, click **Add Profiles** to add profiles of another profile type to the policy, click the **Profile Type** list box to select the profile type, select the check boxes beside the profiles you want to add to the policy, and click **OK**. Repeat this step as necessary to add additional profiles to the policy.
- If you selected any application or patch profiles, you can specify the operating systems on which the application or patch will be evaluated. Also, if you selected more than one application profile, you can prioritize the applications for evaluation.



- In the left navigation Network Access area, click the **RADIUS** enforcement type. To add access templates for a particular access state, click the appropriate policy mode tab, click **Select**, select the option button or check boxes beside the access templates and beside the access states that the templates apply to, and click **OK**. You can also leave or delete the current access templates. The following policy modes and access states are available:

Note: By default, each policy is automatically populated with access templates for each of the access states, based on the templates defined in the Compliance Manager and their associated template compliance states. If you have defined RADIUS Enforcer access templates, all templates of a particular compliance state are automatically applied to each access state; you can prioritize or delete them as necessary.

Policy Mode	Descriptions and Access States
RADIUS	
Report Only	Endpoints are evaluated against profiles in policy and report information is generated in the Compliance Manager; however, no messages are displayed, no remediation actions are performed on the endpoint, and no enforcement actions are taken. Select a RADIUS Enforcer template that enables access for traffic originating from the endpoint. Important: If you apply a RADIUS Enforcer access template that prevents network access in the Report Only mode, all requests that match the selected template will be denied access regardless of their actual compliance state. To enforce a compliance state, you must change the policy mode to Enforce.
Remediate	Endpoints are evaluated against profiles in policy, report information is generated in the Compliance Manager, messages are displayed, and remediation actions are performed on the endpoint; however, no enforcement actions are taken. Select a RADIUS Enforcer access template that enables access for traffic originating from

Policy Mode	Descriptions and Access States
	<p>the endpoint.</p> <p>Important: If you apply a RADIUS Enforcer access template that prevents network access in the Remediate mode, all requests that match the selected template will be denied access regardless of their actual compliance state. To enforce a compliance state, you must change the policy mode to Enforce.</p>
Enforce	<p>Endpoints are evaluated against profiles in policy, report information is generated in the Compliance Manager, messages are displayed and remediation actions are performed on the endpoint, and access templates are enforced for the following access states. The selected RADIUS Enforcer access templates associated with each state in policy determine network access when the endpoint is in that state.</p> <p>Enforcer State:</p> <ul style="list-style-type: none"> • Policy Retrieval Error: The user's compliance state is out-of-date according to the RADIUS Policy Update Threshold field configured in the Configure System > Enforcer Settings area. <p>Compliance States:</p> <ul style="list-style-type: none"> • Compliant: The assessment determined the endpoint is compliant with the policy. • Partially Compliant: The assessment determined the endpoint is partially compliant with the policy. • Non-Compliant: The assessment determined the endpoint is not compliant with the policy.

12. As necessary, use the arrows to prioritize RADIUS Enforcer access templates. If more than one template applies to a particular state, the first template that meets the state is used. Sophos recommends that you prioritize the more specific/strict access templates first and the less specific/strict access templates last.
13. Click **Save**.

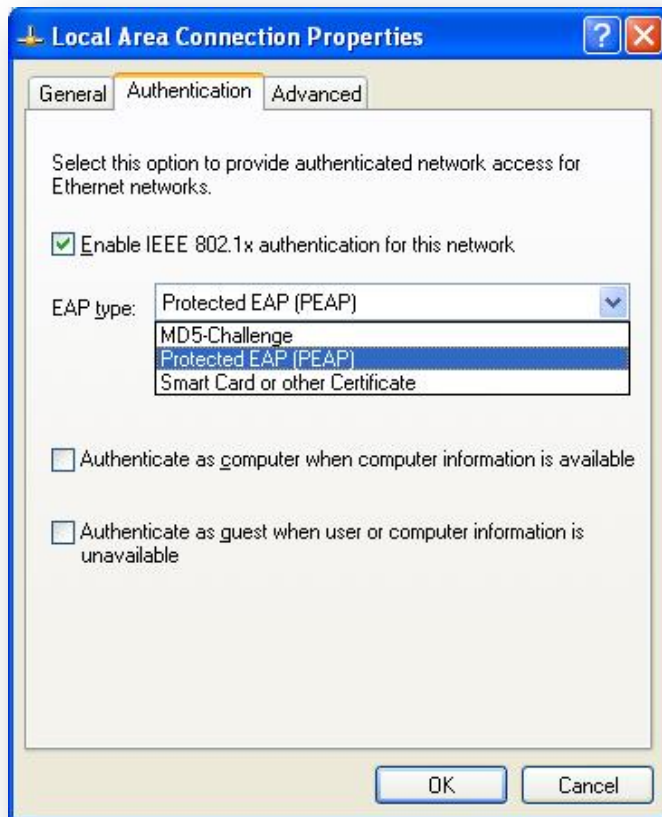
Microsoft Supplicant Settings (Protected EAP Protocol)

To set up the Microsoft supplicant using Protected EAP (PEAP) protocol, use the following procedure for Windows XP (SP1 and SP2) and Windows 2000 SP4.

1. From the Start menu, select **Control Panel > Network Connections**.
2. In the Network Connections window, double-click the local area connection that is connected to the switch. The Properties window for the local area connection displays.
3. In the Local Area Connection Properties window, click the **Authentication** tab.

Note: If the Authentication tab does not appear in the Local Area Connection Properties window in Windows XP, verify that the Wireless Zero Configuration service is started and the startup type is set to Automatic. For Windows 2000 SP4, verify that the Wireless Configuration service is started and the startup type is set to Automatic.

4. Select the **Enable IEEE 802.1x authentication for this network** check box, and select **Protected EAP (PEAP)** from the **EAP type** list box. This step specifies the PEAP protocol between the client and the switch.



5. Click **Properties**.
6. In the Protected EAP Properties window, clear the **Validate server certificate** check box if you are not using server certificates to validate authentication.

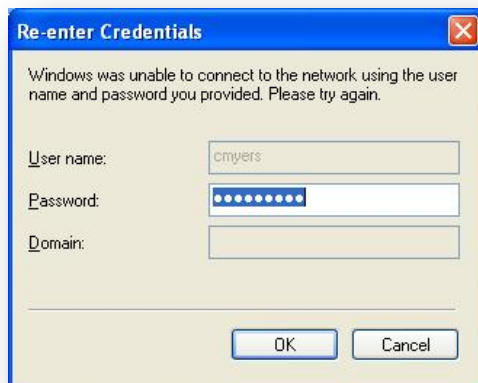


7. From the **Select Authentication** list box, select **Secured password (EAP-MSCHAP v2)** as the authentication method.
8. Click **Configure...**
9. In the EAP MSCHAPv2 Properties window, select **Automatically use my Windows logon name and password** check box if you are using your Windows (local machine) logon and domain to authenticate to 802.1x.



10. Click **OK** on each window to save these new properties.
11. Disable and re-enable the local area connection to force a re-authentication to the 802.1x switch.

12. If you are not using your Windows logon and domain for authentication, a window displays prompting you to re-enter your credentials.



13. Access the Compliance Agent, and type the appropriate user credentials to properly authenticate the machine.
14. Disable and re-enable the local area connection or disconnect and reconnect the network cable.

Note: This step is the only way to force the Microsoft 802.1x supplicant to re-establish access to the proper LAN.

Note: Since Windows caches credentials for Protected EAP authentication, no prompt will display to re-enter credentials until the password has been changed in Active Directory.

Microsoft Supplicant Settings (Protected EAP Protocol) for Windows XP SP3+

For Windows XP SP3 and greater operating systems, Microsoft has changed the default authentication mechanism so that the supplicant uses both Machine authentication and User authentication “MachineOrUser” mode. Details can be found at <http://support.microsoft.com/kb/949984/>.

This behavior is not ideal since the supplicant will try first to authenticate the machine when it is in the boot process. As a result, the machine will send its authentication to the 802.1x switch, which forwards the request to the Compliance Application Server. The Compliance Application Server has no knowledge of the machine since NAC is user-based. As such, the machine will always be put into the quarantine VLAN when it is booting up. Additionally, the Microsoft’s supplicant does not always try to re-authenticate the user when the user logs in. Therefore, even if the user is compliant, the machine may still be in the quarantine VLAN. Because of these reasons, it may be necessary to change this behavior.

In this case, the SP3 supplicant machine’s 802.1x profile can be modified to use only User authentication just as it did for Windows XP SP2. This change can be made by following the steps in the Microsoft knowledgebase article 929847 (<http://support.microsoft.com/kb/929847/>), which describes how to put the machine into computer-only authentication mode. Since the article describes how to put the machine into computer-only mode and the desired mode is user-only, you will need to substitute the word “user” for “machine” within the XML file example:

```

OneX xmlns="http://www.microsoft.com/networking/OneX/v1">

    <cacheUserData>>false</cacheUserData>

    user
    <authMode>machine</authMode>

    <EAPConfig>...</EAPConfig>

</OneX>

```

Important: Do **NOT** forget to complete step 4 (below the wireless connections in the procedure). This step forces the supplicant's profile to use the "user" authentication mode. If this step is not completed, then the machine will continue to be in "UserOrMachine" mode. Once you have confirmed that step 4 was completed, re-run Step 2 to force re-creation of the profiles. You can then confirm that the "user" setting is in the Local Area Connection.xml configuration. If it is not, then you will need to perform the steps in the knowledgebase article again since the setting was not correctly inserted into the supplicant's configuration the first time.

If <authMode> Tags Are Missing

The Microsoft knowledgebase article assumes that the <authMode> tags exist within the Local Area Connection.xml file. If the tags do not exist, then you must modify the XML file to include them since the default is "MachineOrUser" when the tags are not present. You must also place these tags in the correct position. You should insert them below the <OneX xmlns> tags and above the EapConfig tags, as shown here:

Original:

```

<?xml version="1.0"?>
<LANProfile xmlns="http://www.microsoft.com/networking/LAN/profile/v1">
  <MSM>
    <security>
      <OneXEnforced>>false</OneXEnforced>
      <OneXEnabled>>true</OneXEnabled>
      <OneX xmlns="http://www.microsoft.com/networking/OneX/v1">
        <EAPConfig><EapHostConfig xmlns="http://www.microsoft.com/provisioning/EapHostConfig"><EapMethod><Type xmlns="htt
      </OneX>
    </security>
  </MSM>
</LANProfile>

```

New:

```

<?xml version="1.0"?>
<LANProfile xmlns="http://www.microsoft.com/networking/LAN/profile/v1">
  <MSM>
    <security>
      <OneXEnforced>>false</OneXEnforced>
      <OneXEnabled>>true</OneXEnabled>
      <OneX xmlns="http://www.microsoft.com/networking/OneX/v1">
        <authMode>user</authMode>
        <EAPConfig><EapHostConfig xmlns="http://www.microsoft.com/provisioning/EapHostConfig"><EapMethod><Type xmlns="htt
      </OneX>
    </security>
  </MSM>
</LANProfile>

```

After the tags have been added, go to step 4 in the article and run the appropriate command to insert the new profile into the supplicant.

Microsoft Supplicant Settings (MD5-Challenge Protocol)

Note: MD5-Challenge protocol applies to Windows Server 2003 (not Windows Server 2008). Protected EAP (PEAP) protocol can also be used for Windows Server 2003.

To set up the Microsoft supplicant using MD5-Challenge protocol, use following procedure on Windows XP (SP1 and SP2) and Windows 2000 SP4.

1. From the **Start** menu, select **Control Panel ► Network Connections**.
2. In the Network Connections window, double-click the local area connection that is connected to the switch. The Properties window for the local area connection displays.
3. Select the **Authentication** tab.

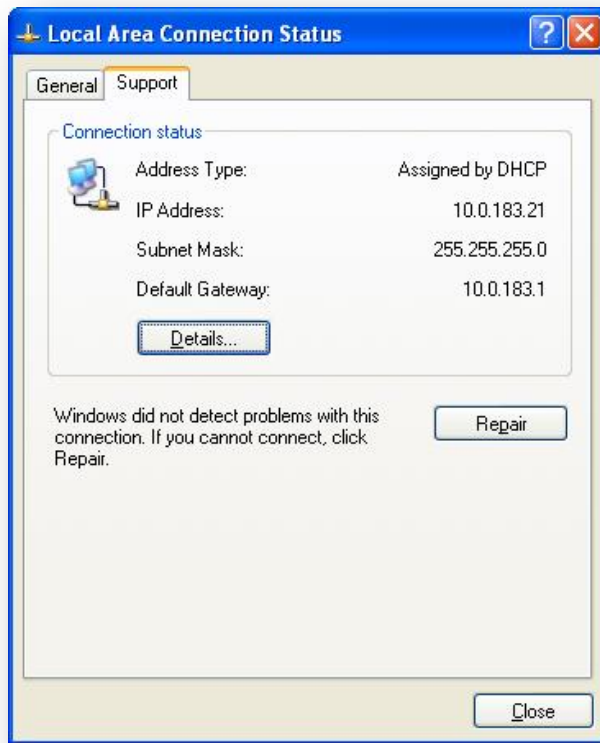
Note: If the Authentication tab does not appear in the Local Area Connection Properties window in Windows XP, verify that the Wireless Zero Configuration service is started and the startup type is set to Automatic. For Windows 2000 SP4, verify that the Wireless Configuration service is started and the startup type is set to Automatic.

4. Select the **Enable IEEE 802.1x authentication for this network** check box, and select **MD5-Challenge** from the **EAP type** list box. This step specifies the MD5 protocol between the client and the switch.
5. Disable and re-enable the local area connection.
6. A balloon message displays above the network icon in the system tray. Click this balloon. The Local Area Connection RADIUS window displays.



7. Type the RADIUS user name, password, and logon domain (if required) in the provided fields, and then click **OK**.

Assuming that the Agent has not been authenticated to Sophos, the machine will be placed in the quarantine VLAN. The Local Area Connection Status window displays that the machine was assigned IP address 10.0.183.21 on the quarantine VLAN.



8. Access the Compliance Agent, and type the appropriate user credentials to properly authenticate the machine.
9. Disable and re-enable the local area connection, or disconnect and reconnect the network cable. The Local Area Connection RADIUS logon window displays.

Note: This step is the only way to force the Microsoft 802.1x supplicant to re-establish access to the proper LAN.

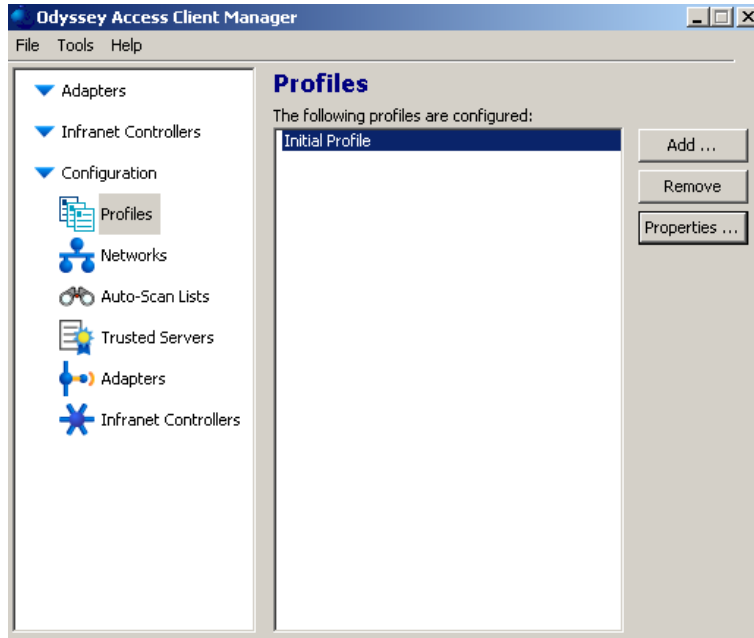
10. Type the appropriate logon information.

Note: Since the client machine has been properly authenticated through Sophos, the machine is placed in the all access VLAN.

Juniper Networks Odyssey Access Client Supplicant

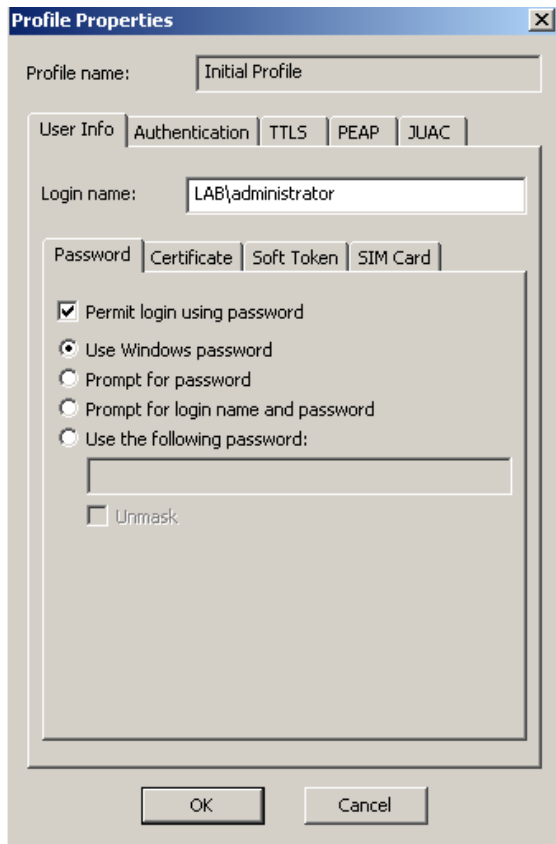
To set up Juniper Networks Odyssey Access Client supplicant using PEAP or MD5-Challenge protocol, use the following procedure for Windows XP (SP2 and SP3).

1. After installing Odyssey Access Client, open Odyssey Access Client Manager, and select **Profiles**.



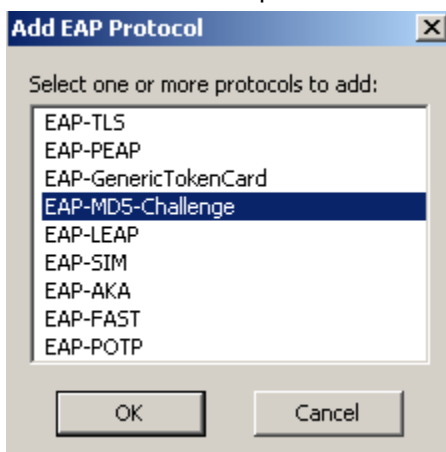
2. Select **Initial Profile** and click the **Properties...**
3. In the Profile Properties window, click the **User Info** tab.

4. Use the login name that is already specified for this profile (for use with SSO), select the **Permit login using password** check box, and select the appropriate password option button.

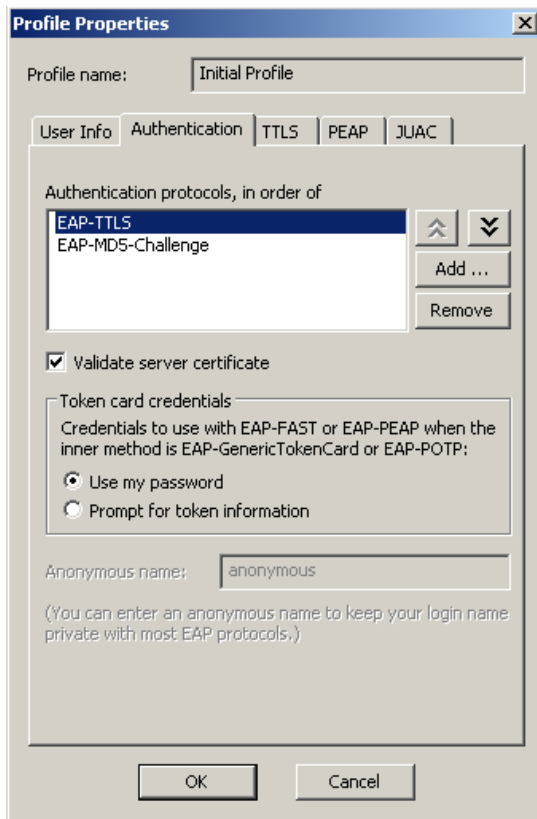


5. Click the **Authentication** tab, and then click **Add....**
6. In the Add EAP Protocol window, select **EAP-PEAP** or **EAP-MD5-Challenge**, and then click **OK**.

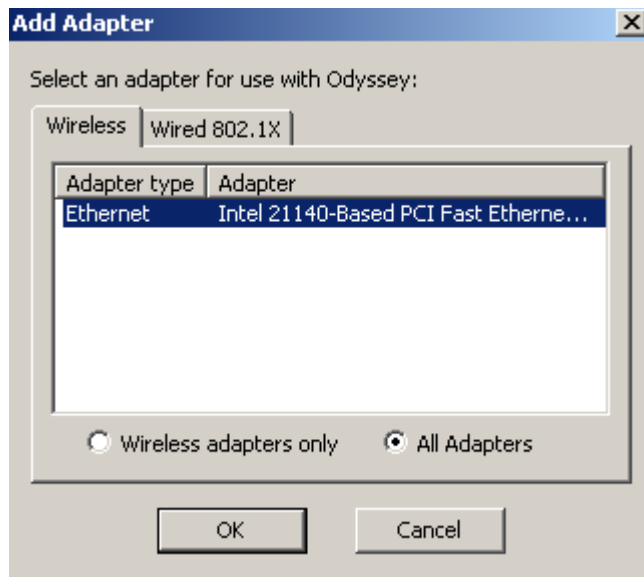
Note: The other EAP protocols were not tested for this document.



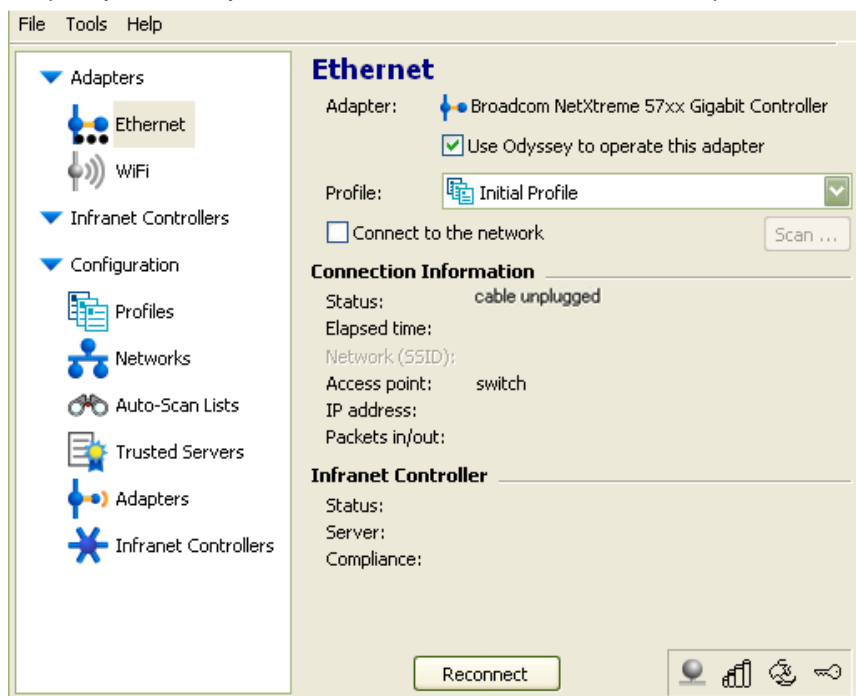
7. In the Profile Properties window, select the **EAP-TTLS** protocol, and then click **Remove**.



8. Click **OK** to return to the Odyssey Access Client Manager.
9. Click **Adapters**, and then click **Add....**
10. In the Add Adapter window, select the adapter that is connected to the 802.1x switch, and then click **OK** to return to the Odyssey Access Client Manager.



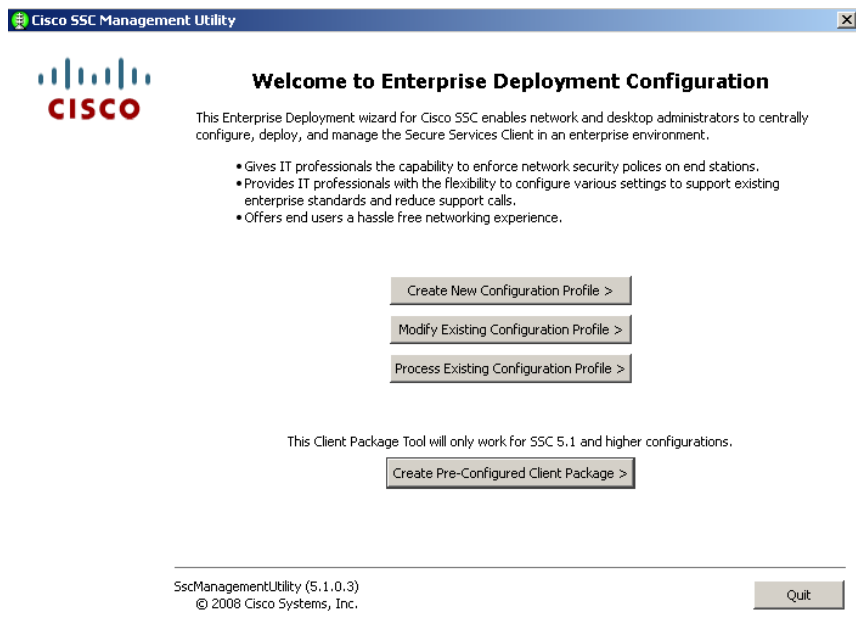
11. In the Adapters section, select the adapter, select the profile from the **Profile** list box, and select the **Connect to the network** check box. If the password was not set in the Odyssey profile properties, a window displays requesting the password.
12. Type a valid password, and then click **OK**. The Odyssey Access Client Manager indicates that the machine is connected to the quarantine or compliant VLAN.
13. Access the Compliance Agent, and type the appropriate user credentials to properly authenticate the machine. These credentials should match what was entered for the supplicant so that the two usernames match. If the usernames do not match, then the user will always be kept in the quarantine VLAN.
14. After an assessment is done and the compliance state changes, assuming that the 802.1x Agent Enforcement Action within the NAC policy is set to “Reauthentication” and the DHCP Enforcement Action is set to “Release/Renew”, the user’s NIC will disable and re-enable and the user will be placed on the network with the newly assigned VLAN and IP address. If the compliance state does not change, then the user’s NIC will not be “flipped” and the user will stay in the same VLAN. If the user wants to force the re-authentication without using the policy, then they can de-select the check box on the adapter and it will disconnect the supplicant.



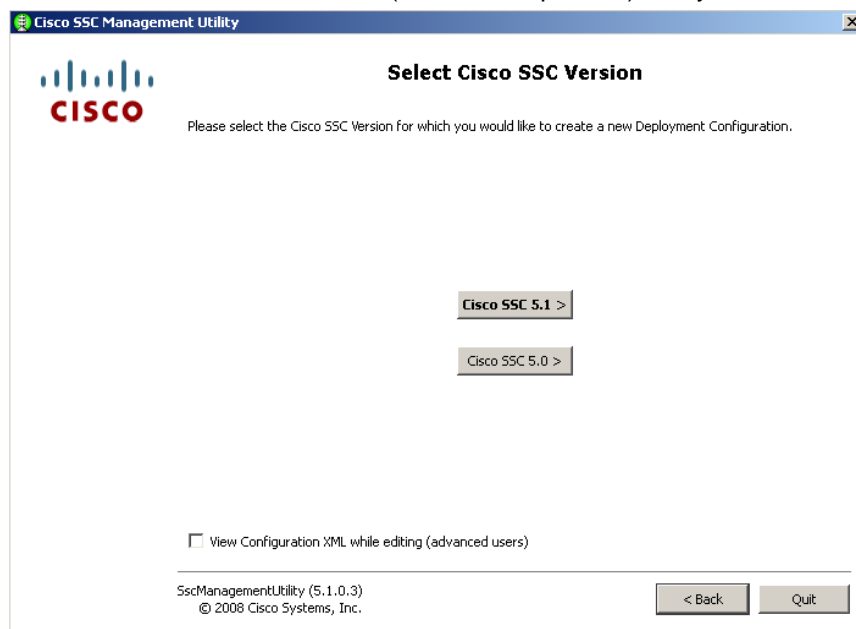
Cisco Secure Services Client Supplicant

To set up Cisco Secure Services Client supplicant using PEAP or MD5-Challenge protocol, use the following procedure for Windows XP (SP2 and SP3).

1. Before downloading Cisco Secure Services Client (SSC), you must first download Cisco Secure Services Client Management Utility (SSCMgmtUtil) and install it so that you can configure the client, as there is no other way to configure the client.
2. After the tool and the client have been downloaded, run the **sscManagementUtility.exe** to open Cisco SSC Management Utility, and click **Create New Configuration Profile**.



3. Select the version of Cisco SSC (in this example, 5.1) that you want to configure, and then click **Next**.



4. Select the **Attempt connection after user logon** option, select the **Allowed Wired (802.3) Media** check box, and then click **Next**

Cisco SSC 5.1 Configuration Profile

Client Policy

License

Provide License

#####

Connection Settings

Attempt connection before user logon
Number of seconds to wait before allowing user to logon: 30

Attempt connection after user logon

Default Connection Timeout: 40 Default Association Timeout: 3

Allowed Media

Allow Wi-Fi (wireless) Media
 Enable validation of WPA/WPA2 handshake

Allow Wired (802.3) Media VPN Authentication Mechanism: Password

Allow VPN

< Back Next > Cancel

5. Select the desired authentication modes (in this example, PEAP and EAP-MSCHAPv2), along with your license information (at the top), and then click **Next**.

Cisco SSC 5.1 Configuration Profile

Authentication Policy

Allowed Association Modes

Select All

Open (no encryption)

Open (Static WEP)

Shared (WEP)

WPA Personal TKIP

WPA Personal AES

WPA2 Personal TKIP

WPA2 Personal AES

Select All

Open (Dynamic (802.1X) WEP)

WPA Enterprise TKIP

WPA Enterprise AES

WPA2 Enterprise TKIP

WPA2 Enterprise AES

CCKM Enterprise TKIP

CCKM Enterprise AES

Allowed Authentication Modes

Select All

LEAP

PEAP

EAP-GTC

EAP-FAST

EAP-MD5

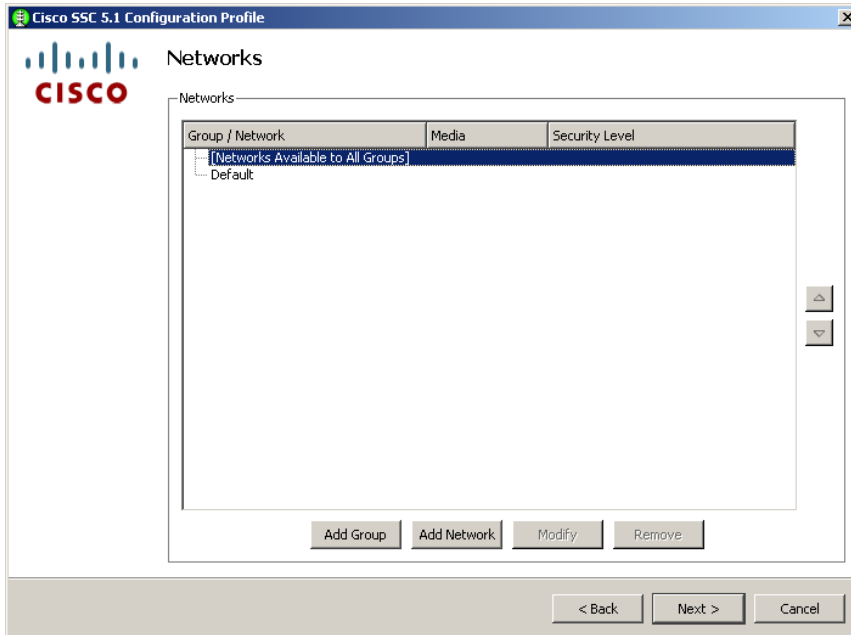
EAP-MSCHAPv2

EAP-TLS

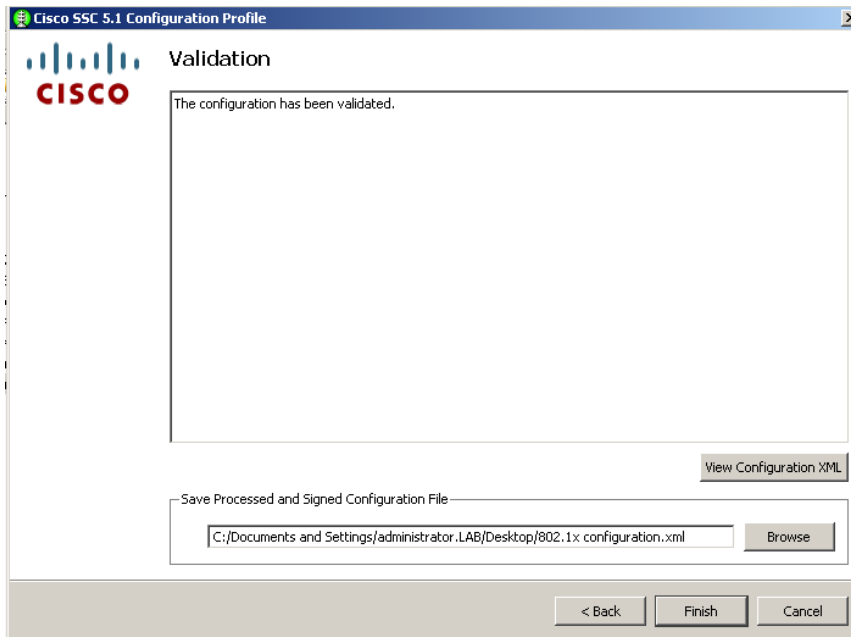
EAP-TTLS

< Back Next > Cancel

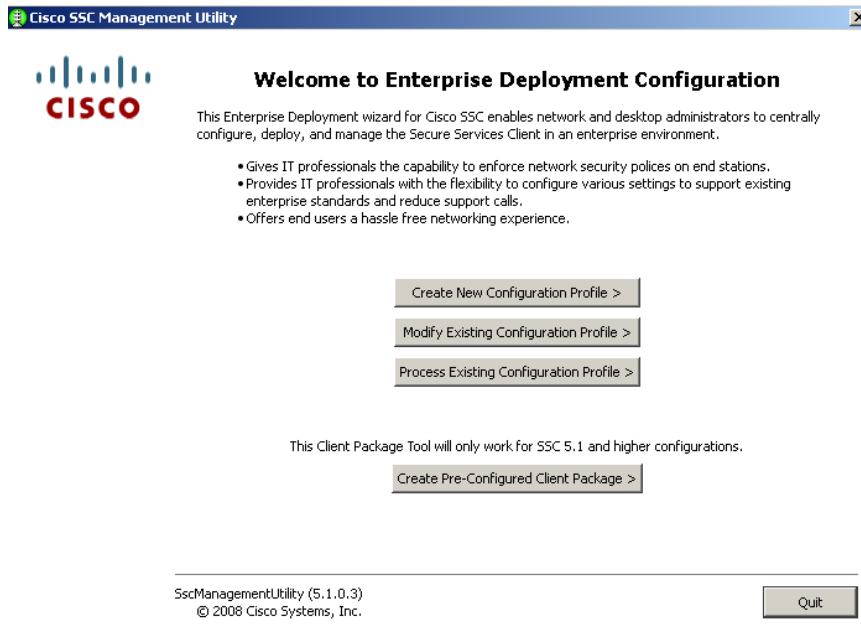
6. Select the **[Networks Available to All Groups]** option, along with any other association modes for which you want to use the supplicant, and then click **Next**.



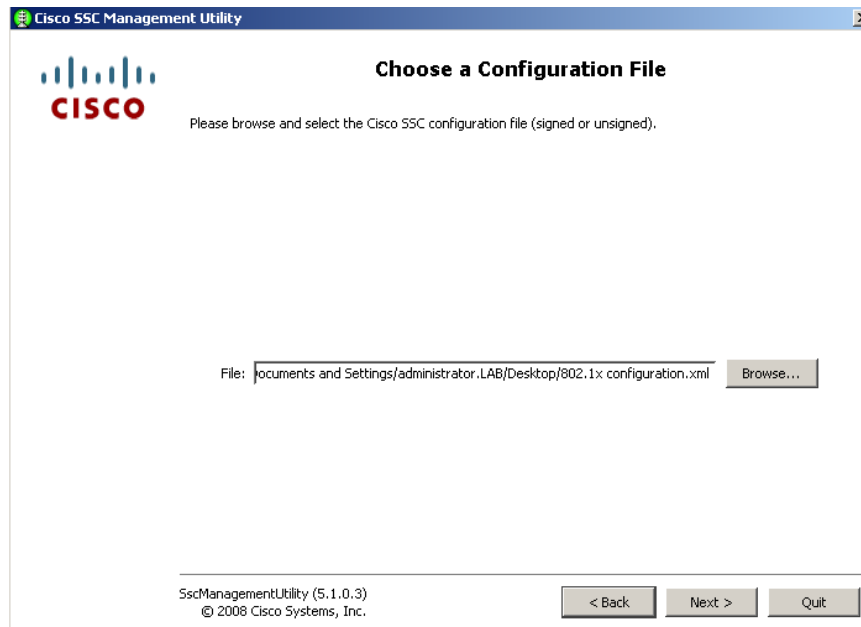
7. Browse to the location where you want to save the configuration file, and then click **Finish**.



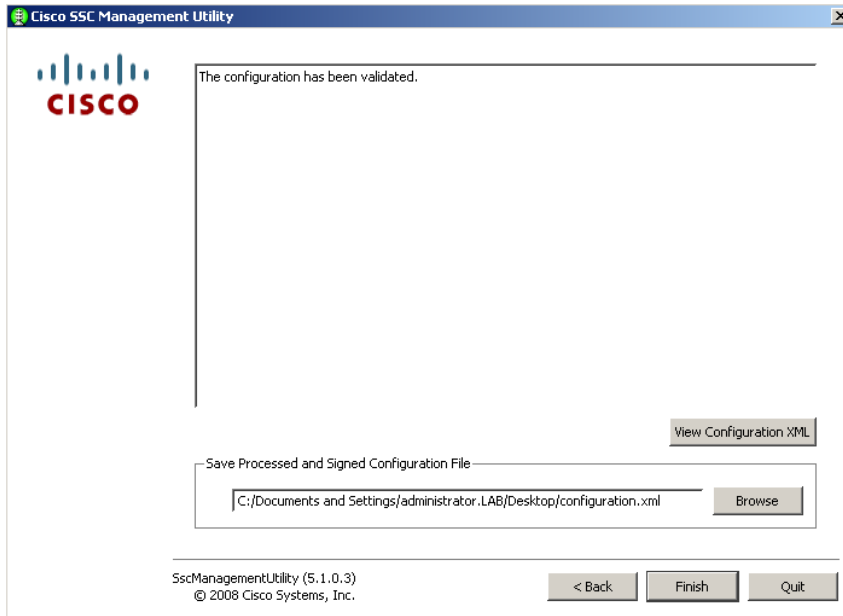
8. Click **Process Existing Configuration Profile**.



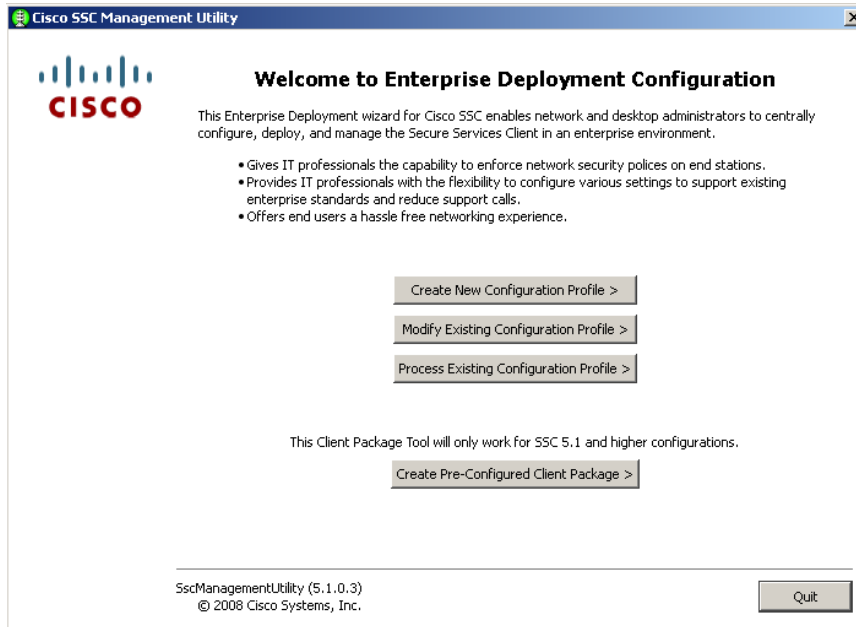
9. Browse to the location where you saved the previously configured configuration file, and then click **Next**.



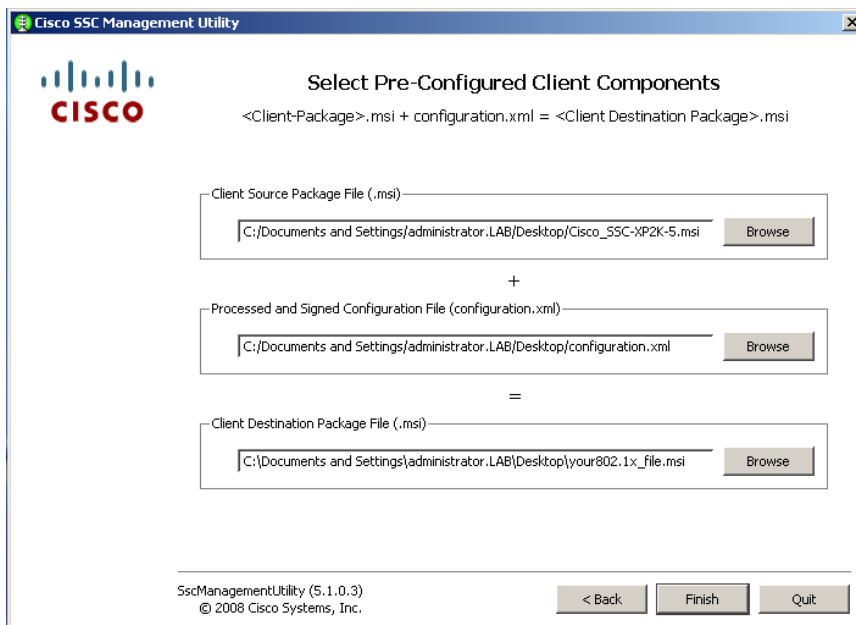
10. Browse to the location where you want to save the signed version of the configuration file (ensure that it is called "configuration.xml"), and then click **Finish**.



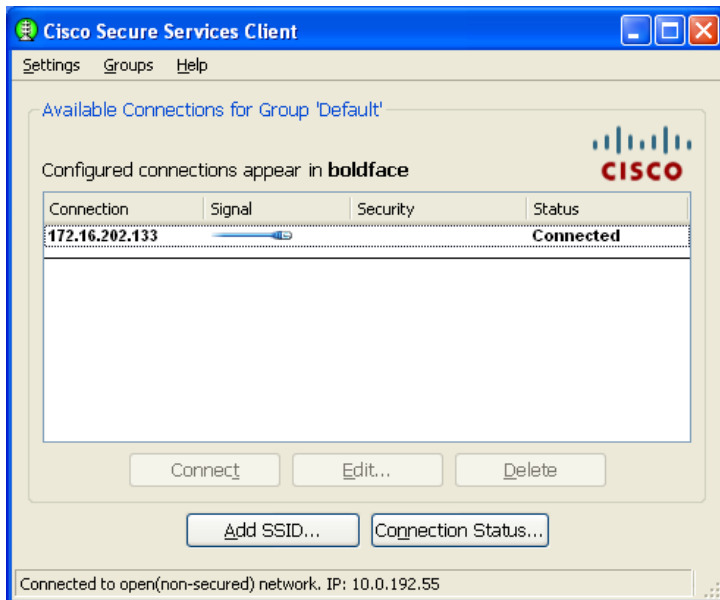
11. Now that the configuration file has been validated/signed, click **Create Pre-Configured Client Package**.



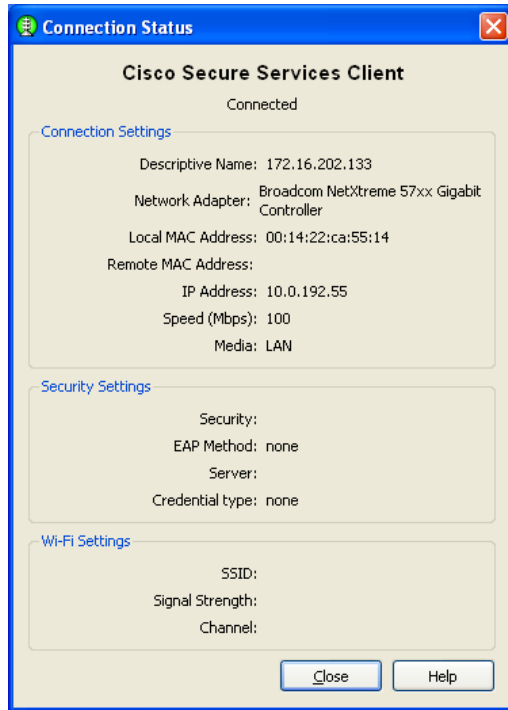
12. In the appropriate fields, select the client source package, the signed configuration file, and the location where you want the destination file to be saved, and click **Finish** to create the new client msi package. Then, click **Quit**.



13. Install Cisco SSC.
14. Cisco SSC connects to the 802.1x network. Depending on the configuration of the VLAN, the IP address is set to either the guest or quarantine VLAN. In this example, the IP address is set to the quarantine VLAN.



15. Access the Compliance Agent, and type the appropriate user credentials to properly authenticate the machine.
16. In the Cisco Secure Services Client window, click **Connect** to restart the supplicant.
The client machine obtains a new IP address. You can click **Connection Status...** to display the connection information for the selected network adapter.



Troubleshooting

The most reported problem is that the switch is not moving the user into the correct VLAN, or is not moving the VLAN at all. There are a number of reasons why this may be occurring, yet the most likely reasons are:

1. The switch doesn't support IEEE 802.1x – VLAN Assignment.
 - In order to troubleshoot this issue, the switch/IOS features should be looked up on Cisco's website as mentioned within the Cisco Switch Supported Options. As long as this has been confirmed, this is likely not the issue.
2. The VLAN NAME that is being returned doesn't match a VLAN that is located on the switch.
 - The best way to confirm if this is the issue is to perform a **debug dot1x all** and save the configuration to a file (it becomes quite verbose) and then view the log to see what was sent to the switch and what the switch didn't like about it.
3. RADIUS is not authorized to dynamically switch the VLAN with its returned attributes.
 - If the following line is missing, this is the problem: **aaa authorization network default group radius**.
4. The Username that is being used in the Supplicant for 802.1x authentication does not match the username that is being used in the Compliance Agent for NAC Advanced registration.
 - The best way to confirm this is to confirm that the username for the NAC Advanced registration matches the username used for the 802.1 x supplicant. To further confirm this, go to the Compliance Manager and look up the username that is being using to authenticate the 802.1x supplicant and confirm that there is a corresponding record for it. If there is no record, then NAC Advanced always returns the VLAN as if the user was an "Unknown Endpoint".

Appendix A: Sample Cisco 802.1x Catalyst 2950 Configuration

The following is a sample configuration of a working Cisco 802.1x Catalyst 2950 switch:

```
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname 2950SW
!
aaa new-model
aaa authentication login default line
aaa authentication login LOCAL local
aaa authentication dot1x default group radius
aaa authorization network default group radius
enable secret 5 $1$h13a$BGw0X5qu2wE0hB0AhBcKe/
!
username swadmin privilege 15 password 7 13360202581E513E7F36
ip subnet-zero
!
ip domain-name endpointsoftware.info
ip ssh time-out 120
ip ssh authentication-retries 3
vtp domain dbdsk-msc
vtp mode transparent
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
dot1x system-auth-control
!
vlan 100
!
vlan 102
name good
!
vlan 103
name deny
!
vlan 104
!
```

```
interface FastEthernet0/1
description NAC Appliance Mgmt Port
switchport mode access
switchport voice vlan 100
no logging event link-status
no keepalive
dot1x port-control auto
dot1x reauthentication
spanning-tree portfast
!
interface FastEthernet0/2
switchport mode access
switchport voice vlan 100
no logging event link-status
no keepalive
dot1x port-control auto
dot1x reauthentication
spanning-tree portfast
!
interface FastEthernet0/3
switchport mode access
switchport voice vlan 100
no logging event link-status
no keepalive
dot1x port-control auto
dot1x reauthentication
spanning-tree portfast
!
interface FastEthernet0/4
switchport mode access
switchport voice vlan 100
no logging event link-status
no keepalive
dot1x port-control auto
dot1x reauthentication
spanning-tree portfast
!
interface FastEthernet0/5
switchport access vlan 102
switchport voice vlan 100
no logging event link-status
no keepalive
spanning-tree portfast
```

```
!  
interface FastEthernet0/6  
  switchport access vlan 102  
  switchport voice vlan 100  
  no logging event link-status  
  no keepalive  
  dot1x timeout reauth-period 30  
  spanning-tree portfast  
!  
interface FastEthernet0/7  
  switchport access vlan 102  
  switchport voice vlan 100  
  no logging event link-status  
  no keepalive  
  spanning-tree portfast  
!  
interface FastEthernet0/8  
  switchport access vlan 102  
  switchport voice vlan 100  
  no logging event link-status  
  no keepalive  
  spanning-tree portfast  
!  
interface FastEthernet0/9  
  switchport access vlan 102  
  switchport voice vlan 100  
  no logging event link-status  
  no keepalive  
  spanning-tree portfast  
!  
interface FastEthernet0/10  
  switchport access vlan 102  
  switchport voice vlan 100  
  no logging event link-status  
  no keepalive  
  spanning-tree portfast  
!  
interface FastEthernet0/11  
  switchport access vlan 102  
  switchport voice vlan 100  
  no logging event link-status  
  no keepalive  
  spanning-tree portfast
```

```
!  
interface FastEthernet0/12  
  switchport access vlan 102  
  switchport voice vlan 100  
  no logging event link-status  
  no keepalive  
  spanning-tree portfast  
!  
interface FastEthernet0/13  
  switchport access vlan 102  
  switchport voice vlan 100  
  no logging event link-status  
  no keepalive  
  spanning-tree portfast  
!  
interface FastEthernet0/14  
  switchport access vlan 102  
  switchport voice vlan 100  
  no logging event link-status  
  no keepalive  
  spanning-tree portfast  
!  
interface FastEthernet0/15  
  switchport access vlan 102  
  switchport voice vlan 100  
  no logging event link-status  
  no keepalive  
  dot1x timeout reauth-period 30  
  spanning-tree portfast  
!  
interface FastEthernet0/16  
  switchport access vlan 102  
  switchport voice vlan 100  
  no logging event link-status  
  no keepalive  
  spanning-tree portfast  
!  
interface FastEthernet0/17  
  switchport access vlan 102  
  switchport voice vlan 100  
  no logging event link-status  
  no keepalive  
  spanning-tree portfast
```

```
!  
interface FastEthernet0/18  
  switchport access vlan 102  
  switchport voice vlan 100  
  no logging event link-status  
  no keepalive  
  spanning-tree portfast  
!  
interface FastEthernet0/19  
  switchport access vlan 102  
  switchport mode access  
  switchport voice vlan 100  
  no logging event link-status  
  no keepalive  
  dot1x port-control auto  
  spanning-tree portfast  
!  
interface FastEthernet0/20  
  switchport access vlan 102  
  switchport voice vlan 100  
  no logging event link-status  
  no keepalive  
  spanning-tree portfast  
!  
interface FastEthernet0/21  
  switchport mode access  
  switchport voice vlan 100  
  no logging event link-status  
  no keepalive  
  dot1x port-control auto  
  dot1x reauthentication  
  spanning-tree portfast  
!  
interface FastEthernet0/22  
  switchport voice vlan 100  
  no logging event link-status  
  no keepalive  
  spanning-tree portfast  
!  
interface FastEthernet0/23  
  switchport access vlan 102  
  switchport voice vlan 100  
  no logging event link-status
```

802.1x Dynamic VLAN Assignment

```
no keepalive
spanning-tree portfast
!
interface FastEthernet0/24
switchport trunk native vlan 104
switchport trunk allowed vlan 1,100,102-104
switchport mode trunk
switchport voice vlan 100
no logging event link-status
no keepalive
speed 100
spanning-tree portfast
!
interface GigabitEthernet0/1
switchport access vlan 104
switchport trunk allowed vlan 1,100,102-104
switchport mode trunk
speed 100
duplex full
!
interface GigabitEthernet0/2
description Mirage ACS
switchport trunk allowed vlan 18,81
switchport mode trunk
speed 100
duplex full
!
interface Vlan1
no ip address
no ip route-cache
shutdown
!
interface Vlan104
ip address 10.0.185.201 255.255.255.192
no ip route-cache
!
ip default-gateway 10.0.185.193
no ip http server
snmp-server community sophos RW
radius-server host 10.0.224.150 auth-port 1812 acct-port 1813
radius-server retransmit 3
radius-server key password
!
```

802.1x Dynamic VLAN Assignment

```
line con 0
line vty 0 4
password 7 13151601181B0B382F
transport input telnet
line vty 5 15
password 7 095C4F1A0A1218000F
login authentication LOCAL
transport input ssh
!
!
end

2950SW#
```