

Sophos NAC DHCP configuration guide

Product version: 3.9

Document date: December 2011



Contents

1 About this guide.....	3
2 DHCP enforcement overview.....	4
3 Installing DHCP enforcement.....	5
4 Upgrading DHCP enforcement.....	18
5 Appendix: Using the DHCP Enforcer Configuration Utility.....	24
6 Technical support.....	27
7 Legal notices.....	28

1 About this guide

This guide helps you configure DHCP enforcement so that you can identify unknown endpoints attaching to your network, assess their security levels, and control their network access. It describes how to configure the NAC DHCP Enforcer and the NAC Server. This document also contains information about upgrading your DHCP enforcement software.

In particular, it provides information on:

- Installing and configuring the DHCP Enforcer software for the first time.
- Configuring DHCP using the NAC Manager.
- Upgrading DHCP enforcement.

This guide is for you if:

- You are using Sophos Enterprise Console.
- You are using the version of Sophos NAC that is integrated with Enterprise Console.
- You want to install and configure DHCP enforcement, or upgrade DHCP enforcement.

See the *Sophos Enterprise Console quick startup guide* prior to reviewing this guide.

Sophos documentation is published at www.sophos.com/support/docs/.

1.1 DHCP Enforcer software requirements

To use DHCP enforcement with Sophos NAC, you must install the Sophos DHCP Enforcer software on each DHCP server.

DHCP Enforcer Software Requirements	
Operating System	<p>The following Windows Server versions are supported:</p> <ul style="list-style-type: none"> ■ Windows Server 2003 base and higher (32-bit) ■ Windows Server 2003 SP2 and higher (64-bit) ■ Windows Server 2003 R2 base and higher (32-bit and 64-bit) ■ Windows Server 2008 base and higher (32 and 64-bit) ■ Windows Server 2008 R2 base and higher (32 and 64-bit) <p>Note: Windows Server 2008 Web and Core editions are not supported.</p>
DHCP Software	Microsoft [®] Dynamic Host Configuration Protocol (DHCP) software

2 DHCP enforcement overview

Sophos NAC contains default DHCP enforcement settings. These default settings target the most common DHCP implementation so that minimal configuration is required once Sophos NAC is installed. However, DHCP implementations vary greatly; therefore, additional configuration may be necessary.

Note: The DHCP enforcement checklist provides a list of tasks required to implement DHCP enforcement. Determine the instructions that you need:

- If you are installing DHCP enforcement for the first time, see [DHCP enforcement installation checklist](#) (page 5).
- If you installed DHCP enforcement for the first time in Sophos NAC version 3.3, 3.5 or 3.7, and are upgrading to version 3.9, see [DHCP enforcement upgrade checklist](#) (page 18).

Pre-defined DHCP enforcement default settings

As needed, use the NAC Manager to change the default settings.

- Unknown endpoints are permitted network access. Unknown endpoints are not managed by Sophos Enterprise Console, do not have the Compliance Agent installed, are not exempted, and have not run the Dissolvable Agent. By default, DHCP servers are set to Report Only. To enable DHCP enforcement and quarantine unknown endpoints, you must change the Unknown Endpoint Mode to Enforce.

Note: When DHCP enforcement is enabled, unknown endpoints are denied access to private IP addresses and the local area network (LAN).

- Known endpoints are permitted network access. Known endpoints are managed by Sophos Enterprise Console and have the Compliance Agent installed and running. NAC policies are set to Report Only. To enable DHCP enforcement for known endpoints, you must change the policy mode to Enforce for each policy you intend to use.

Note: When DHCP enforcement is enabled, compliant and partially compliant endpoints that are running the Agent are permitted network access. Non-compliant endpoints that are running the Agent are denied network access.

We recommend that you use DHCP enforcement for unknown endpoints and Agent enforcement for known endpoints. However, Sophos NAC does allow you to use DHCP enforcement for known endpoints. For more information on Agent enforcement, see the *Sophos Compliance Agent configuration guide*.

3 Installing DHCP enforcement

You can install Sophos NAC DHCP enforcement for the first time by following the steps in this section.

3.1 DHCP enforcement installation checklist

The DHCP enforcement installation checklist provides a list of tasks required to implement DHCP enforcement. All tasks are completed using instructions contained in this document, unless otherwise noted.

Task	Description	Completed
Sophos NAC and Compliance Agent installation		
1.	Install and configure Sophos NAC. For more information, see the <i>Sophos Endpoint Security and Control quick startup guide</i> .	
2.	Install the Compliance Agent on endpoints using Sophos Enterprise Console. For more information, see the <i>Sophos Endpoint Security and Control quick startup guide</i> .	
DHCP server tasks		
3.	Install the DHCP Enforcer software on each DHCP server.	
Sophos NAC Manager tasks		
4.	Run the DHCP Configuration Wizard to configure proxy, remediation, Dissolvable Agent, and DHCP servers to be used with Sophos NAC DHCP enforcement.	
5.	Run the DHCP Enforcer report to: <ul style="list-style-type: none"> ■ Determine whether known endpoints will receive the appropriate network access when DHCP enforcement is enabled. ■ Locate endpoints that require exemption. 	
6.	Create exemptions for endpoints that are not able to run the Compliance Agent, such as endpoints running non-Windows operating systems. Exemptions also apply to endpoints that do not require compliance assessment, such as servers, routers, and printers.	
7.	Enable DHCP enforcement.	

3.2 Install the DHCP Enforcer software

Install the DHCP Enforcer software on each Microsoft DHCP server. The DHCP Enforcer software includes the DHCP Enforcer and the DHCP Enforcer Configuration Utility. The installation configures the DHCP server. If you need to change the DHCP server settings that were specified during the DHCP Enforcer installation, use the DHCP Enforcer Configuration Utility. For more information, see [Appendix: Using the DHCP Enforcer Configuration Utility](#) (page 24).

1. Go to <http://www.sophos.com/support/updates/>.
2. Type your MySophos username and password.
3. On the web page for **Enterprise** downloads, download the NAC DHCP Enforcer installer.
4. Run the installer.

An installation wizard guides you through installation. Accept the default options.

Keep a record of the shared key that you enter on the **Sophos DHCP Enforcer** page. The shared key is used to secure the traffic between the NAC Server and the DHCP server. The same shared key must be entered when you run the DHCP Configuration Wizard using the NAC Manager.

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

3.3 Completing NAC Manager tasks

Once you have installed the DHCP Enforcer on each DHCP server, use the NAC Manager to configure your DHCP servers to work with Sophos NAC. DHCP enforcement requires minimal configuration using the NAC Manager. DHCP enforcement defaults to report only. You must enable enforcement.

- **Unknown endpoints** are not managed by Sophos Enterprise Console, do not have the Compliance Agent installed, are not exempted, and have not run the Dissolvable Agent.
- **Known endpoints** are managed by Sophos Enterprise Console and have the Compliance Agent installed and running.

Note: You must create exemptions for endpoints that are not able to run the Compliance Agent, such as endpoints running non-Windows operating systems. Exemptions also apply to endpoints that do not require compliance assessment, such as servers, routers, and printers. Endpoints that receive a dynamically assigned IP address through DHCP are the only endpoints that need to be exempted.

NAC Manager tasks include the following:

1. Run the DHCP Configuration Wizard to configure proxy, remediation, Dissolvable Agent, and DHCP servers to be used with Sophos NAC DHCP enforcement .

2. Run the NAC Manager DHCP Enforcer report to determine whether known endpoints will receive the appropriate network access when DHCP enforcement is enabled. Also, locate endpoints that require exemption.
3. Create exemptions for endpoints that are not able to run the Compliance Agent or do not require compliance assessment.
4. Enable DHCP enforcement.

3.3.1 Run the DHCP Configuration Wizard

The DHCP Configuration Wizard helps you identify proxy, remediation, Dissolvable Agent, and DHCP servers to be used with Sophos NAC DHCP implementations, and automatically configures the default DHCP Enforcer access templates with your server definitions.

Procedure

1. Log on to the NAC Manager.
2. Click **Enforce > DHCP Configuration Wizard**. Click **Next** to continue.
3. Do one of the following:
 - If you use proxy servers, click **Yes**, and then click **Next**. Go to the next step.
 - If you do **not** use proxy servers, click **No**, and then click **Next**. Go to step 5.

Important: If you do not define a proxy server for internet access, users will not have internet access and the default DHCP - Internet Access DHCP Enforcer access template will provide remediation access only.
4. Define the proxy servers needed to allow internet access, and then click **Next**.
Do either of the following:
 - Clear the check boxes beside those servers you do **not** want included as a proxy server.
 - Click **Add** to add new servers, enter the proxy server information, and click **OK**. Repeat this step as necessary to add additional servers. Once created, these servers can be managed on the **Enforce > Network Resources** page.

Note: The selected proxy servers will replace the servers currently in the default DHCP - Internet Access DHCP Enforcer access template.
5. Define the remediation servers needed to allow remediation access, such as domain controllers, and then click **Next**.
Do either of the following:
 - Clear the check boxes beside those servers you do **not** want included as a remediation server.
 - Click **Add** to add new servers, enter the remediation server information, and click **OK**. Repeat this step as necessary to add additional servers. Once created, these servers can be managed on the **Enforce > Network Resources** page.

Note: The selected remediation servers will replace the servers currently in the default DHCP - Remediation Access DHCP Enforcer access template.

6. Do one of the following:

- If you have installed the Dissolvable Agent, click **Yes**, and then click **Next**. Go to the next step.
- If you have **not** installed the Dissolvable Agent, click **No**, and then click **Next**. Go to step 8.

Note: If you have installed the Dissolvable Agent on the same server as Sophos NAC, you do not need to create an additional Dissolvable Agent server.

7. Define the servers hosting the Dissolvable Agent so that the DHCP Enforcer can allow access to them. This access is required so that unknown endpoints, such as guests, can become known to the network. Click **Add** to add new servers, enter the Dissolvable Agent server information, and click **OK**. Then, click **Next**. Once created, these servers can be managed on the **Configure System > Server Settings** page.

8. Define the DHCP servers that the DHCP Enforcer software is installed on. Click **Add** to add new servers, enter the DHCP Enforcer server information, and click **OK**. Repeat this step as necessary to add additional servers. Then click **Next**. Once created, these servers can be managed on the **Configure System > Server Settings** page.

Note: The shared key must match what you entered during the DHCP Enforcer installation on the server. The shared key is used to secure the traffic between the NAC Server and the DHCP server.

9. Click **Finish**.

3.3.2 Run the DHCP Enforcer report

Run the Sophos NAC DHCP Enforcer report to determine the compliance state of endpoints prior to enabling DHCP enforcement. The pre-defined NAC policies are set to Report Only. The DHCP Enforcer report can be used to determine whether the correct access template will be applied when enforcement is enabled. You can exempt devices and access the assessment details from the DHCP Enforcer report.

Procedure

1. Log on to the NAC Manager.
2. Click **Report > Troubleshooting**.
3. Click the **Report Type** list and select **DHCP Enforcer**.
4. 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.

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.

5. 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 NAC 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.
Compliance State	Endpoint compliance state, assigned during the compliance assessment. Available compliance states are Compliant, Partially Compliant, and Non-Compliant. A triple dash (---) indicates that the Agent did not report a compliance state. The DHCP Enforcer access templates associated with the policy compliance state determine network access.
Template Name (Version)	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 any access templates you have created: <ul style="list-style-type: none"> ■ DHCP - Full Access: Allows full network access. ■ DHCP - Internet Access: Allows access to the internet, and denies access to private IP addresses and the local area network (LAN). Important: If you do not define a proxy server for internet access as a network resource, users will not have internet access and this template will provide remediation access only. ■ DHCP - Remediation Access: Denies all network access except to defined remediation servers, the NAC Server, and the Dissolvable Agent server.
Reason	Reason that a particular access template was assigned by the DHCP Enforcer. Available reasons are: <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. A link displays that accesses details about the compliance assessment associated with this DHCP Enforcer entry.

Field	Description
	<ul style="list-style-type: none"> ■ 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 DHCP Enforcer check box is selected in the Configure System > Enforcer Settings area, the Maintenance Mode/Enforcer Override access templates also designated in that area determine network access. ■ 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 NAC 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.

Field	Description
	<ul style="list-style-type: none"> ■ Unknown Endpoint: No compliance record exists. The Unknown Endpoint access templates designated in the Configure System > Enforcer Settings area determine network access.
Returned User Class	DHCP user class returned to the DHCP server by the DHCP Enforcer for enforcement.
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.
Detailed report entry	
Agent Enforcement Action	<p>Action taken by the endpoint regarding IP address assignment. 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 starts 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:</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.

3.3.3 Creating DHCP exemptions

Exempted endpoints are not able to run the Compliance Agent, such as endpoints running non-Windows operating systems. Exemptions also apply to endpoints that do not require compliance assessment, such as servers, routers, and printers. 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 NAC 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.

3.3.3.1 Create DHCP criteria exemptions

Use the NAC Manager Exemptions page to create exemptions by DHCP criteria. The exemption criteria and DHCP Enforcer access templates are used in conjunction with each other to identify exemptions and designate actions. Once the defined exemption criteria is matched, the associated DHCP Enforcer access templates determine the appropriate network access action to take.

Procedure

1. Log on to the NAC 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 and select **DHCP Criteria**.
5. Under Exemption Criteria, select the **MAC Address**, **User Class**, or **Vendor Class** option 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. If you specify a MAC address without the * symbol, then you must specify the exact MAC address you want to exempt.

6. Click **Select** to add DHCP Enforcer access templates to the exemption, select the **DHCP - Full Access** access template, and click **OK**.

The **DHCP - Full Access** access template is pre-defined in Sophos NAC to permit network access. You have configured this exemption to access the network without a compliance assessment by Sophos NAC.

7. Click **Save**.

3.3.3.2 Create IP scope exemptions

Endpoints that receive a dynamically assigned IP address through DHCP are the only endpoints that need to be exempted. Use the NAC 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 NAC 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 and select **IP Scope**.
5. Under Exempted IP Scopes, click **Select** to add IP scopes to the exemption, select the appropriate scopes, and click **OK**.

If you do not see the IP scope you need, you can create one. This requires you to create a new DHCP Enforcer access template or update one of the pre-defined DHCP Enforcer access templates.

6. As necessary, use the arrows to prioritize the scopes.

If more than one IP scope applies to a particular exemption, the first IP scope met is used. We recommend that you prioritize the more specific/strict IP scopes first and the less specific/strict IP scopes last.

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.

3.3.4 Enabling DHCP enforcement

You can enable DHCP enforcement for both unknown and known endpoints. We recommend that you use DHCP enforcement for unknown endpoints and Agent enforcement for known endpoints. However, Sophos NAC does allow you to use DHCP enforcement for known endpoints.

3.3.4.1 Enable DHCP enforcement for unknown endpoints

You can enable DHCP enforcement for unknown endpoints on each DHCP server. This allows you to specify which DHCP servers will quarantine unknown endpoints. Use this feature to perform a phased rollout of DHCP enforcement.

Prior to enabling DHCP enforcement for unknown endpoints, you must create exemptions. Endpoints that receive a dynamically assigned IP address through DHCP are the only endpoints that need to be exempted.

Procedure

1. Log on to the NAC Manager.
2. Click **Configure System > Server Settings**.
3. Click the name of the DHCP server for which you want to enable DHCP enforcement.

4. Click the **Unknown Endpoint Mode** list and select **Enforce**. The Enforce mode uses the DHCP - Internet Access access template to quarantine unknown endpoints and permit access to the internet or to remediation servers.

Note: If you specified a proxy server when you ran the DHCP Configuration Wizard, endpoints can access the internet. If you did not specify a proxy server, endpoints can instead access the remediation servers that you specified in the DHCP Configuration Wizard. You can change the access template in the **Configure System > Enforcer Settings** area.

5. Click **Save**.

3.3.4.2 Enable DHCP enforcement for known endpoints

You can enable DHCP enforcement for known endpoints in policies. If you plan to use DHCP enforcement or Agent enforcement for known endpoints, 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 NAC 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 NAC 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 for known endpoints.

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.

Pre-defined DHCP Enforcer Template Assignments

- **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 DHCP - Remediation Access access template denies network access except to the remediation servers you specified when you ran the DHCP Configuration Wizard.
 - **Compliant:** The endpoint is compliant. The DHCP - Full Access access template permits network access when the endpoint is compliant.
 - **Partially Compliant:** The endpoint is partially compliant. The DHCP - Full Access access template permits network access when the endpoint is partially compliant.
 - **Non-Compliant:** The endpoint is non-compliant. The DHCP - Remediation Access access template denies network access except to the remediation servers you specified when you ran the DHCP Configuration Wizard.
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**.

3.3.4.2.1 Use the pre-defined policies

You can use the pre-defined policies to enforce security compliance for both managed and unmanaged endpoints.

- **Default:** This policy is used if an endpoint has the Compliance Agent installed and no other policy has been assigned. By default, the policy mode is set to Report Only. This policy performs remediation actions on the endpoint if the policy mode is set to Remediate or Enforce.
- **Managed:** This policy can be used for endpoints that are managed with Sophos Enterprise Console and have a Compliance Agent installed. By default, the policy mode is set to Report Only. This policy performs remediation actions on the endpoint if the policy mode is set to Remediate or Enforce.
- **Unmanaged:** This policy can be used for endpoints from outside of the company. This policy does not perform remediation actions on the endpoint. The Dissolvable Agent uses the Unmanaged policy.

Note: If an endpoint does not have a Compliance Agent installed and is not using the Dissolvable Agent, then Enforcer settings determine network access.

3.3.4.3 DHCP enforcement user experience

Once you have enabled DHCP enforcement, the DHCP enforcement user experience depends on whether an endpoint is unknown or known. Additionally, guests can run the Compliance Dissolvable Agent to gain network access.

- **Unknown endpoints** are not managed by Sophos Enterprise Console, do not have the Compliance Agent installed, are not exempted, and have not run the Dissolvable Agent.
- **Guest endpoints** can use the Compliance Dissolvable Agent for network access control.
- **Known endpoints** are managed by Sophos Enterprise Console and have the Compliance Agent installed and running.

DHCP enforcement user experience for unknown endpoints

When DHCP enforcement is enabled, unknown endpoints will have the following experience:

1. Endpoint starts up.
2. When DHCP enforcement for unknown endpoints is enabled, endpoints receive limited network access. These endpoints can access the internet or remediation servers. If you specified a proxy server when you ran the DHCP Configuration Wizard, endpoints can access the internet. If you did not specify a proxy server, endpoints can instead access the remediation servers that you specified in the DHCP Configuration Wizard.

DHCP enforcement user experience for guest endpoints

When DHCP enforcement is enabled and guest endpoints are required to use the Compliance Dissolvable Agent, guest users will have the following experience:

1. Endpoint starts up.
2. User opens Internet Explorer, navigates to the Compliance Dissolvable Agent URL, and runs the Compliance Dissolvable Agent.
3. The Compliance Dissolvable Agent completes an assessment and determines whether the endpoint is compliant, partially compliant, or non-compliant with NAC policy.
4. When DHCP enforcement is configured and enabled, the following occurs:
 - Compliant endpoints are permitted network access.
 - Partially-compliant endpoints are permitted network access. The Compliance Dissolvable Agent displays messages to users so that they can remediate their endpoints to become compliant. If the NAC policy is configured to remediate the endpoint automatically, endpoint remediation takes place. By default, remediation is disabled. We recommend that you do not remediate a guest user's endpoint.
 - Non-compliant endpoints are denied network access. These endpoints can access the internet or remediation servers. If you specified a proxy server when you ran the DHCP Configuration Wizard, endpoints can access the internet. If you did not specify a proxy server, endpoints can instead access the remediation servers that you specified in the DHCP Configuration Wizard. The Compliance Dissolvable Agent displays messages to users so that they can remediate their endpoints to become compliant. If the NAC policy is configured to remediate

the endpoint automatically, endpoint remediation takes place. By default, remediation is disabled. We recommend that you do not remediate a guest user's endpoint.


DHCP enforcement experience for known endpoints

When DHCP enforcement is enabled, known endpoints will have the following DHCP experience:

1. Endpoint starts and Compliance Agent runs.
2. Compliance Agent completes an assessment and determines whether the endpoint is compliant, partially compliant, or not compliant with NAC policy.
3. When DHCP enforcement is configured and enabled, the following occurs:
 - Compliant endpoints are permitted network access.
 - Partially compliant endpoints are permitted network access. The Compliance Agent displays messages to users so that they can remediate their endpoints to become compliant. If the NAC policy is configured to remediate the endpoint automatically, remediation takes place.
 - Non-compliant endpoints are denied network access. These endpoints can access remediation servers that you specified when you ran the DHCP Configuration Wizard. The Compliance Agent displays messages to users so that they can remediate their endpoints to become compliant. If the NAC policy is configured to remediate the endpoint automatically, endpoint remediation takes place.

4 Upgrading DHCP enforcement

To use DHCP enforcement in Sophos NAC version 3.9, you must upgrade your DHCP enforcement software. To upgrade, you must uninstall your existing DHCP enforcement software and then install the new software. You must also disable DHCP enforcement prior to uninstalling the software and enable DHCP enforcement after installing the new software.

 **Caution:** To upgrade, you must turn DHCP enforcement off. We recommend that you upgrade DHCP enforcement at a time that poses the least risk to your network.

4.1 DHCP enforcement upgrade checklist

The DHCP enforcement upgrade checklist provides a list of tasks required to upgrade DHCP enforcement to Sophos NAC version 3.9. All tasks are completed using instructions contained in this document, unless otherwise noted.

Task	Description	Completed
Sophos NAC upgrade		
1.	Upgrade Sophos NAC. For more information, go to the Endpoint Security and Control Upgrade Center at http://www.sophos.com/support/upgrades/ .	
Sophos NAC Manager tasks, part 1		
2.	Disable DHCP enforcement.	
DHCP server tasks		
3.	Uninstall the existing DHCP Enforcer software on each DHCP server.	
4.	<p>Install the new DHCP Enforcer software on each DHCP server.</p> <p>Important: When you install the DHCP Enforcer software on a DHCP server, you must re-enter a shared key. If possible, you should use the shared key from the previous version, because it will match the shared key in the NAC Manager for the same DHCP server. If you do not know the shared key that was used in the previous version, you can create a new one during the software installation. However, you must then update the shared key in the NAC Manager for that DHCP server so that the keys match.</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>	
Sophos NAC Manager tasks, part 2		
5.	Update the shared key for each DHCP server. (Optional Task)	

Task	Description	Completed
6.	Enable DHCP enforcement.	

4.2 Disabling DHCP enforcement

You must disable DHCP enforcement for both unknown and known endpoints when upgrading DHCP enforcement. We recommend that you use DHCP enforcement for unknown endpoints and Agent enforcement for known endpoints. However, Sophos NAC does allow you to use DHCP enforcement for known endpoints.

4.2.1 Disable DHCP enforcement for unknown endpoints

To disable DHCP enforcement for unknown endpoints, you must change the Unknown Endpoint Mode on each DHCP server from Enforce to Report Only.

Procedure

1. Click **Configure System > Server Settings**.
2. Click the name of the DHCP server for which you want to disable DHCP enforcement.
3. Click the **Unknown Endpoint Mode** list and select **Report Only**. The Report Only mode uses the DHCP - Full Access access template to permit network access to unknown endpoints.
4. Click **Save**.

4.2.2 Disable DHCP enforcement for known endpoints

To disable DHCP enforcement, you must change the Policy Mode from Enforce to Report Only 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.

Note: If you are using Agent enforcement instead of DHCP enforcement for known endpoints, this task is not required.

Procedure

1. Log on to the NAC 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 NAC Manager. No messages display, no remediation actions are performed, and no enforcement actions are taken. The Report Only mode uses the DHCP - Full Access access template to permit network access to known endpoints.

4. Click **Save**.

4.3 Uninstall the DHCP Enforcer software

Uninstall the DHCP Enforcer software on each Microsoft DHCP server. The DHCP Enforcer software includes the DHCP Enforcer and the DHCP Enforcer Configuration Utility.

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

4.4 Install the DHCP Enforcer software

Install the DHCP Enforcer software on each Microsoft DHCP server. The DHCP Enforcer software includes the DHCP Enforcer and the DHCP Enforcer Configuration Utility. The installation configures the DHCP server. If you need to change the DHCP server settings that were specified during the DHCP Enforcer installation, use the DHCP Enforcer Configuration Utility. For more information, see [Appendix: Using the DHCP Enforcer Configuration Utility](#) (page 24).

1. Go to <http://www.sophos.com/support/updates/>.
2. Type your MySophos username and password.
3. On the web page for **Enterprise** downloads, download the NAC DHCP Enforcer installer.
4. Run the installer.

An installation wizard guides you through installation. Accept the default options.

Keep a record of the shared key that you enter on the **Sophos DHCP Enforcer** page. The shared key is used to secure the traffic between the NAC Server and the DHCP server. The same shared key must be entered when you run the DHCP Configuration Wizard using the NAC Manager.

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

4.5 Update the DHCP server shared key

The shared key is used to secure the traffic between the NAC Server and the DHCP server.

When you install the DHCP Enforcer software on a DHCP server, you must re-enter a shared key. If possible, you should use the shared key from the previous version, because it will match the shared key in the NAC Manager for the same DHCP server. If you do not know the shared key that was used in the previous version, you can create a new one during the software installation. However, you must then update the shared key in the NAC Manager for that DHCP server so that the keys match.

Note: If you used the shared key from the previous version during the DHCP Enforcer software installation, this task is not required.

Procedure

1. Click **Configure System > Server Settings**.
2. Click the name of the DHCP server for which you need to update the shared key.
3. Type and confirm the server's shared key.

Important: The shared key must match what you entered during the DHCP Enforcer software installation on the DHCP server.

4. Click **Save**.

4.6 Enabling DHCP enforcement

You can enable DHCP enforcement for both unknown and known endpoints. We recommend that you use DHCP enforcement for unknown endpoints and Agent enforcement for known endpoints. However, Sophos NAC does allow you to use DHCP enforcement for known endpoints.

4.6.1 Enable DHCP enforcement for unknown endpoints

You can enable DHCP enforcement for unknown endpoints on each DHCP server. This allows you to specify which DHCP servers will quarantine unknown endpoints. Use this feature to perform a phased rollout of DHCP enforcement.

Prior to enabling DHCP enforcement for unknown endpoints, you must create exemptions. Endpoints that receive a dynamically assigned IP address through DHCP are the only endpoints that need to be exempted.

Procedure

1. Log on to the NAC Manager.
2. Click **Configure System > Server Settings**.
3. Click the name of the DHCP server for which you want to enable DHCP enforcement.
4. Click the **Unknown Endpoint Mode** list and select **Enforce**. The Enforce mode uses the DHCP - Internet Access access template to quarantine unknown endpoints and permit access to the internet or to remediation servers.

Note: If you specified a proxy server when you ran the DHCP Configuration Wizard, endpoints can access the internet. If you did not specify a proxy server, endpoints can instead access the remediation servers that you specified in the DHCP Configuration Wizard. You can change the access template in the **Configure System > Enforcer Settings** area.

5. Click **Save**.

4.6.2 Enable DHCP enforcement for known endpoints

You can enable DHCP enforcement for known endpoints in policies. If you plan to use DHCP enforcement or Agent enforcement for known endpoints, 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 NAC 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 NAC 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 for known endpoints.
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.

Pre-defined DHCP Enforcer Template Assignments

- **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 DHCP - Remediation Access access template denies network access except to the remediation servers you specified when you ran the DHCP Configuration Wizard.
- **Compliant:** The endpoint is compliant. The DHCP - Full Access access template permits network access when the endpoint is compliant.
- **Partially Compliant:** The endpoint is partially compliant. The DHCP - Full Access access template permits network access when the endpoint is partially compliant.
- **Non-Compliant:** The endpoint is non-compliant. The DHCP - Remediation Access access template denies network access except to the remediation servers you specified when you ran the DHCP Configuration Wizard.

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 Appendix: Using the DHCP Enforcer Configuration Utility

If you need to change the DHCP Enforcer settings that were specified during the DHCP Enforcer installation, use the DHCP Enforcer Configuration Utility. The DHCP Enforcer installation installs this utility on the DHCP server. If you have more than one DHCP server, you must change the DHCP Enforcer settings on each DHCP server.

5.1 Update the shared key

Procedure

The shared key must match what you entered during the DHCP Enforcer installation on the server. The shared key is used to secure the traffic between the NAC Server and the DHCP server.

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

The **DHCP Enforcer Configuration Utility** dialog box displays with the **Enforcer** tab selected.

2. In the **DHCP Enforcer Configuration Utility** dialog box, click the **Edit** button.
3. In the **DHCP Enforcer RADIUS Enforcer Server Settings** dialog box, enter and confirm the new shared key, and click **OK**.

5.2 Update the advanced settings

This section describes how to update the advanced DHCP Enforcer settings using the DHCP Enforcer Configuration Utility. In most cases, these settings should not have to be updated.

Procedure

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

The **DHCP Enforcer Configuration Utility** dialog box displays with the **Enforcer** tab selected.

2. On the **DHCP Enforcer Configuration Utility** dialog box, click the **Advanced** tab.
3. As needed, change the DHCP Enforcer settings.
4. Click **OK**.

Repeat these instructions on all applicable DHCP servers.

5.2.1 DHCP Enforcer Configuration Utility fields and descriptions

Fields	Descriptions
Enforcer tab	
Access for Multiple Servers	This option button is not applicable to Sophos Endpoint Security and Control.
DHCP Enforcer RADIUS Enforcer Server Settings dialog box	
Click the Edit button to access this dialog box.	
Note: The fields on this dialog box are in relation to the NAC Server.	
Enable	Displays whether the NAC Server is enabled. When it is enabled, the NAC Server is used for policy compliance and reporting activity.
IP Address	Designates the IP address of the NAC Server.
Authentication Port	Designates the authentication port of the NAC Server.
Accounting Port	Designates the accounting port of the NAC Server.
Shared Key	Identifies the shared key of the DHCP server. The shared key is the same shared key that was used in the DHCP Enforcer installation.
Confirm Shared Key	Confirms the DHCP server shared key.
DHCP Enforcer Resolve IP dialog box	
Hostname	Identifies the hostname, when the IP address is not known, of the NAC Server. When you enter the hostname, you can resolve the hostname to the IP address.
Advanced 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 assessment.
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.

Fields	Descriptions
Error	When selected, enables Microsoft error messages to be saved to the Application Event Log.
Warning	When selected, enables Microsoft warning messages to be saved to the Application Event Log.
Information	When selected, enables Microsoft information messages to be saved to the Application Event Log.
Trace	When selected, enables Microsoft trace logging to be saved to the Application Event Log.
Subnet Mask Override	Specifies the subnet mask available to users who are not compliant with policy and overrides the subnet on the DHCP server to limit network access.
Black Hole IP Address	This dummy IP address is used by the DHCP Enforcer to silently discard/drop blocked resource traffic.
DHCP Enforcer Informs IP Address dialog box	
IP Address	Designates the IP address associated with the client, such as a remote access concentrator (RAC), for which you want to bypass policy compliance and reporting for DHCP inform packets. By default, policy compliance and reporting are performed for DHCP inform packets. When an IP address is specified, policy compliance and reporting are not performed for DHCP inform packets from that client.
DHCP Enforcer Resolve IP dialog box	
Hostname	Identifies the hostname, when the IP address is not known, of the client for which you want to bypass policy compliance and reporting. When you enter the hostname, you can resolve the hostname to the IP address.

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 license 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.