

SOPHOS

Sophos NAC Advanced distributed DHCP implementation guide

Product version: 3.2

Document date: March 2011



Contents

1 About This Document.....	3
2 Distributed DHCP Enforcement Overview.....	5
3 Installing DHCP Enforcement.....	6
4 Upgrading DHCP Enforcement.....	35
5 Software Uninstalls.....	41
6 Technical Support.....	42
7 Legal Notices.....	43

1 About This Document

This document helps you implement distributed DHCP enforcement as part of Sophos NAC Advanced. DHCP enforcement enables you to identify managed and unmanaged endpoints attaching to your network, assess their security levels, and control their network access. If most of your DHCP servers are co-located with Sophos NAC Advanced, you do not need to install the distributed DHCP enforcement components. For standard DHCP configuration, see the *Sophos NAC Advanced DHCP enforcement guide*.

You must either install or upgrade to Sophos NAC Advanced version 3.2.2 before installing the distributed DHCP enforcement components. For more information, see the *Sophos NAC Advanced installation guide*.

This document contains information about the following:

- Installing and configuring the distributed DHCP enforcement components.
- Upgrading your existing DHCP implementation to use the distributed DHCP enforcement components.

This guide is for you if:

- You are using Sophos NAC Advanced.
- You are using DHCP enforcement at various locations around the world, with DHCP servers residing at those locations.

Important: We recommend that you use DHCP enforcement for unknown endpoints and guest endpoints using the Dissolvable Agent. Additionally, we recommend Agent enforcement for known endpoints using the Quarantine Agent.

1.1 System Requirements

You must install Sophos NAC Advanced before installing the distributed DHCP enforcement components. The distributed DHCP enforcement components consist of two installers: DHCP Cache Databases and DHCP Cache Server. The DHCP Cache Databases and DHCP Cache Server have the same system requirements as the Sophos NAC Advanced system requirements.

Note: If you are using SQL Server 2008, you must install the SQL Distributed Management Objects (SQL-DMO) prior to installing the DHCP Cache Databases.

The distributed DHCP enforcement component system requirements are:

- Internet Authentication Service (IAS) (Windows Server 2003) or Network Policy Server (Windows Server 2008)
- Microsoft Messaging Queue (MSMQ)
- One standard domain account on the domain controller, created before installing Sophos NAC Advanced. This service account must have a password that never expires, and must be set so the password cannot be changed. This service account must also have **read** access to the users' **member of** attribute.

For system requirements, go to the system requirements page of the Sophos website (<http://www.sophos.com/products/all-sysreqs.html>).

2 Distributed DHCP Enforcement Overview

Sophos distributed DHCP enforcement optimizes the performance of Sophos NAC Advanced when it is implemented on geographically distributed DHCP servers. Install Sophos NAC Advanced at one location and the distributed DHCP enforcement components and DHCP servers at remote locations.

You must either install or upgrade to Sophos NAC Advanced version 3.2.2 before installing the distributed DHCP enforcement components. If you have configured DHCP enforcement in a previous version, the Sophos NAC Advanced upgrade keeps the DHCP configuration intact. No configuration changes to Sophos NAC Advanced settings are required.

The distributed DHCP enforcement installation does not alter the Sophos NAC Advanced default settings. These settings target the most common DHCP implementation so that minimal configuration is required once Sophos NAC Advanced is installed. However, DHCP implementations vary greatly; therefore, additional configuration may be necessary.

The distributed DHCP enforcement components are:

- **DHCP Cache Databases:** The DHCP Cache Databases contain compliance data that is replicated from the Sophos NAC Advanced Compliance Databases. This replication of data allows the DHCP Cache Server to retrieve compliance data and respond more quickly to local DHCP requests. The DHCP Cache Databases are installed in the same geographic location as the DHCP Cache Server, and can be installed on the same server.
- **DHCP Cache Server:** The DHCP Cache Server manages the flow of compliance data among the Sophos NAC Advanced Compliance Databases, the DHCP Cache Databases, and the local DHCP server. The DHCP Cache Server authenticates DHCP compliance requests and sends responses to the DHCP server based on compliance data stored in the DHCP Cache Databases. The DHCP Cache Server is installed in the same geographic location as the DHCP Cache Databases and the local DHCP server, and can be installed on the same server as the DHCP Cache Databases.
- **DHCP Enforcer software:** The DHCP Enforcer software is a standard component of all Sophos NAC Advanced DHCP implementations. You must install the DHCP Enforcer software on the DHCP server in each remote location and configure each DHCP server to communicate with its local DHCP Cache Server for DHCP enforcement to work.

Note: If you are installing and configuring Sophos NAC Advanced DHCP enforcement for the first time, use the Installation Checklist. If you are upgrading existing DHCP enforcement, use the Upgrade Checklist. Detailed instructions for checklist items are provided in this document or the appropriate guide is referenced for detailed information. For more information, see [Installation Checklist](#) (page 6) or [Upgrade Checklist](#) (page 35).

3 Installing DHCP Enforcement

Use this section of the document if you are installing and configuring Sophos NAC Advanced DHCP enforcement for the first time. If you are upgrading existing DHCP enforcement, see [Upgrading DHCP Enforcement](#) (page 35).

3.1 Installation Checklist

Use this installation checklist to verify that you have completed all tasks necessary to install the distributed DHCP enforcement components. This checklist assumes you are not upgrading existing DHCP enforcement software. If you are upgrading, see the [Upgrade Checklist](#) (page 35).

Task	Description	Completed
Sophos NAC Advanced Installation, Configuration, and Compliance Agent Deployment		
1.	Install Sophos NAC Advanced before installing any distributed DHCP enforcement components. For more information, see the <i>Sophos NAC Advanced installation guide</i> .	
2.	Create DHCP exemptions using the Compliance Manager. For more information, see DHCP Exemptions (page 8). DHCP exemptions are for endpoints that are either not able to run the Compliance Agent or do not require compliance assessment, such as servers, routers, printers, or endpoints that are deemed "safe." Endpoints that receive a dynamically assigned IP address through DHCP are the only endpoints that need to be exempted.	
3.	Distribute the Sophos Compliance Agent to known endpoints. For more information, see the <i>Sophos NAC Advanced installation guide</i> .	
Sophos DHCP Cache Installation		
4.	Install the Sophos DHCP Cache Databases. You will use the standard domain account you created for Sophos NAC Advanced when installing the distributed DHCP enforcement components. For more information, see DHCP Cache Databases Installation (page 10). Note: If you are using SQL Server 2008, you must install the SQL Distributed Management Objects (SQL-DMO) prior to installing the DHCP Cache Databases.	

Task	Description	Completed
5.	<p>Install the Sophos DHCP Cache Server. For more information, see DHCP Cache Server Installation (page 11).</p> <p>You can install the DHCP Cache Databases and DHCP Cache Server on a single server. However, scalability, network configuration, or network dependencies may require that you install the DHCP Cache Databases and DHCP Cache Server on separate servers, or that you install the DHCP Cache Server on more than one server. If you install the DHCP Cache Databases and DHCP Cache Server on separate servers, they must be joined to the same domain.</p>	
DHCP Settings on the Sophos DHCP Cache Server		
6.	Create a Connection Request Policy on the DHCP Cache Server. For more information, see Create a Connection Request Policy for DHCP (Windows Server 2003) (page 12) or Create a Connection Request Policy for DHCP (Windows Server 2008) (page 13).	
7.	Add a RADIUS Client for the DHCP server on the DHCP Cache Server. For more information, see Add a RADIUS Client for the DHCP Server (Windows Server 2003) (page 15) or Add a RADIUS Client for the DHCP Server (Windows Server 2008) (page 15).	
Multiple Sophos DHCP Cache Servers Configuration (Optional Tasks)		
8.	If you are installing the DHCP Cache Server on more than one server at each location, you must configure all additional DHCP Cache Servers to be identical to the primary DHCP Cache Server. For more information, see Configuring Multiple DHCP Cache Servers (Optional Tasks) (page 16).	
DHCP Enforcer Settings on the DHCP Server		
9.	<p>Install the DHCP Enforcer software on the DHCP server. For more information, see DHCP Enforcer Software Installation (page 16).</p> <p>Note: After the DHCP Enforcer software is installed, you need to verify that the DHCP Service is running on each DHCP server.</p>	
10.	Add the DHCP Cache Server details to the DHCP Enforcer Configuration Tool on the DHCP server. For more information, see Add the DHCP Cache Server Details (page 17).	
DHCP Server Configuration		
11.	Configure the Microsoft DHCP server to work with the DHCP Enforcer. For more information, see Microsoft DHCP Server Configuration (page 19).	
Sophos Compliance Manager Settings		

Task	Description	Completed
12.	Create a policy. For more information, see Create a Policy (page 25).	
13.	Create a group and assign the policy to the group. For more information, see Create a Group and Assign the Policy to the Group (page 27).	
14.	Verify the DHCP Enforcer settings. For more information, see Verify the Enforcer Settings (page 28).	
15.	Run the DHCP Enforcer report to determine the compliance state of endpoints prior to enabling DHCP enforcement. For more information, see Run the DHCP Enforcer Report (page 28). Note: Use the DHCP Enforcer report to determine whether endpoints will receive the appropriate network access when DHCP enforcement is enabled.	
16.	Verify DHCP Enforcer access templates and enable DHCP enforcement. For more information, see Verify Access Templates and Enable DHCP Enforcement (page 32).	
Sophos Compliance Dissolvable Agent Distribution		
17.	Distribute the Sophos Compliance Dissolvable Agent address to guest endpoints. For more information, see the <i>Sophos NAC Advanced installation guide</i> .	

3.2 DHCP Exemptions

Endpoints can be exempted if they are not able to run the Compliance Agent or do not require compliance assessment, such as servers, routers, printers, or endpoints that are deemed "safe." Endpoints that receive a dynamically assigned IP address through DHCP are the only endpoints that need to be exempted. You must create DHCP exemptions for these endpoints or these endpoints will be denied network access when you enable DHCP enforcement.

Using the Compliance Manager, you can create two types of DHCP exemptions:

- **DHCP Criteria Exemptions:** Exemptions created by MAC address, user class, and vendor class.
- **IP Scope Exemptions:** Exemptions created for network segments.

3.2.1 Create DHCP Criteria Exemptions

Use the Compliance Manager Exemptions page to create exemptions by DHCP criteria. DHCP criteria exemptions are exemptions created with either a single MAC address, user class, or vendor class, or any combination of MAC addresses, user classes, and vendor classes. The DHCP exemption

and DHCP Enforcer access templates are used together to identify an exemption and to determine network access for the exemption.

Procedure

1. Log on to the Compliance Manager.
2. Click **Enforce > Exemptions**. Then, click **Create Exemption** in the lower-left section of the page.
3. Type a name and description for the exemption.
4. Click the **Exemption Type** list box and select **DHCP Criteria**.
5. Under Exemption Criteria, select the **MAC Address**, **User Class**, or **Vendor Class** option button to specify the exemption criteria you want to define, type the appropriate MAC address (or prefix), user class, or vendor class in the provided field, and click **Add**.

Repeat this step as necessary to add additional exemption criteria.

Note: You can use the * to specify wildcard exemptions as long as the * symbol is last. For example, if you specify AA* as the MAC address, all MAC addresses that begin with AA are exempted. Likewise, if you specify AA without the * symbol, only MAC addresses that are named AA are exempted.

6. Click **Select** to add a DHCP Enforcer access template to the exemption, select the Default - DHCP Permit (NULL User Class) access template, and click **OK**.

Note: The Default - DHCP Permit (NULL User Class) access template is pre-defined in Sophos NAC Advanced to permit network access. You have configured this exemption to access the network without a compliance assessment by Sophos NAC Advanced.

7. Click **Save**.

Important: Once you have created exemptions, you can prioritize them on the Exemptions list page. If more than one exemption applies to a particular endpoint, the first exemption associated with that endpoint is used. We recommend that you prioritize the more specific/strict exemptions first and the less specific/strict exemptions last.

3.2.2 Create IP Scope Exemptions

Endpoints that receive a dynamically assigned IP address through DHCP are the only endpoints that can be exempted. Use the Compliance Manager Exemptions page to create exemptions by IP scope. IP scope exemptions are exemptions created for network segments. IP scope exemptions are useful when performing a phased rollout of enforcement throughout the enterprise; you can exempt network segments that you do not want to enforce yet.

Procedure

1. Log on to the Compliance Manager.
2. Click **Enforce > Exemptions**. Then, click **Create Exemption** in the lower-left section of the page.

3. Type a name and description for the exemption.
4. Click the **Exemption Type** list box and select **IP Scope**.
5. Click **Select** to add a DHCP Enforcer access template to the exemption, select the Default - DHCP Permit (NULL User Class) access template, and click **OK**.

Note: The Default - DHCP Permit (NULL User Class) access template is pre-defined in Sophos NAC Advanced to permit network access. You have configured this exemption to access the network without a compliance assessment by Sophos NAC Advanced.

6. Click **Save**.

Important: Once you have created exemptions, you can prioritize them on the Exemptions list page. If more than one exemption applies to a particular endpoint, the first exemption associated with that endpoint is used. We recommend that you prioritize the more specific/strict exemptions first and the less specific/strict exemptions last.

3.3 DHCP Cache Databases Installation

This installs the databases that manage distributed DHCP enforcement. The DHCP Cache Databases communicate with the DHCP Cache Server for DHCP enforcement. The DHCP Cache Databases are installed in the same geographic location as the DHCP Cache Server, and can be installed on the same server.

The Sophos NAC Advanced installation requires that you use a domain account with local administrator privileges. The account installing NAC must be defined as a SQL Server User or must be part of a group that is defined as a SQL Server User, and that SQL Server User must be assigned the sysadmin server role in SQL. You must use this same domain account to install the DHCP Cache Databases. If you install the DHCP Cache Databases and DHCP Cache Server on separate servers, they must also be joined to the same domain.

Note: If you are using SQL Server 2008, you must install the SQL Distributed Management Objects (SQL-DMO) prior to installing the DHCP Cache Databases.

1. Download the DHCP Cache Databases installation from the Sophos website.
2. Double-click the installation file to run the installation.
3. Click **Next** to continue.
4. Read the End-User License Agreement, select the **I Accept the terms of the License Agreement** option button, and then click **Next** to continue.
5. Select the appropriate SQL server database instance and authentication method for the DHCP Cache Databases. Click **Next** to continue.
6. Type the Service Account Information in the appropriate fields. Click **Next** to continue.
This is the standard domain account required by the SQL servers and the DHCP Cache Server. This service account was created during the Sophos NAC Advanced installation.
7. Click **Install** to begin the installation.
The Sophos DHCP Cache Databases are configured, and the installation progress displays.

8. Click **Finish**.

Important: If installation errors occur, use the Event Log to view additional information.

3.4 DHCP Cache Server Installation

This installs the application that manages distributed DHCP enforcement. The DHCP Cache Server communicates with the Sophos NAC Advanced Compliance Databases, DHCP Cache Databases, and the local DHCP server for DHCP enforcement. The DHCP Cache Server is installed in the same geographic location as the DHCP Cache Databases and the local DHCP server.

You can install the DHCP Cache Databases and DHCP Cache Server on a single server. However, scalability, network configuration, or network dependencies may require that you install the DHCP Cache Databases and DHCP Cache Server on separate servers, or that you install the DHCP Cache Server on more than one server. If you install the DHCP Cache Databases and DHCP Cache Server on separate servers, they must be joined to the same domain.

Important: If you are installing the DHCP Cache Server on more than one server at each location, you must configure all additional DHCP Cache Servers to be identical to the primary DHCP Cache Server. For more information, see [Configuring Multiple DHCP Cache Servers \(Optional Tasks\)](#) (page 16).

1. Download the DHCP Cache Server installation from the Sophos website.
2. Double-click the installation file to run the installation.
3. Click **Next** to continue.
4. Read the End-User License Agreement, select the **I Accept the terms of the License Agreement** option button, and then click **Next** to continue.
5. Type the Sophos Compliance Database Server name.
When you are not using the default SQL instance, the server and instance name must be in the form of server\instancename. The installation verifies the connection between the server you are installing and the Compliance Database Server.
6. Type the Sophos DHCP Cache Database Server name.
When you are not using the default SQL instance, the server and instance name must be in the form of server\instancename. The installation verifies the connection between the server you are installing and the DHCP Cache Database Server.
7. Type the Service Account Information in the appropriate fields. Click **Next** to continue.
This is the standard domain account required by the SQL servers and the DHCP Cache Server. This service account information must match the service account information you entered when you installed the Sophos DHCP Cache Databases.
8. Verify the installation directory, server names, and service account information.
9. Click **Install** to begin the installation.

The DHCP Cache Server is configured, and the installation progress displays.

10. Click **Finish**.

Note: If installation errors occur, use the Event Log to view additional information.

3.5 DHCP Server Connection Request Policy and RADIUS Client

For DHCP to function properly, you must create a connection request policy and a RADIUS client for the DHCP server. Both of these tasks are performed on the DHCP Cache Server. The connection request policy differentiates DHCP compliance requests from other requests. The DHCP server must be a RADIUS client so that the DHCP server is permitted to send enforcement requests to the DHCP Cache Server.

3.5.1 Create a Connection Request Policy for DHCP (Windows Server 2003)

To use DHCP enforcement, you must create a connection request policy on the Sophos DHCP Cache Server. The connection request policy differentiates DHCP compliance requests from other requests. The policy is created so that the DHCP Cache Server can distinguish this request from non-DHCP requests and provide proper enforcement.

Note: For distributed DHCP enforcement, you must create the connection request policy on the DHCP Cache Server instead of the Compliance Application Server.

1. From the Start menu on the Sophos DHCP Cache Server, click **Administrative Tools > Internet Authentication Service**.

IAS opens.

2. Click **Connection Request Processing**.
3. Right-click **Connection Request Policies**, and then click **New Connection Request Policy**.

The Connection Request Policy Wizard displays.

4. Click **Next**.
5. Select the **A custom policy** option button.
6. Type DHCP as the policy name for the connection request policy, and then click **Next**.

The name **DHCP** indicates that this connection request policy is used for DHCP enforcement.

7. Click **Add** to add a policy condition.
8. Select **User-Name**, and then click **Add**.
9. Type `^[0-9a-f]{2,32}$` as the User-Name, and then click **OK**.

Note: For the purpose of DHCP, Sophos uses a MAC address for a User-Name. This value takes the form of a hex string containing 2-32 characters.

10. Click **Add** to add another policy condition.
11. Select **Calling-Station-ID**, and then click **Add**.

12. Type `^[0-9a-f]{2,32}$` as the Calling-Station-ID, and then click **OK**.

Note: For the purpose of DHCP, Sophos uses a MAC address as the Calling-Station-ID. This value takes the form of a hex string containing 2-32 characters.

13. Click **Add** to add another policy condition.

14. Select **Service-Type**, and then click **Add**.

15. Select **Authenticate Only**, and then click **Add** to add Authenticate Only to the Selected Types.

16. Click **OK**.

17. Click **Add** to add another policy condition.

18. Select **Client-Friendly-Name**, and then click **Add**.

19. Type DHCP, click **OK**, and then click **Next**.

Note: The RADIUS client name must contain "DHCP" somewhere in its name for DHCP to work properly. The client name is not case sensitive.

20. Click **Edit Profile**.

21. Click the **Accept user without validating credentials** option button, and then click **OK**.

Note: The connection request policy is set to not require user authentication because this step is done by the Compliance Agent. Sophos NAC Advanced performs authorization on all DHCP request packets. Users that are not authenticated by the Agent or are not exempted are considered non-compliant.

22. Click **Next**.

23. Click **Finish**.

Note: If you double-click the policy you just created, a window displays with the policy conditions.

3.5.2 Create a Connection Request Policy for DHCP (Windows Server 2008)

To use DHCP enforcement, you must create a connection request policy on the Sophos DHCP Cache Server. The connection request policy differentiates DHCP compliance requests from other requests. The policy is created so that the DHCP Cache Server can distinguish this request from non-DHCP requests and provide proper enforcement.

Note: For distributed DHCP enforcement, you must create the connection request policy on the DHCP Cache Server instead of the Compliance Application Server.

1. From the Start menu on the Sophos DHCP Cache Server, click **Administrative Tools > Network Policy Server**.

Network Policy Server opens.

2. Under Policies, right-click **Connection Request Policies**, and click **New**.

The New Connection Request Policy Wizard displays.

3. Type DHCP as the policy name for the connection request policy, leave **Unspecified** as the network connection method, and then click **Next**.

The name **DHCP** indicates that this connection request policy is used for DHCP enforcement.

4. Click **Add** to add a policy condition.
5. Select **User Name**, and then click **Add**.
6. Type `^[0-9a-f]{2,32}$` as the User Name, and then click **OK**.

Note: For the purpose of DHCP, Sophos uses a MAC address for a User Name. This value takes the form of a hex string containing 2-32 characters.

7. Click **Add** to add another policy condition.
8. Select **Calling Station ID**, and then click **Add**.
9. Type `^[0-9a-f]{2,32}$` as the Calling-Station-ID, and then click **OK**.

Note: For the purpose of DHCP, Sophos uses a MAC address as the Calling Station ID. This value takes the form of a hex string containing 2-32 characters.

10. Click **Add** to add another policy condition.
11. Select **Service Type**, and then click **Add**.
12. Select **Authenticate Only**, and then click **Add**.
13. Click **OK**.
14. Click **Add** to add another policy condition.
15. Select **Client Friendly Name**, and then click **Add**.
16. Type DHCP, click **OK**, and then click **Next**.

Note: The RADIUS client name must contain "DHCP" somewhere in its name for DHCP to work properly. The client name is not case sensitive.

17. In the **Authentication** section, select the **Accept users without validating credentials** option button, and then click **Next**.

Note: The connection request policy is set to not require user authentication because this step is done by the Compliance Agent. Sophos NAC Advanced performs authorization on all DHCP request packets. Users that are not authenticated by the Agent or are not exempted are considered non-compliant.

18. Click **Next**. You do not need to set attributes for this policy.
19. Click **Finish**.

Note: If you double-click the policy you just created, a window displays with the policy conditions.

3.5.3 Add a RADIUS Client for the DHCP Server (Windows Server 2003)

On the Sophos DHCP Cache Server, you must add your DHCP server to IAS. The DHCP server must be a RADIUS client so that the DHCP server is permitted to send enforcement requests to the DHCP Cache Server.

Note: For distributed DHCP enforcement, you must create the RADIUS client on the DHCP Cache Server instead of the Compliance Application Server.

1. From the Start menu on the Sophos DHCP Cache Server, click **Administrative Tools > Internet Authentication Service**.

This step opens IAS.

2. Right-click **RADIUS Clients**, and click **New RADIUS Client**.
3. Type DHCP in the **Friendly name** field, and then type the IP address or DNS name of your DHCP server in the **Client address** field. Click **Next** to continue.

Note: Name the RADIUS client **DHCP** for DHCP to work properly. This name matches the policy name you gave the Connection Request Policy.

4. Type DHCP as the shared secret of your DHCP server in the appropriate field and confirm the shared secret. You will use the DHCP shared secret later when you configure the DHCP server to work with the DHCP Cache Server.

Note: In the Client-Vendor field, leave the default RADIUS Standard option unchanged.

5. Verify that the **Request must contain the Message Authenticator attribute** check box is **not** selected.
6. Click **Finish**.

3.5.4 Add a RADIUS Client for the DHCP Server (Windows Server 2008)

On the Sophos DHCP Cache Server, you must add your DHCP server to Network Policy Server. The DHCP server must be a RADIUS client so that the DHCP server is permitted to send enforcement requests to the DHCP Cache Server.

Note: For distributed DHCP enforcement, you must create the RADIUS client on the DHCP Cache Server instead of the Compliance Application Server.

1. From the Start menu on the Sophos DHCP Cache Server, click **Administrative Tools > Network Policy Server**.

Network Policy Server opens.

2. Right-click **RADIUS Clients**, and click **New RADIUS Client**.

3. Type DHCP in the **Friendly name** field, and then type the IP address or DNS name of your DHCP server in the **Address (IP or DNS)** field.

Note: Name the RADIUS client **DHCP** for DHCP to work properly. This name matches the policy name you gave the Connection Request Policy.

4. Type DHCP as the shared secret of your DHCP server in the appropriate field and confirm the shared secret. You will use the DHCP shared secret later when you configure the DHCP server to work with the DHCP Cache Server.

Note: In the Vendor name field, leave the default RADIUS Standard option unchanged.

5. Verify that the **Access-Request messages must contain the Message-Authenticator attribute** check box is **not** selected.
6. Click **OK**.

3.6 Configuring Multiple DHCP Cache Servers (Optional Tasks)

Multiple DHCP Cache Servers enable you to scale DHCP enforcement at each location. You must install and properly configure all additional DHCP Cache Servers to be identical with the primary DHCP Cache Server.

The following tasks are required when multiple DHCP Cache Servers are used:

- Create a RADIUS Client for each DHCP server on each DHCP Cache Server. For more information, see [Add a RADIUS Client for the DHCP Server \(Windows Server 2003\)](#) (page 15) or [Add a RADIUS Client for the DHCP Server \(Windows Server 2008\)](#) (page 15).
- Add each DHCP Cache Server to the DHCP Enforcer Configuration Tool on each DHCP server. For more information, see [Add the DHCP Cache Server Details](#) (page 17).
- Specify load balancing options for the DHCP Cache Servers in the DHCP Enforcer Configuration Tool on each DHCP server. For more information, see step 10 in [Add the DHCP Cache Server Details](#) (page 17).

3.7 DHCP Enforcer Software Installation

Install the DHCP Enforcer software on your Microsoft DHCP server. The DHCP Enforcer software includes the DHCP Enforcer and the DHCP Enforcer Configuration Tool.

1. Download the DHCP Enforcer software from the Sophos website.
2. Double-click the DHCP Enforcer software installation file to run the DHCP Enforcer software installation.
3. Click **Next**.

The DHCP Enforcer installation wizard displays.

4. Select the **Complete** option button. Click **Next**.

Note: The installation scans for the Microsoft DHCP server and automatically installs the appropriate DHCP Enforcer software components.

5. Click **Install** to install the software.
6. Click **Finish**.

Note: Once installation completes, use the DHCP Enforcer Configuration Tool to configure settings on your DHCP server. For more information, see [Add the DHCP Cache Server Details](#) (page 17).

Note: After the DHCP Enforcer software is installed, you need to verify that the DHCP Service is running on each DHCP server.

3.8 Add the DHCP Cache Server Details

The DHCP server must be configured to communicate with the DHCP Cache Server for DHCP enforcement. Therefore, you must add the DHCP Cache Server to the DHCP Enforcer Configuration Tool on the DHCP server. The DHCP Enforcer Configuration Tool is installed as part of the DHCP Enforcer installation and supports Windows servers running Microsoft Dynamic Host Configuration Protocol (DHCP) software.

1. From the Start menu on the DHCP server, select **Sophos > NAC > Support Tools > DHCP Enforcer Configuration Tool**.

The DHCP Configuration window displays with the Enforcer tab selected.

2. Leave the **Default User Class** field blank.

The default user class is used only if one is not returned from the DHCP Cache Server. For example, a user class may not be returned from the DHCP Cache Server when the DHCP Cache Server is down, the connection between the DHCP server and the DHCP Cache Server is down, or when Sophos NAC Advanced cannot find a user class for the scope. The default user class is NULL, which is pre-defined in Sophos NAC Advanced to permit network access.

3. In the RADIUS Enforcer Servers section, click **Add** to specify the DHCP Cache Server. The DHCP Cache Server must be able to communicate with the DHCP server.

Important: For distributed DHCP enforcement, you must specify the DHCP Cache Server instead of the Compliance Application Server. If you are upgrading your DHCP enforcement software to use the distributed DHCP enforcement components, you must delete any previous entries for Compliance Application Servers.

4. Leave the **Enable** check box selected to keep the DHCP Cache Server active.
5. Type the IP address of the DHCP Cache Server in the **IP Address** field. Otherwise, click **Resolve IP...**, type the hostname in the provided field, and then click **OK**.
6. Leave the default authentication port and accounting port settings unless your DHCP server is using different ports.

7. Type DHCP as the shared secret, and type DHCP again to confirm the shared secret of the DHCP server.

DHCP matches the shared secret that was used when adding a RADIUS client for the DHCP server on the DHCP Cache Server. For more information, see [Add a RADIUS Client for the DHCP Server \(Windows Server 2003\)](#) (page 15) or [Add a RADIUS Client for the DHCP Server \(Windows Server 2008\)](#) (page 15).

8. Click **OK**.

Note: Leave the default settings on the Microsoft tab because no changes are required.

9. Repeat steps 3 through step 8 to specify more than one DHCP Cache Server.
10. If you specified more than one DHCP Cache Server, select the appropriate **Access for Multiple Servers** option button.

Sequential access attempts to access all DHCP Cache Servers in the order specified. Balanced access attempts to access all servers equally, using load balancing.

Note: You can prioritize the order of the servers for sequential access using the **Move Up** and **Move Down** buttons.

11. Click **OK**.

3.8.1 Configuration Tool Fields and Descriptions

Fields	Descriptions
Enforcer tab	
Enable Policy Compliance	When selected, policy compliance and reporting are enabled for all DHCP request packets, except for those identified by the reserved option code.
Attempts	Designates how many times policy compliance is initiated for a DHCP request packet.
Timeout	Designates, in seconds, how long the DHCP server will wait before initiating another policy compliance check.
Default User Class	Identifies the user class to use if the user class defined in policy cannot be obtained because of an error during a policy compliance assessment.
Enable Reserved Option Reporting	When selected, reporting is enabled to identify reserved option codes.
Attempts	Designates how many times reporting is initiated for a DHCP request packet.

Fields	Descriptions
Timeout	Designates, in seconds, how long the DHCP server will wait before initiating another reporting event.
Access for Multiple Servers	Designates how access is performed for multiple DHCP Cache Servers. Sequential access attempts to access all DHCP Cache Servers in the order specified. Balanced access attempts to access all DHCP Cache Servers equally, using load balancing. Note: You can prioritize the order of the DHCP Cache Servers for sequential access using the Move Up and Move Down buttons.
DHCP Enforcer RADIUS Enforcer Server Settings window	
Note: The fields on this window are in relation to the DHCP Cache Server.	
Enable	Displays whether the DHCP Cache Server is enabled. When it is enabled, the DHCP Cache Server is used for policy compliance and reporting activity.
IP Address	Designates the IP address of the DHCP Cache Server.
Authentication Port	Designates the authentication port of the DHCP Cache Server.
Accounting Port	Designates the accounting port of the DHCP Cache Server.
Shared Secret	Identifies the shared secret of the DHCP server. The shared secret matches the shared secret that was used in the DHCP server configuration. For more information, see Add a RADIUS Client for the DHCP Server (Windows Server 2003) (page 15) or Add a RADIUS Client for the DHCP Server (Windows Server 2008) (page 15).
Confirm Shared Secret	Confirms the DHCP server shared secret. The shared secret matches the shared secret that was used in the DHCP server configuration. For more information, see Add a RADIUS Client for the DHCP Server (Windows Server 2003) (page 15) or Add a RADIUS Client for the DHCP Server (Windows Server 2008) (page 15).
Resolve IP window	
Hostname	Identifies the hostname, if the IP address is not known, of the DHCP Cache Server.

3.9 Microsoft DHCP Server Configuration

To configure the Microsoft DHCP server, you must create DHCP user classes that match the user classes that are pre-defined in Sophos NAC Advanced. The NULL user class is for compliant or

partially compliant endpoints. Compliant and partially compliant endpoints are permitted network access.

The NACDeny user class is for non-compliant endpoints and endpoints that do not have the Compliance Agent installed. Non-compliant endpoints are quarantined and receive limited network access. Network access is determined by the Microsoft scope options you define. For more information, see [Modify Microsoft Scope Options to Specify User Classes](#) (page 21).

If you have printers or non-Windows based OSs on the network that receive a dynamically assigned IP address through DHCP, you must create exemptions for these endpoints using the Compliance Manager. For more information, see [DHCP Exemptions](#) (page 8). You must create DHCP exemptions for these endpoints or these endpoints will be denied network access when you enable DHCP enforcement. When exempted, endpoints are permitted network access. For more information, see [Create DHCP Criteria Exemptions](#) (page 8) and [Create IP Scope Exemptions](#) (page 9).

Note: This section refers to a NULL user class. Microsoft refers to the NULL user class as the default user class on the DHCP server. The NULL user class is pre-defined in Sophos NAC Advanced to permit network access.

3.9.1 Define Microsoft DHCP User Classes

To configure the Microsoft DHCP server, you must create DHCP user classes that match the user classes that are pre-defined in Sophos NAC Advanced. The NULL user class is pre-defined in Sophos NAC Advanced for compliant or partially compliant endpoints. Compliant and partially compliant endpoints are permitted network access. The NACDeny user class is pre-defined in Sophos NAC Advanced for non-compliant endpoints, endpoints that do not have the Compliance Agent installed, and endpoints that have not run the Dissolvable Agent. Non-compliant endpoints are quarantined and receive limited network access.

Note: The NULL user class is pre-defined on the Microsoft DHCP server so that you do not need to define a user class for NULL.

1. On the Microsoft DHCP server, open the DHCP management console, right-click the DHCP server name, and select **Define User Classes**.

The DHCP User Classes window displays.

2. Click **Add**.

The New Class window displays.

3. Type NACDeny as the display name and Sophos NAC Advanced Deny User Class as the description.
4. Place the cursor in the ASCII column, and then type NACDeny as the user class.

Note: This user class is case sensitive and must be typed exactly as it appears in this step so that the user class matches the pre-defined user class in Sophos NAC Advanced. The NACDeny user class is pre-defined in the Default - DHCP Deny (NACDeny User Class) access template.

5. Click **OK** to create the NACDeny user class.

Note: The NULL user class is pre-defined on the Microsoft DHCP server so that you do not need to define a user class for NULL.

6. Click **Close** to close the DHCP User Classes window.

3.9.2 Modify Microsoft Scope Options to Specify User Classes

The DHCP Enforcer operates by matching a user class to every DHCP request. Endpoints that are not compliant and not exempted, including endpoints that do not have the Compliance Agent installed and those that have not run the Dissolvable Agent, are matched to the NACDeny user class that is pre-defined in Sophos NAC Advanced and configured on the DHCP server. Endpoints that are compliant and partially compliant are matched to the NULL user class that is pre-defined in Sophos NAC Advanced and the DHCP server. The NULL user class permits full access to the internal network and the Internet. The NACDeny user class quarantines non-compliant endpoints. You can provide limited network access by specifying static routes for any DNS servers, remediation servers, or other network resources that you want non-compliant endpoints to access.

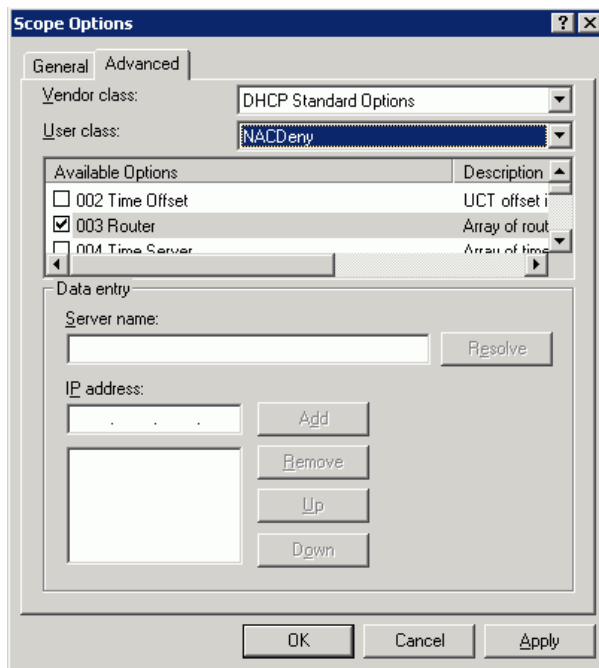
Important: These instructions modify just one scope. For additional scopes, you must repeat these instructions. One scope usually equates to one network segment.

1. On the Microsoft DHCP server, open the DHCP management console, expand the folder for the appropriate scope, right-click **Scope Options**, and then select **Configure Options**.
2. Select the **Advanced** tab, and then select **NACDeny** from the **User class** list box.

You defined the NACDeny user class on the DHCP server. For more information, [Define Microsoft DHCP User Classes](#) (page 20).

3. Select the **003 Router** check box from the Available Options area.

Note: You are configuring quarantine for those endpoints that are not compliant, not exempted, do not have the Compliance Agent installed, or have not run the Dissolvable Agent. This configuration applies an empty gateway to endpoints so that they are denied network access. You can provide limited network access by specifying static routes for any DNS servers, remediation servers, a proxy server for Internet access, or other network resources that you want non-compliant endpoints to access while in quarantine.



4. Click **Apply** to set this option.

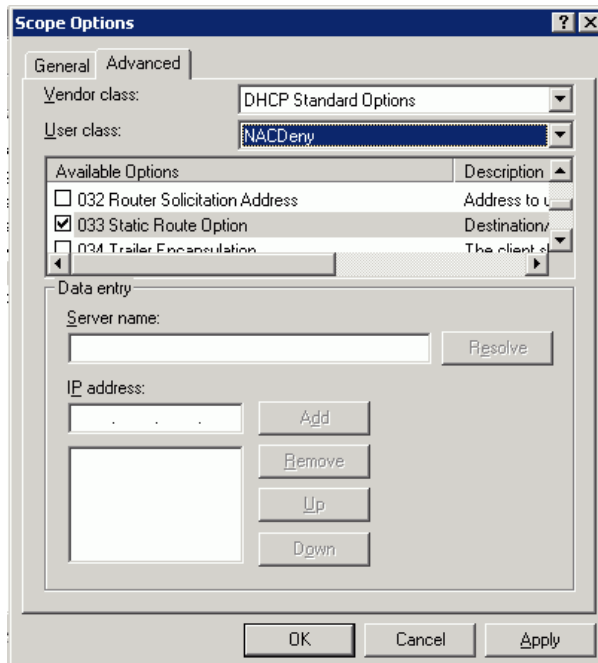
Do not add any IP addresses for the router user class. This step applies an empty gateway to endpoints so that they are denied network access.

5. Select **NACDeny** from the **User class** list box.

Note: You created the NACDeny user class on the DHCP server to quarantine users. For more information, see [Define Microsoft DHCP User Classes](#) (page 20).

6. Select the **033 Static Route Option** check box from the Available Options area.

Endpoints that are not compliant, not exempted, do not have the Compliance Agent installed, or have not run the Dissolvable Agent are not given a gateway. You are configuring a static route to the DHCP Cache Server so that the non-compliant endpoints can communicate with the DHCP Cache Server.



7. Type the server name of the DHCP Cache Server in the **Server name** field, and then click **Resolve**; or type the IP address of the DHCP Cache Server in the **IP address** field, and then click **Add**.

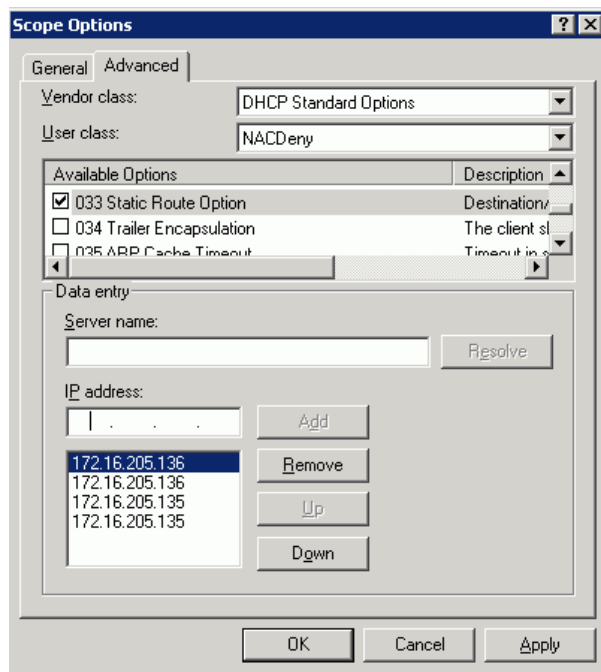
Note: The DHCP static route option requires a pair of IP addresses, destination and router, for each static route. For addresses on the same segment as the endpoint, add this address again so that it appears twice in the list of IP addresses. For addresses on a different segment, add the address for the router through which the endpoint will reach the destination.

8. Type the server name of your remediation server in the **Server name** field, and then click **Resolve**; or type the IP address of the remediation server in the **IP address** field, and then click **Add**.

Note: The DHCP static route option requires a pair of IP addresses, destination and router, for each static route. For addresses on the same segment as the endpoint, add this address again so that it appears twice in the list of IP addresses. For addresses on a different segment, add the address for the router through which the endpoint will reach the destination.

- Repeat step 8 to add additional IP addresses for any DNS servers, remediation servers, a proxy server for Internet access, or other network resources that you want non-compliant endpoints to access while in quarantine.

Note: Permitting access to only these static routes places non-compliant endpoints in quarantine. Network access is limited to those static IP addresses you have defined and to the Internet. Internal IP addresses are not reachable. The following addresses are for illustration purposes only.



- Click **OK** to finish.

Important: These instructions modify just one scope. For additional scopes, you must repeat these instructions. One scope usually equates to one network segment.

3.10 Compliance Manager Tasks

DHCP enforcement should work with little or no configuration changes using the Compliance Manager. At a minimum, you need to create a policy, create a group and assign the policy to the group, and then enable DHCP enforcement.

Compliance Manager tasks include the following:

- Create a policy.
- Create a group and assign the policy to the group.

- Verify that the pre-defined DHCP Enforcer settings are appropriate for your DHCP implementation.
- Run the Compliance Manager DHCP Enforcer report to review DHCP report information.
Note: Use the DHCP Enforcer report to determine whether endpoints will receive the appropriate network access when DHCP enforcement is enabled.
- Verify DHCP Enforcer access templates and enable DHCP enforcement.

3.10.1 Create a Policy

Policies control access to enterprise network resources based on profile evaluations on the endpoint. Policies manage the configuration that determines the endpoint compliance state, messages that display, remediation actions that are performed, and enforcement actions that are taken. Policies contain Agent settings, profiles, and access template assignments.

Important: All policies and policy changes are effective on the network enforcement points immediately, but a policy is not applied on the endpoint until the Agent retrieves it.

Procedure

1. Log on to the Compliance Manager.
2. Click **Manage > Policies**. Then, click **Create Policy** in the lower-left section of the page.
3. Type a name and description for the policy.
4. Leave the policy mode setting.
5. Specify DHCP Agent Settings. These settings apply only if you are implementing DHCP enforcement:
 - **Agent Enforcement Action:** Establishes the method used to obtain new IP addresses for the endpoint. The Agent obtains new IP addresses when the Agent launches and initiates a compliance assessment, when the endpoint compliance state changes, when the policy mode changes, and when the DHCP Enforcer access templates defined in the endpoint's policy change. Available values include:
 - **None:** IP addresses for the endpoint are not released and not renewed. Select None when you are **not** using DHCP enforcement.
 - **Release Renew:** IP addresses for the endpoint are released and then renewed using the DHCP server. The current IP addresses are dropped prior to new IP addresses being obtained. You **must** select Release Renew when using DHCP enforcement.
 - Note:** If an endpoint is running the Dissolvable Agent on Windows Vista and needs to release renew its IP addresses, the Agent will display a message to the user requesting either administrative credentials or a user-initiated restart of the endpoint.
6. Click **Add Profiles**.

7. 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. Policy behavior is evaluated as follows:

- **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 are evaluated in this way. Application profiles that you want to prevent on the endpoint can be evaluated in this way.

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.

8. 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.

9. 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.

Deselect the check boxes for the operating systems on which you do not want the applications or patches evaluated. As necessary, use the arrows to prioritize the application evaluations. Grayed out boxes indicate that an evaluation of the application on a particular operating system is not available or supported.

10. Click **Save**.

Once you create a policy, you must ensure that you have assigned the policy to a group. A specific group can be assigned only one policy; however, a single policy can be assigned to an unlimited number of groups.

3.10.2 Create a Group and Assign the Policy to the Group

Creating a group establishes a name that maps a group of users or endpoints to a user store, and assigns a policy to the group.

You must assign policies to groups to ensure that endpoints registering with Sophos NAC Advanced can be assessed against a compliance policy. Group membership is determined when the endpoint accesses Sophos NAC Advanced using the Agent. The policy is retrieved according to the designated policy refresh interval.

You can assign a policy to a group when you create the group or on the Groups list page. A specific group can be assigned only one policy; however, a single policy can be assigned to an unlimited number of groups. Once you have created groups, you can prioritize them on the Groups list page.

Procedure

1. Log on to the Compliance Manager.
2. Click **Manage > Groups**. Then, click **Create Group** in the lower-left section of the page.
3. Type a name and description for the group.

Important:

- If you are using Sophos NAC Advanced as a RADIUS proxy (configuring the software in proxy mode in front of another RADIUS server), the group name must match the value returned from the RADIUS server for the user to receive the correct policy. If the group name does not match the RADIUS server value or no group name is returned from the RADIUS server, the user receives the default policy, if one is assigned.
 - If you are using Active Directory, the group name must match a security group name in the user store. If the group name does not match a security group in the user store, the user receives the default policy, if one is assigned.
4. Click the **Policy** list box to select the policy with which the group will be associated.

Important: If no policy is selected and a default policy is not assigned, then the endpoint is not assessed for compliance. In this case, the endpoint is assigned the following access template. We recommend that you always assign a default policy.

- **DHCP Enforcer:** The endpoint is assigned the DHCP Enforcer access template associated with the Default access state in the **Configure System > Enforcer Settings** area.

5. Click **Save**.

Important: Once you have created groups, you can prioritize them on the Groups list page. If more than one group applies to a particular endpoint, the first group associated with that endpoint is used. We recommend that you prioritize the more specific/strict groups first and the less specific/strict groups last.

3.10.3 Verify the Enforcer Settings

The Compliance Manager Enforcer Settings page enables you to configure settings that specify how enforcement is performed by Sophos NAC Advanced. Verify that the pre-defined settings are appropriate for your DHCP implementation. In most cases, you will not have to make changes to the Enforcer settings.

Procedure

1. Log on to the Compliance Manager.
2. Click **Configure System > Enforcer Settings**.
3. Leave the default values in the Policy Threshold Settings.
4. Leave the default values in the Enforcer Server Settings.
5. Click the **DHCP Enforcer** tab.
6. Verify that the access templates are correct for each access state. The following access states are available:
 - **Unknown Endpoint:** Determines network access when no compliance record exists. Unknown endpoints are unmanaged and not exempted. The assigned access template denies network access to unknown endpoints.
 - **Maintenance Mode/Enforcer Override:** Determines network access when the system is in maintenance mode or enforcement on the DHCP Enforcer has been disabled using the Override Enforcers check box. The assigned access template permits network access to endpoints.
 - **Default:** Determines network access if a default policy is not designated or an associated access template cannot be found. The assigned access template permits network access to endpoints.
7. To add or change access templates for a particular access state, click **Select**, select the check boxes beside the access templates and beside the access states the templates apply to, and click **OK**.
8. As necessary, use the arrows to prioritize access templates.

If more than one template applies to a particular state, the first template that meets the state is used. We recommend that you prioritize the more specific/strict access templates first and the less specific/strict access templates last.
9. Click **Save**.

3.10.4 Run the DHCP Enforcer Report

Run the Compliance Manager DHCP Enforcer report to determine the compliance state of endpoints prior to enabling DHCP enforcement. The DHCP Enforcer report can be used to determine whether the correct access template will be applied when enforcement is enabled.

The DHCP Enforcer report is available using current or archived data. Server settings designate how long data is kept current and when the data is archived. The default settings are to retain the

current data for two days and to archive data once a day. The date/time of the last data archive displays beside the Use Data from Last Archive check box.

- **DHCP Enforcer:** This report provides details on the compliance state of endpoints, the associated access template, and the reason a particular access template was applied. You can access the Exemptions page from the DHCP Enforcer report to create exemptions for endpoints that require it prior to enabling DHCP enforcement.

Note: In some cases, since real-time data must be merged from multiple sources, current data may be incomplete.

Procedure

1. Log on to the Compliance Manager.
2. Click **Report > Troubleshooting**.
3. Click the **Report Type** list box and select **DHCP Enforcer**.
4. If you want to use archived data, select the **Use Data from Last Archive** check box.
5. If applicable, click the **plus sign** beside **Report Criteria**, and type or select the appropriate search options. You can also click the **Custom Sort** link to expand your sort options; custom sort options are changed temporarily for the report while it is being run.

For more information on specific fields, see the Fields and Descriptions table.

Note: You can use the * or % symbol to perform a wildcard search on most fields. For example, if you type M% in the Returned User Class field, all user classes that begin with the letter M display. Likewise, if you type M without the % symbol in the Returned User Class field, only user classes that are named M display.

6. Click **Run**.

Fields and Descriptions

Field	Description
Summary Report Entry	
Date/Time	Date and time of the network access attempt. Note: The date and time are derived from the time zone of the web browser accessing the Compliance Manager.
MAC Address	MAC address of the device attempting to connect to the network. The MAC address listed is assigned to the NIC associated with the DHCP client request.
Computer Name	Name of the device attempting to connect to the network. The computer name is derived from the client request.

Field	Description
Compliance State	<p>Endpoint compliance state, assigned during the compliance assessment. Available compliance states are:</p> <ul style="list-style-type: none"> ■ Compliant: The assessment determined the endpoint is compliant with the policy. The compliant DHCP Enforcer access templates associated with the policy determine network access. ■ Partially Compliant: The assessment determined the endpoint is partially compliant with the policy. The partially compliant DHCP Enforcer access templates associated with the policy determine network access. ■ Non-Compliant: The assessment determined the endpoint is not compliant with the policy. The non-compliant DHCP Enforcer access templates associated with the policy determine network access. <p>Important: The endpoint's compliance state is determined by the evaluation of profile conditions on the endpoint coupled with the assigned policy behavior for that profile type. Each condition's compliance state is rolled up to the profile level, and multiple profiles are rolled up to the policy level to determine the overall compliance state. The least compliant state determines the overall compliance state. Once a compliance state is determined, network access based on that compliance state can be enforced using the access templates assigned in policy.</p>
Template Name (Version)	<p>Name and version of the access template that determined the action taken by the DHCP Enforcer. The access template used is based on the reason. Available access templates include the following default templates along with enterprise-specific templates:</p> <ul style="list-style-type: none"> ■ Default - DHCP Permit (NULL User Class): DHCP Enforcer access template used to return the NULL user class to permit network access. ■ Default - DHCP Deny (NACDeny User Class): DHCP Enforcer access template used to return the NACDeny user class to deny network access.
Reason	<p>Reason that a particular access template was assigned by the DHCP Enforcer. Available reasons are:</p> <ul style="list-style-type: none"> ■ Assessment: The assessment performed by the Agent determined the compliance state. The DHCP Enforcer access templates associated with the policy compliance state determine network access. ■ Default Template: The endpoint may have an associated policy or be a designated exemption, but an associated access template was not found. The Default access templates designated in the Configure System > Enforcer Settings area determine network access. ■ Enforcer Override: Enforcement was not checked. If the Override Enforcers check box is selected in the Configure System > Enforcer Settings area, the

Field	Description
	<p>Maintenance Mode/Enforcer Override access templates also designated in that area determine network access.</p> <ul style="list-style-type: none"> ■ Exempted: The endpoint is exempted based on exemption criteria defined in the Enforce > Exemptions area. The access templates associated with the exemption criteria determine network access. The following Exempted sub-reasons display in parentheses: <ul style="list-style-type: none"> ■ User Class: The user class was specified as an exemption. ■ Vendor Class: The vendor class was specified as an exemption. ■ MAC: The MAC address was specified as an exemption. ■ IP Scope: The IP scope was specified as an exemption. ■ Maintenance Mode: The software is in maintenance mode. The Maintenance Mode/Enforcer Override access templates designated in the Configure System > Enforcer Settings area determine network access. ■ Policy Retrieval Error: The endpoint's compliance state is out-of-date according to the DHCP Policy Update Threshold field configured in the Configure System > Enforcer Settings area. The policy's DHCP Enforcer access templates associated with the Policy Retrieval Error state determine network access. ■ Remediate: The policy is in Remediate mode. The DHCP Enforcer access templates associated with the Remediate policy mode determine network access. ■ Report Only: The policy is in Report Only mode. The DHCP Enforcer access templates associated with the Report Only policy mode determine network access. ■ Reserved: The MAC address of the device requesting network access is reserved as a special device on the DHCP server. ■ System Error: The Enforcer encountered an error that prevented successful completion of its operation. The SystemErrors registry setting on the Compliance Application Server is set by default to deny network access. ■ Template Error: An associated access template was not found, and the Default access templates designated in the Configure System > Enforcer Settings area could not be used. If this error is received, network access is determined by the DHCP server, which will not return a user class and will deny access to the user. ■ Unknown Endpoint: No compliance record exists. The Unknown Endpoint access templates designated in the Configure System > Enforcer Settings area determine network access.

Field	Description
Returned User Class	DHCP user class returned to the DHCP server by the DHCP Enforcer for enforcement.
Username	Username of the user initiating the network access attempt.
DHCP Server	IP address of the DHCP server requesting network access from the DHCP Enforcer. This is the DHCP server that the DHCP Enforcer software is installed on.
Exempt	Icon that accesses the Exemptions page to create an exemption based on the DHCP criteria in this report entry. The icon displays only if the reason is not Exempted.
Detailed Report Entry	
Agent Enforcement Action	<p>Action taken by the endpoint. The endpoint initiates releasing and renewing IP addresses based on the Agent Enforcement Action specified in policy. The Agent obtains new IP addresses when the Agent launches and initiates a compliance assessment, when the endpoint compliance state changes, and when the DHCP Enforcer access templates defined in the user's policy change. Available values include:</p> <ul style="list-style-type: none"> ■ None: IP addresses for the endpoint are not released and not renewed. ■ Release Renew: IP addresses for the endpoint are released and then renewed using the DHCP server. The current IP addresses are dropped prior to new IP addresses being obtained. ■ Triple Dash (---): The Agent did not report an action.
Vendor Class	Vendor class of the DHCP client.
DHCP Relay	IP address of the DHCP relay (if present in the original DHCP request) used by the DHCP Enforcer to select a DHCP Enforcer access template. 0.0.0.0 displays if a DHCP relay is not used.
Transaction ID	Transaction ID that is returned from the DHCP server. The transaction ID associates DHCP client messages with server responses.

3.10.5 Verify Access Templates and Enable DHCP Enforcement

To enable DHCP enforcement, you must change the Policy Mode from Report Only to Enforce in the appropriate policies. At the same time you enable enforcement, verify that the pre-defined access template assignments are appropriate for your DHCP implementation.

Important: All policies and policy changes are effective immediately, but a policy is not applied on the endpoint until the Agent retrieves it.

Procedure

1. Log on to the Compliance Manager.
2. Click **Manage > Policies**. Then, click the name of the policy you want to update.
3. Click the **Policy Mode** list box to change the policy mode to Enforce. 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 5.
 - **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 5.
 - **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 5.
4. Specify the DHCP Agent Settings.
 - **Agent Enforcement Action:** Establishes the method used to obtain new IP addresses for the endpoint. The Agent obtains new IP addresses when the Agent launches and initiates a compliance assessment, when the endpoint compliance state changes, and when the DHCP Enforcer access templates defined in the endpoint's policy change. Available values include:
 - **None:** IP addresses for the endpoint are not released and not renewed. Select **None** when you are **not** doing DHCP enforcement.
 - **Release Renew:** IP addresses for the endpoint are released and then renewed using the DHCP server. The current IP addresses are dropped prior to new IP addresses being obtained. You **must** select **Release Renew** for DHCP enforcement.

5. In the left navigation Network Access area, click **DHCP**. Click the **Enforce** tab and verify the pre-defined access template assignments.

Note: By default, each policy is automatically populated with pre-defined access templates. Ensure that the correct access templates are applied. Leave the pre-defined Report Only and Remediate access template assignments. The pre-defined assignments for Report Only and Remediate permit network access.

Pre-defined DHCP Enforcer Access Templates

- **Policy Retrieval Error:** The endpoint's compliance state is out-of-date according to the DHCP Policy Update Threshold field configured in the **Configure System > Enforcer Settings** area. The pre-defined Default - DHCP Deny (NACDeny User Class) access template quarantines the endpoint and provides limited network access when there is a policy retrieval error.
 - **Compliant:** The endpoint is compliant. The pre-defined Default - DHCP Permit (NULL User Class) access template permits network access when the endpoint is compliant.
 - **Partially Compliant:** The endpoint is partially compliant. The pre-defined Default - DHCP Permit (NULL User Class) access template permits network access when the endpoint is partially compliant.
 - **Non-Compliant:** The endpoint is non-compliant. The pre-defined Default - DHCP Deny (NACDeny User Class) access template quarantines the endpoint and provides limited network access when the endpoint is non-compliant.
6. As necessary, use the arrows to prioritize DHCP Enforcer access templates.
If more than one template applies to a particular state, the first template that meets the state is used. We recommend that you prioritize the more specific/strict access templates first and the less specific/strict access templates last.
 7. Click **Save**.

4 Upgrading DHCP Enforcement

Use this section of the document if you are upgrading Sophos NAC Advanced DHCP enforcement to use the distributed DHCP enforcement components. If you are installing DHCP enforcement for the first time, see [Installing DHCP Enforcement](#) (page 6).

Note: This section requires you to follow procedures in section 3 of this document.

4.1 Upgrade Checklist

Use this checklist to verify that you have completed all tasks necessary to upgrade existing DHCP enforcement software to use the distributed DHCP enforcement components. If you do not have existing software to upgrade, see [Installation Checklist](#) (page 6).

Task	Description	Completed
Sophos NAC Advanced Upgrade and Compliance Manager Enforcement		
1.	Upgrade Sophos NAC Advanced before installing any distributed DHCP enforcement components. For more information, see the <i>Sophos NAC Advanced installation guide</i> . We recommend that you back up your databases prior to upgrading the software.	
2.	Disable DHCP enforcement. For more information, see Disable DHCP Enforcement (page 37).	
Sophos DHCP Cache Installation		
3.	Install the Sophos DHCP Cache Databases. You will use the standard domain account you created for Sophos NAC Advanced when installing the distributed DHCP enforcement components. For more information, see DHCP Cache Databases Installation (page 10). Note: If you are using SQL Server 2008, you must install the SQL Distributed Management Objects (SQL-DMO) prior to installing the DHCP Cache Databases.	
4.	Install the Sophos DHCP Cache Server. For more information, see DHCP Cache Server Installation (page 11). You can install the DHCP Cache Databases and DHCP Cache Server on a single server. However, scalability, network configuration, or network dependencies may require that you install the DHCP Cache Databases and DHCP Cache Server on separate servers, or that you install the DHCP Cache Server on more than one server. If you install the DHCP Cache Databases	

Task	Description	Completed
	and DHCP Cache Server on separate servers, they must be joined to the same domain.	
DHCP Settings on the Sophos DHCP Cache Server		
5.	Create a Connection Request Policy on the DHCP Cache Server. For more information, see Create a Connection Request Policy for DHCP (Windows Server 2003) (page 12) or Create a Connection Request Policy for DHCP (Windows Server 2008) (page 13).	
6.	Add a RADIUS Client for the DHCP server on the DHCP Cache Server. For more information, see Add a RADIUS Client for the DHCP Server (Windows Server 2003) (page 15) or Add a RADIUS Client for the DHCP Server (Windows Server 2008) (page 15).	
Multiple Sophos DHCP Cache Servers Configuration (Optional Tasks)		
7.	If you are installing the DHCP Cache Server on more than one server at each location, you must configure all additional DHCP Cache Servers to be identical to the primary DHCP Cache Server. For more information, see Configuring Multiple DHCP Cache Servers (Optional Tasks) (page 16).	
Delete DHCP Settings on the Sophos Compliance Application Server		
8.	Delete the Connection Request Policy from the Compliance Application Server. For more information, see Delete the Existing Connection Request Policy for DHCP (Windows Server 2003) (page 37) or Delete the Existing Connection Request Policy for DHCP (Windows Server 2008) (page 38).	
9.	Delete the RADIUS Client for the DHCP server from the Compliance Application Server. For more information, see Delete the Existing RADIUS Client for the DHCP Server (Windows Server 2003) (page 38) or Delete the Existing RADIUS Client for the DHCP Server (Windows Server 2008) (page 38).	
Update DHCP Enforcer Settings on the DHCP Server		
10.	Add the DHCP Cache Server details to the DHCP Enforcer Configuration Tool on the DHCP server, and delete the existing Compliance Application Server entries. For more information, see Add the DHCP Cache Server Details (page 17).	
Sophos Compliance Manager Enforcement		
11.	Enable DHCP enforcement. For more information, see Enable DHCP Enforcement (page 39).	

4.2 Disable DHCP Enforcement

To disable DHCP enforcement, you must change the Policy Mode from Enforce to Report Only in the appropriate policies. Use this feature when upgrading DHCP enforcement.

Important: All policies and policy changes are effective immediately, but a policy is not applied on the endpoint until the Agent retrieves it.

Procedure

1. Log on to the Compliance Manager.
2. Click **Manage > Policies**. Then, click the name of the policy you want to update.
3. Click the **Policy Mode** list and select **Report Only**.
 - **Report Only:** Report only policy mode specifies that endpoints are evaluated against the assigned policy and report information is generated in the Compliance Manager. No messages display, no remediation actions are performed, and no enforcement actions are taken.
4. Click **Save**.

4.3 Delete DHCP Server Connection Request Policy and RADIUS Client

For DHCP to function properly when upgrading existing DHCP enforcement to use the distributed DHCP enforcement components, you must delete the connection request policy and RADIUS client for the DHCP server that were previously created on the Compliance Application Server.

4.3.1 Delete the Existing Connection Request Policy for DHCP (Windows Server 2003)

On the Sophos Compliance Application Server, you must delete the connection request policy that you created for DHCP.

Note: For distributed DHCP enforcement, you must create the connection request policy on the DHCP Cache Server instead of the Compliance Application Server.

1. From the Start menu on the Sophos Compliance Application Server, click **Administrative Tools > Internet Authentication Service**.

IAS opens.
2. Click **Connection Request Processing**.
3. Click **Connection Request Policies**.
4. Right-click the connection request policy named **DHCP**, and select **Delete**.
5. Click **Yes**.

4.3.2 Delete the Existing Connection Request Policy for DHCP (Windows Server 2008)

On the Sophos Compliance Application Server, you must delete the connection request policy that you created for DHCP.

Note: For distributed DHCP enforcement, you must create the connection request policy on the DHCP Cache Server instead of the Compliance Application Server.

1. From the Start menu on the Sophos Compliance Application Server, click **Administrative Tools > Network Policy Server**.

Network Policy Server opens.

2. Under Policies, click **Connection Request Policies**.
3. Right-click the connection request policy named **DHCP**, and select **Delete**.
4. Click **OK**.

4.3.3 Delete the Existing RADIUS Client for the DHCP Server (Windows Server 2003)

On the Sophos Compliance Application Server, you must delete the RADIUS client that you created for the DHCP server.

Note: For distributed DHCP enforcement, you must create the RADIUS client on the DHCP Cache Server instead of the Compliance Application Server.

1. From the Start menu on the Sophos Compliance Application Server, click **Administrative Tools > Internet Authentication Service**.

IAS opens.

2. Click **RADIUS Clients**.
3. Right-click the RADIUS client named **DHCP**, and select **Delete**.
4. Click **Yes**.

4.3.4 Delete the Existing RADIUS Client for the DHCP Server (Windows Server 2008)

On the Sophos Compliance Application Server, you must delete the RADIUS client that you created for the DHCP server.

Note: For distributed DHCP enforcement, you must create the RADIUS client on the DHCP Cache Server instead of the Compliance Application Server.

1. From the Start menu on the Sophos Compliance Application Server, click **Administrative Tools > Network Policy Server**.

Network Policy Server opens.

2. Under RADIUS Clients and Servers, click **RADIUS Clients**.
3. Right-click the RADIUS client named **DHCP**, and select **Delete**.
4. Click **OK**.

4.4 Enable DHCP Enforcement

To enable DHCP enforcement, you must change the Policy Mode from Report Only to Enforce in the appropriate policies.

Important: All policies and policy changes are effective immediately, but a policy is not applied on the endpoint until the Agent retrieves it.

Procedure

1. Log on to the Compliance Manager.
2. Click **Manage > Policies**. Then, click the name of the policy you want to update.
3. Click the **Policy Mode** list and select **Enforce**.
 - **Enforce:** Enforce policy mode specifies that endpoints are evaluated against the assigned policy and report information is generated in the Compliance Manager. Messages display, remediation actions are performed, and enforcement actions are taken by using the access templates for the appropriate access state. The Enforce mode uses the access templates assigned in step 5.
4. Click the **Agent Enforcement Action** list and select **Release Renew**. You **must** select Release Renew when using DHCP enforcement.

5. In the left navigation Network Access area, click **DHCP**. Click the **Enforce** tab and verify the access template assignments.

Note: By default, each policy is automatically populated with access templates. Ensure that the correct access templates are applied. Leave the Report Only and Remediate access template assignments.

DHCP Enforcer Access Template States:

- **Policy Retrieval Error:** The endpoint's compliance state is out-of-date according to the DHCP Policy Update Threshold field configured in the **Configure System > Enforcer Settings** area.
 - **Compliant:** The endpoint is compliant with the policy.
 - **Partially Compliant:** The endpoint is partially compliant with the policy.
 - **Non-Compliant:** The endpoint is non-compliant with the policy.
6. As necessary, use the arrows to prioritize DHCP Enforcer access templates.
If more than one template applies to a particular state, the first template that meets the state is used. We recommend that you prioritize the more specific/strict access templates first and the less specific/strict access templates last.
 7. Click **Save**.

5 Software Uninstalls

To uninstall the distributed DHCP enforcement components, you must uninstall both the DHCP Cache Databases and the DHCP Cache Server, in either order, on the appropriate server. To uninstall the DHCP Enforcer software, you must uninstall the software on the DHCP server.

5.1 DHCP Cache Databases Uninstall

Uninstalling the databases removes only the files that were used to create the databases and not the actual databases. Uninstalling the databases does not delete any items you have created in the Sophos NAC Advanced Compliance Manager for DHCP enforcement. All items, such as DHCP exemptions and access templates, are stored in the Sophos NAC Advanced Compliance Databases.

1. From the Start menu, click **Control Panel > Add or Remove Programs**.
2. Select **Sophos DHCP Cache Databases** and click **Remove**.
3. Click **Yes** to confirm the removal of the server files that were used to create the databases. The server files are removed, and the databases remain intact.

5.2 DHCP Cache Server Uninstall

Uninstalling the DHCP Cache Server does not delete any items you have created in the Sophos NAC Advanced Compliance Manager for DHCP enforcement. All items, such as DHCP exemptions and access templates, are stored in the Sophos NAC Advanced Compliance Databases.

1. From the Start menu, click **Control Panel > Add or Remove Programs**.
2. Select **Sophos DHCP Cache Server** and click **Remove**.
3. Click **Yes** to confirm the removal of the DHCP Cache Server. The application is removed.

5.3 Microsoft DHCP Enforcer Software Uninstall

1. From the Start menu on the DHCP server, select **Control Panel > Add or Remove Programs**.
2. Select **Microsoft DHCP Enforcer Software**, and then click **Remove**.
3. Click **Yes** to confirm the removal of the DHCP Enforcer software.

6 Technical Support

You can find technical support for Sophos products in any of these ways:

- Visit the SophosTalk community at <http://community.sophos.com/> and search for other users who are experiencing the same problem.
- Visit the Sophos support knowledgebase at <http://www.sophos.com/support/>.
- Download the product documentation at <http://www.sophos.com/support/docs/>.
- Send an email to support@sophos.com, including your Sophos software version number(s), operating system(s) and patch level(s), and the text of any error messages.

7 Legal Notices

Copyright © 2011 Sophos Limited. All rights reserved. No part of this publication may be reproduced, stored in a 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 mentioned are trademarks or registered trademarks of their respective owners.