

# SOPHOS

## Sophos NAC DHCP Guida alla configurazione

Versione prodotto: 3.5

Data documento: giugno 2010



# Sommario

1	Informazioni sulla guida.....	3
2	Panoramica sull'attuazione DHCP.....	4
3	Checklist per l'attuazione DHCP.....	5
4	Installazione del software DHCP Enforcer.....	6
5	Completamento delle operazioni di NAC Manager .....	7
6	Appendice A: Upgrade dell'attuazione DHCP senza riconfigurazione.....	18
7	Appendice B: Upgrade dell'attuazione DHCP con riconfigurazione.....	26
8	Appendice C: Utilizzo dell'utilità di configurazione di DHCP Enforcer.....	40
9	Supporto tecnico.....	43
10	Note legali.....	44

# 1 Informazioni sulla guida

Questa guida fornisce supporto per configurare l'attuazione DHCP, inclusa in Sophos Endpoint Security and Control, in modo tale da identificare i computer sconosciuti che si connettono alla rete, verificarne livello di sicurezza e controllarne l'accesso alla rete. Descrive come configurare NAC DHCP Enforcer e il Server NAC. Questo documento contiene inoltre informazioni su come effettuare l'upgrade del software dell'attuazione DHCP.

Nello specifico, fornisce informazioni relative a:

- Installazione e configurazione iniziali del software DHCP Enforcer .
- Configurazione di DHCP tramite NAC Manager.
- Upgrade dell'attuazione DHCP

Questa guida sarà utile se:

- Si sta utilizzando Enterprise Console:
- Si sta utilizzando Sophos NAC per Endpoint Security and Control.
- Si desidera installare e configurare l'attuazione DHCP, oppure effettuarne l'upgrade.

Prima di consultare questa guida, leggere la *Guida di avvio rapido di Sophos Endpoint Security and Control*.

Tutti i documenti relativi a Sophos Endpoint Security and Control sono disponibili alla pagina: [http://www.sophos.it/support/docs/Endpoint\\_Security\\_Control-all.html](http://www.sophos.it/support/docs/Endpoint_Security_Control-all.html).

## 1.1 Requisiti del software DHCP Enforcer

Per utilizzare l'attuazione DHCP con Sophos NAC, è necessario installare il software Sophos DHCP Enforcer in tutti i server DHCP.

Requisiti del software DHCP Enforcer	
Sistema operativo	<p>Le seguenti edizioni di Windows Server sono supportate:</p> <ul style="list-style-type: none"> <li>■ Windows Server 2003 versione base e superiore (32-bit)</li> <li>■ Windows Server 2003 SP2 e superiore (64-bit)</li> <li>■ Windows Server 2003 R2 versione base e superiore (32-bit e 64-bit)</li> <li>■ Windows Server 2008 versione base e superiore (32 e 64-bit)</li> <li>■ Windows Server 2008 R2 versione base e superiore (32 e 64-bit)</li> </ul> <p><b>Nota:</b> Windows Server 2008 Web e Core non sono supportate.</p>
Software DHCP	Software Microsoft <sup>®</sup> Dynamic Host Configuration Protocol (DHCP)

## 2 Panoramica sull'attuazione DHCP

Sophos NAC comprende impostazioni predefinite per l'attuazione DHCP. Tali impostazioni si riferiscono alle più comuni implementazioni DHCP in modo tale che, dopo l'installazione di Sophos NAC, la configurazione necessaria sia ridotta al minimo. Tuttavia, le implementazioni DHCP possono variare molto le une dalle altre e, di conseguenza, può essere necessaria una configurazione aggiuntiva.

**Nota:** La checklist per l'attuazione DHCP fornisce un elenco di operazioni necessarie ad implementare l'attuazione DHCP. Determinare il tipo di istruzioni di cui si ha bisogno per l'installazione o per l'upgrade:

- Se si sta installando l'attuazione DHCP per la prima volta, consultare la sezione [Checklist per l'attuazione DHCP](#) a pagina 5.
- Se l'attuazione DHCP è stata installata per la prima volta in NAC versione 3.3 e si sta effettuando l'upgrade alla versione 3.5, consultare la sezione [Checklist per l'upgrade dell'attuazione DHCP senza riconfigurazione](#) a pagina 18.
- Se si sta eseguendo l'upgrade da NAC versione 3.1.2 alla versione 3.5, consultare la sezione [Checklist per l'upgrade dell'attuazione DHCP con riconfigurazione](#) a pagina 26.

### Impostazioni predefinite per l'attuazione DHCP

Se necessario, utilizzare NAC Manager per modificare le impostazioni predefinite.

- Viene consentito l'accesso alla rete da parte di computer sconosciuti. Tali computer non dispongono dell'agente installato e non sono esenti. Per impostazione predefinita, nei server DHCP viene eseguita la modalità Report Only. Per abilitare l'attuazione DHCP e la quarantena di computer sconosciuti, è necessario cliccare su Unknown Endpoint Mode e selezionare Enforce.

**Nota:** Quando è abilitata l'attuazione DHCP, ai computer sconosciuti viene negato l'accesso ad indirizzi IP privati ed alla rete di area locale (LAN).

- Ai computer noti, ovvero i computer su cui è in esecuzione l'agente, viene consentito l'accesso alla rete. I criteri di NAC sono impostati su Report Only. Per abilitare l'attuazione DHCP nei computer noti, è necessario cambiare la modalità del criterio e selezionare Enforce; questa operazione deve essere svolta per tutti i criteri che si intende utilizzare.

**Nota:** quando l'attuazione di DHCP è abilitata, viene concesso accesso alla rete a tutti i computer conformi o parzialmente conformi che eseguono l'agente. I computer non conformi che eseguono l'agente non possono accedere alla rete.

Sophos consiglia di utilizzare l'attuazione DHCP per i computer sconosciuti e quella dell'agente per i computer noti. Sophos NAC consente comunque l'utilizzo dell'attuazione DHCP anche per i computer noti. Per ulteriori informazioni sull'attuazione dell'agente, consultare la *Guida alla configurazione di Sophos Compliance Agent*.

### 3 Checklist per l'attuazione DHCP

La checklist per l'attuazione DHCP fornisce l'elenco di operazioni necessarie per eseguire l'implementazione dell'attuazione DHCP. È possibile completare tutte le operazioni seguendo le istruzioni contenute in questo documento, se non diversamente indicato.

Operazione	Descrizione	Completata
<b>Installazione di Sophos NAC e Compliance Agent</b>		
1.	Installare e configurare Sophos NAC. Per ulteriori informazioni, consultare la <i>Guida di avvio rapido di Endpoint Security and Control</i> .	
2.	Installare il Compliance Agent nei computer tramite Sophos Enterprise Console. Per ulteriori informazioni, consultare la <i>Guida di avvio rapido di Sophos Endpoint Security and Control</i> .	
<b>Operazioni del server DHCP</b>		
3.	Installare il software DHCP Enforcer in tutti i server DHCP.	
<b>Operazioni di Sophos NAC Manager</b>		
4.	Utilizzare la procedura guidata di configurazione di DHCP per eseguire la configurazione di proxy, delle azioni correttive, del Dissolvable Agent e dei server DHCP che si desidera utilizzare con l'attuazione Sophos NAC DHCP.	
5.	Eseguire il report DHCP Enforcer per: <ul style="list-style-type: none"> <li>■ Determinare se, una volta abilitata l'attuazione DHCP, ai computer noti verrà concesso l'accesso alla rete appropriato.</li> <li>■ Localizzare i computer che richiedono esenzioni.</li> </ul>	
6.	Creare esenzioni per i computer che non possono eseguire il Compliance Agent, quali computer con sistemi operativi non Windows. Le esenzioni vengono inoltre applicate ai computer che non richiedono la verifica della conformità, quali server, router e stampanti.	
7.	Abilitare l'attuazione DHCP.	

## 4 Installazione del software DHCP Enforcer

Installare il software DHCP Enforcer in tutti i server Microsoft DHCP. Il software DHCP Enforcer include DHCP Enforcer e l'utilità di configurazione di DHCP Enforcer. Durante l'installazione viene configurato il server DHCP. Se si desidera modificare le impostazioni del server DHCP specificate durante l'installazione di DHCP Enforcer, utilizzare l'utilità di configurazione di DHCP Enforcer. Per ulteriori informazioni, consultare la sezione [Appendice C: Utilizzo dell'utilità di configurazione di DHCP Enforcer](#) a pagina 40.

1. Andare al sito web di Sophos, scaricare il programma di installazione di Sophos NAC per DHCP Enforcer ed eseguirlo.  
In alternativa, inserire il CD Sophos per l'installazione di DHCP Enforcer. Il CD si avvia automaticamente.
2. Viene avviata la procedura guidata di installazione. Nella finestra di dialogo **Benvenuti nella procedura guidata per la protezione dei computer**, cliccare su **Avanti**.
3. Nella finestra di dialogo **Sophos DHCP Enforcer**, inserire l'indirizzo IP del Server NAC, la chiave condivisa del Server NAC e la conferma della chiave condivisa. Cliccare su **Avanti**. Memorizzare la chiave condivisa inserita. La chiave condivisa viene utilizzata per proteggere il traffico tra Server NAC e il server DHCP. Quando si esegue la procedura guidata di configurazione di DHCP tramite NAC Manager, si deve utilizzare la medesima chiave condivisa. Una volta identificato un server DHCP in NAC Manager, è possibile aggiornarne la chiave condivisa nell'area **Configure System > Server Settings**.
4. Nella finestra di dialogo **Pronta per l'installazione del programma**, cliccare su **Installa** per installare DHCP Enforcer.
5. Cliccare su **Fine**.

**Nota:** dopo aver installato il software DHCP Enforcer, è necessario verificare che DHCP Enforcer sia in esecuzione su ciascun server DHCP.

## 5 Completamento delle operazioni di NAC Manager

Una volta terminata l'installazione di DHCP Enforcer in tutti i server DHCP, utilizzare NAC Manager per configurare tali server in modo che possano operare congiuntamente a Sophos NAC. L'attuazione DHCP, eseguita tramite NAC Manager, richiede una configurazione minima. Per impostazione predefinita, l'attuazione DHCP è in modalità Report Only. È necessario abilitare l'attuazione.

- **Computer sconosciuti** non sono gestiti da Sophos Enterprise Console, non dispongono del Compliance Agent installato, non sono esenti e non hanno eseguito il Dissolvable Agent.
- **Computer noti** sono gestiti da Sophos Enterprise Console e hanno il Compliance Agent installato e operativo.

**Nota:** è necessario creare esenzioni per i computer che non possono eseguire il Compliance Agent, quali ad esempio computer con sistemi operativi non Windows. Le esenzioni vengono inoltre applicate ai computer che non richiedono la verifica della conformità, quali server, router e stampanti. I computer a cui è assegnato un indirizzo IP in modo dinamico tramite DHCP sono i soli computer a poter essere esentati.

Le operazioni di NAC Manager comprendono:

1. L'utilizzo della procedura guidata di configurazione di DHCP per eseguire la configurazione di proxy, delle azioni correttive, del Dissolvable Agent e dei server DHCP che si desidera utilizzare con l'attuazione DHCP di Sophos NAC.
2. L'utilizzo del report DHCP Enforcer di NAC Manager per stabilire se i computer riceveranno l'accesso alla rete adeguato una volta abilitata l'attuazione DHCP, e l'identificazione dei computer che richiedono esenzioni.
3. La creazione di esenzioni per i computer che non possono eseguire il Compliance Agent o che non richiedono la verifica della conformità.
4. L'abilitazione dell'attuazione DHCP.

### 5.1 Esecuzione della procedura guidata di configurazione di DHCP

La Procedura guidata di configurazione di DHCP aiuta ad identificare i server proxy, di correzione, del Dissolvable Agent e DHCP da utilizzare con le implementazioni di Sophos NAC e per configurare automaticamente i modelli di accesso predefiniti di DHCP in base alle definizioni del proprio server.

#### Procedura

1. Accedere a NAC Manager.
2. Cliccare su **Enforce > DHCP Configuration Wizard** . Cliccare su **Avanti** per continuare.
3. Effettuare una delle seguenti operazioni:
  - Se si utilizzano server proxy, cliccare su **Yes** e poi su **Next**. Passare al punto seguente.
  - Se **non** si eseguono server proxy, cliccare su **No** e poi su **Next**. Passare al punto 5.

**Importante:** Se non viene definito un server proxy per l'accesso a internet, gli utenti non avranno accesso a internet, e il modello di accesso predefinito DHCP - Internet Access DHCP Enforcer fornirà esclusivamente accesso per azioni correttive.

4. Definire i server proxy necessari per consentire l'accesso a Internet e poi cliccare su **Next**. Eseguire una delle seguenti procedure.

- Deselezionare la casella accanto ai server che **non** si desidera includere come server proxy.
- Cliccare su **Add** per aggiungere nuovi server, inserire i dati relativi al server proxy e cliccare su **OK**. Ripetere eventualmente questo passaggio per aggiungere altri server. Una volta creati, questi server possono essere gestiti dalla pagina **Enforce > Network Resources** .

**Nota:** i server proxy selezionati sostituiranno tutti i server che si trovano correntemente nel modello di accesso predefinito di DHCP - Internet Access DHCP Enforcer.

5. Definire i server di correzione necessari per apportare correzioni all'accesso, quali controller di dominio, e successivamente cliccare su **Next**.

Eseguire una delle seguenti procedure.

- Deselezionare la casella accanto ai server che **non** si desidera includere come server di correzione.
- Cliccare su **Add** per aggiungere nuovi server, inserire i dati relativi al server di correzione e cliccare su **OK**. Ripetere eventualmente questo passaggio per aggiungere altri server. Una volta creati, questi server possono essere gestiti dalla pagina **Enforce > Network Resources** .

**Nota:** i server di correzione selezionati sostituiranno tutti i server che si trovano correntemente nel modello di accesso predefinito di DHCP - Remediation Access DHCP Enforcer.

6. Effettuare una delle seguenti operazioni:

- Se il Dissolvable Agent è installato, cliccare su **Yes** e successivamente su **Next**. Passare al punto seguente.
- Se il Dissolvable Agent **non** è installato, cliccare su **No** e successivamente su **Next**. Passare al punto 8.

**Nota:** se il Dissolvable Agent è stato installato nello stesso server di Sophos NAC, non è necessario creare un server del Dissolvable Agent aggiuntivo.

7. Definire i server che ospitano il Dissolvable Agent in modo tale che DHCP Enforcer ne possa consentire l'accesso. Questo tipo di accesso è necessario per poter consentire ai computer sconosciuti, quali i computer ospiti, di venire riconosciuti all'interno della rete. Cliccare su **Add** per aggiungere nuovi server, inserire i dati relativi al server del Dissolvable Agent e cliccare su **OK**. Quindi cliccare su **Next**. Una volta creati, questi server possono essere gestiti dalla pagina **Configure System > Server Settings** .

8. Definire i server che verranno utilizzati per l'attuazione DHCP. Cliccare su **Add** per aggiungere nuovi server, inserire i dati relativi al server di DHCP Enforcer e cliccare su **OK**. Ripetere eventualmente questo passaggio per aggiungere altri server. Quindi cliccare su **Next**. Una volta creati, questi server possono essere gestiti dalla pagina **Configure System > Server Settings** .

**Nota:** la chiave condivisa deve corrispondere a quanto inserito durante l'installazione di DHCP Enforcer nel server. La chiave condivisa viene utilizzata per proteggere il traffico tra Server NAC e il server DHCP.

9. Cliccare su **Fine**.

## 5.2 Esecuzione del report DHCP Enforcer

Prima di abilitare l'attuazione DHCP, eseguire il report DHCP Enforcer di Sophos NAC per determinare lo stato di conformità dei computer. I criteri predefiniti di NAC sono impostati su Report Only. Il report DHCP Enforcer è utilizzabile per stabilire se, una volta abilitata l'attuazione, verranno applicati i modelli di accesso corretti. Dal report DHCP Enforcer è possibile rendere esenti i dispositivi e accedere ai dati di rilevamento.

### Procedura

1. Accedere a NAC Manager.
2. Cliccare su **Report > Troubleshooting**.
3. Cliccare sull'elenco **Report Type** e selezionare **DHCP Enforcer**.
4. Se pertinente, cliccare sul **segno più** accanto a **Report Criteria** e digitare o selezionare le opzioni di ricerca appropriate. È anche possibile cliccare sul link **Custom Sort** per ampliare le opzioni di ordinamento; le opzioni di ordinamento personalizzato vengono modificate temporaneamente durante l'esecuzione del report.

**Nota:** è possibile utilizzare, nella maggior parte dei campi, il simbolo \* o % per eseguire una ricerca con caratteri jolly. Per esempio, se si digita M% nel campo Returned User Class, vengono visualizzate tutte le classi di utenti che iniziano con la lettera M. Se invece si specifica M senza il carattere %, verranno visualizzate solo le classi di utenti con il nome M.

5. Cliccare su **Run**.

### Campi e descrizioni

Campo	Descrizione
<b>Voce del report riepilogativo</b>	
Date/Time	Data e ora del tentativo di accesso alla rete. <b>Nota:</b> la data e l'ora vengono ricavate dal fuso orario del browser web che accede a NAC Manager.
MAC Address	Indirizzo MAC del dispositivo che sta tentando di connettersi alla rete. L'indirizzo MAC elencato è assegnato al NIC associato alla richiesta del client DHCP.
Computer Name	Nome del dispositivo che sta tentando di connettersi alla rete. Nome del computer ricavato dalla richiesta del client.
Compliance State	Stato di conformità di un computer, assegnato durante la verifica della conformità. Gli stati di conformità disponibili sono Compliant, Partially Compliant e Non-Compliant. Un trattino triplo (---) indica che l'agente non ha registrato alcuno stato di conformità. L'accesso alla rete è determinato dai

Campo	Descrizione
	modelli di accesso di DHCP Enforcer conformi, associati allo stato di conformità del criterio.
Template Name (Version)	<p>Nome e versione del modello di accesso che determina l'azione intrapresa dall'Agent Enforcer. Il modello di accesso utilizzato si basa sul motivo. I modelli di accesso disponibili includono i seguenti modelli predefiniti, oltre che i modelli personalizzati:</p> <ul style="list-style-type: none"> <li>■ <b>DHCP - Full Access:</b> consente pieno accesso alla rete.</li> <li>■ <b>DHCP - Internet Access:</b> consente accesso a Internet, e nega l'accesso agli indirizzi IP privati e alla rete di area locale (LAN).  <b>Importante:</b> Se non viene definito un server proxy per l'accesso a internet come risorsa di rete, gli utenti non avranno accesso a internet, e questo modello fornirà esclusivamente accesso per azioni correttive.</li> <li>■ <b>DHCP - Remediation Access:</b> nega qualsiasi accesso alla rete, eccezion fatta per i server di correzione specificati, i Sophos Server NAC, e il server del Dissolvable Agent.</li> </ul>
Reason	<p>Motivo per cui un particolare modello di accesso è stato assegnato da DHCP Enforcer. Motivi disponibili:</p> <ul style="list-style-type: none"> <li>■ <b>Assessment:</b> la verifica eseguita dall'agente ha determinato lo stato di conformità. L'accesso alla rete è determinato dai modelli di accesso di DHCP Enforcer conformi, associati allo stato di conformità del criterio. Viene visualizzato un collegamento che dà accesso ai dati della verifica di conformità associata a questa voce di DHCP Enforcer.</li> <li>■ <b>Default Template:</b> il computer può avere un criterio associato oppure essere un'esenzione designata, ma non è stato trovato un modello di accesso associato. L'accesso alla rete è determinato dai modelli di accesso predefiniti designati nell'area <b>Configure System &gt; Enforcer Settings</b> .</li> <li>■ <b>Enforcer Override:</b> l'attuazione non è stata verificata. Se la casella Override DHCP Enforcer nell'area <b>Configure System &gt; Enforcer Settings</b> è spuntata, l'accesso alla rete è determinato dai modelli di accesso Maintenance Mode/Enforcer Override, designati nella medesima area.</li> <li>■ <b>Exempted:</b> il computer è esentato in base ai criteri di esenzione definiti nell'area <b>Enforce &gt; Exemptions</b> . L'accesso alla rete è determinato dai modelli di accesso associati al criterio di esenzione. I seguenti sottomotivi di Exempted sono visualizzati fra parentesi: <ul style="list-style-type: none"> <li>■ <b>User Class:</b> la classe dell'utente specificata come esenzione.</li> <li>■ <b>Vendor Class:</b> la classe del fornitore specificata come esenzione.</li> <li>■ <b>MAC:</b> l'indirizzo MAC specificato come esenzione.</li> <li>■ <b>IP Scope:</b> l'ambito IP specificato come esenzione.</li> </ul> </li> <li>■ <b>Maintenance Mode:</b> il software è in modalità manutenzione. L'accesso alla rete è determinato dai modelli di accesso Maintenance Mode/Enforcer Override designati nell'area <b>Configure System &gt; Enforcer Settings</b> .</li> </ul>

Campo	Descrizione
	<ul style="list-style-type: none"> <li>■ <b>Policy Retrieval Error:</b> lo stato di conformità del computer è obsoleto secondo il campo DHCP Policy Update Threshold configurato nell'area <b>Configure System &gt; Enforcer Settings</b> . L'accesso alla rete è determinato dai modelli di accesso di DHCP Enforcer del criterio e associati allo stato Policy Retrieval Error.</li> <li>■ <b>Remediate:</b> il criterio è in modalità Remediate. L'accesso alla rete è determinato dai modelli di accesso di DHCP Enforcer associati alla modalità Remediate del criterio.</li> <li>■ <b>Report Only:</b> il criterio è in modalità Report Only. L'accesso alla rete è determinato dai modelli di accesso di DHCP Enforcer associati alla modalità Report Only del criterio.</li> <li>■ <b>Reserved:</b> l'indirizzo MAC del dispositivo che richiede accesso alla rete è riservato come dispositivo speciale nel server DHCP.</li> <li>■ <b>System Error:</b> Enforcer ha riscontrato un errore che ha impedito il completamento dell'operazione. L'impostazione del registro SystemErrors del Server NAC nega l'accesso alla rete per impostazione predefinita.</li> <li>■ <b>Template Error:</b> non è stato rilevato alcun modello associato e i modelli di accesso predefiniti designati nell'area <b>Configure System &gt; Enforcer Settings</b> non possono essere utilizzati. Se si riceve questo errore, l'accesso alla rete è determinato dal server DHCP, che non restituirà una classe di utenti e negherà accesso all'utente.</li> <li>■ <b>Unknown Endpoint:</b> non esiste alcun dato relativo alla conformità. L'accesso alla rete è determinato dai modelli di accesso Unknown Endpoint designati nell'area <b>Configure System &gt; Enforcer Settings</b> .</li> </ul>
Returned User Class	Classe dell'utente DHCP restituita al server DHCP dal DHCP Enforcer per l'attuazione.
DHCP Server	Indirizzo IP del server DHCP che ha richiesto l'accesso alla rete da DHCP Enforcer. Si tratta del server DHCP nel quale DHCP Enforcer è installato.
<b>Voce del report nel dettaglio</b>	
Agent Enforcement Action	<p>Azione intrapresa dal computer riguardo l'assegnazione dell'indirizzo IP. Il computer inizia il rilascio e rinnovo degli indirizzi IP in base all'azione dell'Agent Enforcement specificata nel criterio. L'agente ottiene indirizzi IP nuovi: quando si avvia e inizia la verifica della conformità, quando lo stato di conformità del computer cambia, quando la modalità del criterio cambia, quando i modelli di accesso di DHCP Enforcer definiti nel criterio del computer cambiano. Valori disponibili:</p> <ul style="list-style-type: none"> <li>■ <b>None:</b> gli indirizzi IP per il computer non sono né rilasciati né rinnovati.</li> <li>■ <b>Release Renew:</b> gli indirizzi IP per il computer vengono rilasciati e poi rinnovati utilizzando il server DHCP. Gli indirizzi IP correnti vengono abbandonati prima di ottenere quelli nuovi.</li> <li>■ <b>Triple Dash (---):</b> l'agente non ha registrato alcuna azione.</li> </ul>

Campo	Descrizione
Vendor Class	Classe del produttore del client DHCP.
DHCP Relay	Indirizzo IP del relay DHCP (se presente nella richiesta DHCP originale) utilizzato da DHCP Enforcer per selezionare un modello di accesso di DHCP Enforcer. Se non si utilizza un relay DHCP viene visualizzato 0.0.0.0.
Transaction ID	Identificativo della transazione che viene restituito dal server DHCP. L'identificativo della transazione associa i messaggi del client DHCP con le risposte del server.

### 5.3 Creazione delle esenzioni DHCP

I computer esentati non possono eseguire il Compliance Agent; si tratta per esempio di computer con sistemi operativi non Windows. Le esenzioni vengono inoltre applicate ai computer che non richiedono la verifica della conformità, quali server, router e stampanti. I computer a cui è assegnato un indirizzo IP in modo dinamico tramite DHCP sono i soli computer a poter essere esentati. Per tali computer è necessario creare delle esenzioni DHCP; in caso contrario, una volta abilitata l'attuazione DHCP, sarà loro negato l'accesso alla rete.

Tramite NAC Manager si possono creare due tipi di esenzioni DHCP:

- **Esenzioni per criteri DHCP:** esenzioni create in base a indirizzo MAC, classe dell'utente e del produttore del software
- **Esenzioni per ambito IP:** esenzioni create per segmenti di rete.

#### 5.3.1 Creazione di esenzioni per i criteri DHCP

Utilizzare la pagina Exemptions di NAC Manager per creare le esenzioni per i criteri DHCP. Per individuare le esenzioni e designare le azioni, vengono utilizzati congiuntamente i criteri di esenzione e i modelli di accesso di DHCP Enforcer. Una volta soddisfatto il criterio di esenzione definito, il modello di accesso di DHCP Enforcer associato determina l'azione di accesso alla rete più appropriata da intraprendere.

##### Procedura

1. Accedere a NAC Manager.
2. Cliccare su **Enforce > Exemptions**. Quindi, cliccare su **Create Exemption** nella pagina in basso a sinistra.
3. Digitare un nome e una descrizione per l'esenzione.
4. Cliccare sull'elenco **Exemption Type** e selezionare **DHCP Criteria**.

5. In **Exemption Criteria**, per indicare quale criterio di esenzione si desidera definire: cliccare sul pulsante di opzione **MAC Address**, **User Class** o **Vendor Class**, nel relativo campo digitare l'appropriato indirizzo MAC (o prefisso), classe dell'utente o classe del fornitore e infine cliccare su **Add**.

Ripetere eventualmente questo passaggio per aggiungere altri criteri di esenzione.

**Nota:** per specificare le esenzioni si può utilizzare il carattere \* , purché sia l'ultimo del nome. Per esempio, se si specifica AA\* come indirizzo MAC, verranno esentati tutti gli indirizzi MAC che iniziano con AA. Se si specifica un indirizzo MAC senza il simbolo \* , è necessario indicare l'esatto indirizzo MAC che si desidera esentare.

6. Cliccare su **Select** per aggiungere all'esenzione modelli di accesso di DHCP Enforcer, selezionare il modello di accesso **DHCP - Full Access** e cliccare su **OK**.

In Sophos NAC, il modello di accesso **DHCP - Full Access** è predefinito in modo tale da consentire accesso alla rete. Questa esenzione è così configurata per consentire l'accesso alla rete senza alcuna verifica della conformità da parte di Sophos NAC.

7. Cliccare su **Save**.

### 5.3.2 Creazione delle esenzioni per ambito IP

I computer a cui è assegnato un indirizzo IP in modo dinamico tramite DHCP sono i soli computer a poter essere esentati. Utilizzare la pagina **Exemptions** di NAC Manager per creare le esenzioni per ambito IP. Le esenzioni per ambito IP sono esenzioni create per segmenti di rete. Le esenzioni per ambito IP sono utili per implementare l'attuazione in fasi in tutta l'azienda; è possibile esentare dei segmenti di rete che non si desidera ancora sottoporre all'attuazione dei criteri di sicurezza.

#### Procedura

1. Accedere a NAC Manager.
2. Cliccare su **Enforce > Exemptions** . Quindi, cliccare su **Create Exemption** nella pagina in basso a sinistra.
3. Digitare un nome e una descrizione per l'esenzione.
4. Cliccare sull'elenco **Exemption Type** e selezionare **IP Scope**.
5. Sotto **Exempted IP Scopes**, cliccare su **Select** per aggiungere uno scope IP all'esenzione, selezionare gli scope appropriati e cliccare su **OK**.  
Se non si trova lo scope IP che si sta cercando, è possibile crearlo. Per far ciò è necessario creare un nuovo modello di accesso di DHCP Enforcer o aggiornare uno di quelli predefiniti.
6. Eventualmente, utilizzare le frecce per determinare la priorità degli intervalli.

Se a una particolare esenzione è applicato più di uno scope IP, viene utilizzato il primo di essi. Sophos consiglia di dare maggiore priorità agli scope IP più specifici e di dare minore priorità a quelli meno specifici.

7. Cliccare su **Save**.

**Importante:** una volta create le esenzioni, è possibile ordinarle per priorità nella pagina **Exemptions**. Se a un particolare computer è applicata più di una esenzione, viene utilizzata la prima di esse. Sophos consiglia di dare maggiore priorità alle esenzioni più specifiche e di dare minore priorità a quelle meno specifiche.

## 5.4 Abilitazione dell'attuazione DHCP

È possibile abilitare l'attuazione DHCP sia per computer sconosciuti che noti. Sophos consiglia di utilizzare l'attuazione DHCP per i computer sconosciuti e quella dell'agente per i computer noti. Sophos NAC consente comunque l'utilizzo dell'attuazione DHCP anche per i computer noti.

### 5.4.1 Abilitazione dell'attuazione DHCP per computer sconosciuti

È possibile abilitare l'attuazione DHCP per computer sconosciuti su tutti i server DHCP. Ciò consente di specificare quali server DHCP metteranno in quarantena i computer sconosciuti. Utilizzare questa funzione per svolgere l'attuazione DHCP in fasi.

Prima di abilitare l'attuazione DHCP per computer autonomi, è necessario creare le esenzioni. I computer a cui è assegnato un indirizzo IP in modo dinamico tramite DHCP sono i soli computer a poter essere esentati.

#### Procedura

1. Accedere a NAC Manager.
2. Cliccare su **Configure System > Server Settings**.
3. Cliccare sul nome del server DHCP per cui si desidera abilitare l'attuazione DHCP.
4. Cliccare sull'elenco **Unknown Endpoint Mode** e selezionare **Enforce**. La modalità Enforce utilizza il modello di accesso "DHCP - Internet Access" per mettere in quarantena i computer sconosciuti e consentire l'accesso a internet o a server di correzione.

**Nota:** se si è specificato un server proxy durante l'esecuzione della procedura guidata di configurazione di DHCP, i computer possono accedere a internet. Se invece non è stato specificato un server proxy, i computer possono accedere ai server di correzione precedentemente indicati durante la procedura guidata di configurazione di DHCP. È possibile cambiare il modello di accesso nell'area **Configure System > Enforcer Settings**.

5. Cliccare su **Save**.

### 5.4.2 Abilitazione dell'attuazione DHCP per computer noti

È possibile abilitare l'attuazione DHCP per i computer noti nei criteri. Se per i computer noti si intende utilizzare l'attuazione DHCP o dell'agente, è necessario cambiare, nei relativi criteri, la modalità del criterio (Policy Mode) da Report Only a Enforce.

**Importante:** tutti i criteri e le modifiche agli stessi hanno effetto immediato, ma un criterio non viene applicato finché l'agente non lo recupera.

## Procedura

1. Accedere a NAC Manager.
2. Cliccare su **Manage > Policies** . Quindi, cliccare sul nome del criterio che si desidera aggiornare.
3. Cliccare sull'elenco **Policy Mode** e selezionare **Enforce**.
  - **Enforce:** la modalità del criterio Enforce indica che i computer sono valutati in base al criterio assegnato e che all'interno di NAC Manager viene generato un report informativo. I messaggi vengono visualizzati e vengono intraprese azioni correttive e di attuazione tramite i modelli di accesso relativi agli adeguati stati di accesso. La modalità Enforce utilizza i modelli di accesso assegnati al punto 5.
4. Cliccare sull'elenco **Agent Enforcement Action** e selezionare **Release Renew**. È **necessario** selezionare Release Renew quando si utilizza l'attuazione DHCP per computer noti.
5. Nell'area di navigazione Network Access a sinistra, cliccare su **DHCP**. Cliccare sulla scheda **Enforce** e verificare le assegnazioni dei modelli di accesso.

**Nota:** Per impostazione predefinita, ogni criterio viene automaticamente popolato con i modelli di accesso. Assicurarsi che siano applicati i modelli di accesso corretti. Conservare le assegnazioni dei modelli di accesso Report Only e Remediate.

### Assegnazione dei modelli di DHCP Enforcer predefiniti

- **Policy Retrieval Error:** lo stato di conformità del computer è obsoleto secondo il campo DHCP Policy Update Threshold configurato nell'area **Configure System > Enforcer Settings** . Il modello di accesso DHCP - Remediation Access nega l'accesso alla rete, eccezion fatta per i server di correzione specificati durante l'esecuzione della procedura guidata di configurazione di DHCP.
  - **Compliant:** il computer è conforme. Il modello di accesso DHCP - Full Access consente l'accesso alla rete quando il computer è conforme.
  - **Partially Compliant:** il computer è parzialmente conforme. Il modello di accesso DHCP - Full Access consente l'accesso alla rete quando il computer è parzialmente conforme.
  - **Non-Compliant:** il computer non è conforme. Il modello di accesso DHCP - Remediation Access nega l'accesso alla rete, eccezion fatta per i server di correzione specificati durante l'esecuzione della procedura guidata di configurazione di DHCP.
6. Eventualmente, utilizzare le frecce per ordinare i modelli di accesso di DHCP Enforcer in base alla priorità.

Se più di un modello è applicabile a un particolare stato, viene utilizzato il primo modello che soddisfa tale stato. Sophos consiglia di dare maggiore priorità ai modelli di accesso più specifici/rigidi e di dare minore priorità a quelli meno specifici/rigidi.
  7. Cliccare su **Save**.

#### 5.4.2.1 Utilizzo dei criteri predefiniti

È possibile utilizzare i criteri predefiniti per supportare la conformità ai criteri di protezione per computer gestiti e non.

- **Default:** questo criterio viene utilizzato se in un computer è installato il Compliance Agent, ma non gli è stato attribuito alcun criterio. Per impostazione predefinita, il criterio è in modalità Report Only. Se il criterio è impostato su Remediate o Enforce, tale criterio svolgerà azioni correttive sul computer.
- **Managed:** questo criterio può essere utilizzato per i computer che sono gestiti da Sophos Enterprise Console e che hanno il Compliance Agent installato. Per impostazione predefinita, il criterio è in modalità Report Only. Se il criterio è impostato su Remediate o Enforce, tale criterio svolgerà azioni correttive sul computer.
- **Unmanaged:** questo criterio può essere utilizzato per i computer esterni all'azienda. Non svolge attività correttive nel computer. Il Dissolvable Agent utilizza il criterio Unmanaged.

**Nota:** se il computer non ha un Compliance Agent installato e non utilizza il Dissolvable Agent, l'accesso alla rete sarà determinato dalle impostazioni di Enforcer.

#### 5.4.3 Esperienza dell'utente relativa all'attuazione DHCP

Una volta abilitata l'attuazione DHCP, l'utente può trovarsi in situazioni diverse a seconda che il computer sia sconosciuto o noto. Gli ospiti possono anche eseguire il Compliance Dissolvable Agent per ottenere accesso alla rete.

- **Computer sconosciuti** non sono gestiti dal Compliance Agent, non dispongono del Compliance Agent installato, non sono esenti e non hanno eseguito il Dissolvable Agent.
- **Computer ospiti** possono eseguire il Compliance Dissolvable Agent per il controllo dell'accesso alla rete.
- **Computer noti** sono gestiti da Sophos Enterprise Console e hanno il Compliance Agent installato e operativo.

##### Esperienza dell'utente relativa all'attuazione DHCP in computer sconosciuti

Quando l'attuazione DHCP è abilitata, i computer sconosciuti si troveranno nella seguente situazione:

1. Il computer viene avviato.
2. Quando l'attuazione DHCP per computer sconosciuti è abilitata, tali computer ricevono accesso limitato alla rete. È loro permesso di accedere a internet o a server di correzione. Se si è specificato un server proxy durante l'esecuzione della procedura guidata di configurazione di DHCP, i computer possono accedere a internet. Se invece non è stato specificato un server proxy, i computer possono accedere ai server di correzione precedentemente indicati durante la procedura guidata di configurazione di DHCP.

##### Esperienza dell'utente relativa all'attuazione DHCP in computer ospiti

Quando l'attuazione DHCP è abilitata e ai computer ospiti è richiesto di utilizzare il Compliance Dissolvable Agent, gli utenti ospiti si troveranno nella seguente situazione:

1. Il computer viene avviato.

2. L'utente apre Internet Explorer, inserisce l'URL del Compliance Dissolvable Agent ed esegue il Compliance Dissolvable Agent.
3. Il Compliance Dissolvable Agent conduce una verifica e stabilisce se il computer è conforme, parzialmente conforme o non conforme al criterio di NAC.
4. Quando l'attuazione DHCP è configurata e abilitata, si verifica quanto riportato di seguito:
  - I computer conformi possono accedere alla rete.
  - I computer parzialmente conformi possono accedere alla rete. Il Compliance Dissolvable Agent visualizza messaggi agli utenti in modo tale che possano apportare azioni correttive sui loro computer e renderli conformi. Se il criterio di NAC è configurato in modo tale da apportare automaticamente azioni correttive sul computer, vengono svolte tali azioni. Per impostazione predefinita, l'azione correttiva è disabilitata. Nella maggior parte dei casi, non si desidera apportare azioni correttive su computer ospiti.
  - I computer non conformi non possono accedere alla rete. È loro permesso di accedere a internet o a server di correzione. Se si è specificato un server proxy durante l'esecuzione della procedura guidata di configurazione di DHCP, i computer possono accedere a internet. Se invece non è stato specificato un server proxy, i computer possono accedere ai server di correzione precedentemente indicati durante la procedura guidata di configurazione di DHCP. Il Compliance Dissolvable Agent visualizza messaggi agli utenti in modo tale che possano apportare azioni correttive sui loro computer e renderli conformi. Se il criterio di NAC è configurato in modo tale da apportare automaticamente azioni correttive sul computer, vengono svolte tali azioni. Per impostazione predefinita, l'azione correttiva è disabilitata. Nella maggior parte dei casi, è meglio non apportare azioni correttive su computer ospiti.

### **Esperienza dell'attuazione DHCP per computer noti**

Quando l'attuazione DHCP è abilitata, i computer noti si troveranno nella seguente situazione concernente DHCP:

1. Il computer viene avviato ed esegue il Compliance Agent.
2. Il Compliance Agent conduce una verifica e stabilisce se il computer è conforme, parzialmente conforme o non conforme al criterio di NAC.
3. Quando l'attuazione DHCP è configurata e abilitata, si verifica quanto riportato di seguito:
  - I computer conformi possono accedere alla rete.
  - I computer parzialmente conformi possono accedere alla rete. Il Compliance Agent visualizza messaggi agli utenti in modo tale che possano apportare azioni correttive sui loro computer e renderli conformi. Se il criterio di NAC è configurato in modo tale da apportare automaticamente azioni correttive sul computer, vengono svolte tali azioni.
  - I computer non conformi non possono accedere alla rete. Possono accedere ai server di correzione specificati durante l'esecuzione della procedura guidata di configurazione di DHCP. Il Compliance Agent visualizza messaggi agli utenti in modo tale che possano apportare azioni correttive sui loro computer e renderli conformi. Se il criterio di NAC è configurato in modo tale da apportare automaticamente azioni correttive sul computer, vengono svolte tali azioni.

## 6 Appendice A: Upgrade dell'attuazione DHCP senza riconfigurazione

Per utilizzare l'attuazione DHCP in Sophos NAC versione 3.5, è necessario effettuare l'upgrade del software dell'attuazione DHCP.

- Se l'attuazione DHCP è stata installata per la prima volta in NAC versione 3.3, non è richiesta la riconfigurazione della stessa. In questo caso, durante l'upgrade, l'attuazione DHCP di cui si dispone funzionerà senza alcun problema.
- Se si sta effettuando l'upgrade da NAC versione 3.1.2 alla versione 3.5, è necessario riconfigurare l'attuazione DHCP. Per ulteriori informazioni, consultare la sezione [Appendice B: Upgrade dell'attuazione DHCP con riconfigurazione](#) a pagina 26.



**Attenzione:** Per eseguire l'upgrade, è necessario disattivare l'attuazione DHCP. Sophos consiglia di svolgere l'upgrade dell'attuazione DHCP ad un orario in cui i rischi ai quali è esposta la propria rete siano minimi.

Per effettuare l'upgrade della configurazione di DHCP da NAC versione 3.3 alla versione 3.5, è necessario disinstallare l'attuale software DHCP Enforcer, e successivamente installare quello nuovo. È inoltre necessario disabilitare l'attuazione DHCP prima di disinstallare il software ed abilitare l'attuazione DHCP dopo aver installato il nuovo software.

### 6.1 Checklist per l'upgrade dell'attuazione DHCP senza riconfigurazione

La checklist per l'upgrade dell'attuazione DHCP senza riconfigurazione fornisce un elenco di operazioni necessarie per l'upgrade dell'attuazione DHCP da Sophos NAC versione 3.3 alla versione 3.5. È possibile completare tutte le operazioni seguendo le istruzioni contenute in questo documento, se non diversamente indicato.

Operazione	Descrizione	Completata
<b>Upgrade di Sophos NAC</b>		
1.	Effettuare l'upgrade Sophos NAC. Per ulteriori informazioni, visitare il <b>Centro Upgrade di Endpoint Security and Control 9.5</b> su <a href="http://www.sophos.it/support/upgrades">http://www.sophos.it/support/upgrades</a> .	
<b>Operazioni di Sophos NAC Manager, parte 1</b>		
2.	Disattivare l'attuazione DHCP	
<b>Operazioni del server DHCP</b>		
3.	Disinstallare il software DHCP Enforcer attualmente in uso da tutti i server DHCP.	

Operazione	Descrizione	Completata
4.	<p>Installare il nuovo software DHCP Enforcer su tutti i server DHCP.</p> <p><b>Importante:</b> quando si installa la versione 3.5 del software DHCP Enforcer su un server DHCP, è necessario inserire nuovamente una chiave condivisa. Se possibile, utilizzare la stessa chiave condivisa della versione 3.3, poiché in questo modo corrisponderà alla chiave condivisa di NAC Manager per lo stesso server DHCP. Se non si è a conoscenza della chiave condivisa utilizzata nella versione 3.3, è possibile crearne una nuova durante l'installazione del software. Tuttavia, è poi necessario aggiornare anche la chiave condivisa di NAC Manager per il server DHCP in questione, in modo che le chiavi siano identiche.</p> <p><b>Nota:</b> Dopo aver installato il software DHCP Enforcer, è necessario verificare che DHCP Enforcer sia in esecuzione su ciascun server DHCP.</p>	
<b>Operazioni di Sophos NAC Manager, parte 2</b>		
5.	Aggiornare la chiave condivisa di ciascun server DHCP (operazione facoltativa).	
6.	Abilitare l'attuazione DHCP.	

## 6.2 Disabilitazione dell'attuazione DHCP

Quando si esegue l'upgrade dell'attuazione DHCP, è necessario disabilitarla sia sui computer noti, sia su quelli sconosciuti. Sophos consiglia di utilizzare l'attuazione DHCP per i computer sconosciuti e quella dell'agente per i computer noti. Sophos NAC consente comunque l'utilizzo dell'attuazione DHCP anche per i computer noti.

### 6.2.1 Disabilitazione dell'attuazione DHCP per computer sconosciuti

Per disabilitare l'attuazione DHCP per i computer sconosciuti, è necessario cliccare su "Unknown Endpoint Mode" su ciascun server DHCP, e modificare tale modalità da "Enforce" a "Report Only". Utilizzare questa funzione quando si effettua l'upgrade dell'attuazione DHCP.

#### Procedura

1. Cliccare su **Configure System > Server Settings**.
2. Cliccare sul nome del server DHCP per cui si desidera disabilitare l'attuazione DHCP.
3. Cliccare sull'elenco **Unknown Endpoint Mode** e selezionare **Report Only**. La modalità di criterio Report Only utilizza il modello di accesso "DHCP - Full Access", per consentire l'accesso alla rete ai computer sconosciuti.
4. Cliccare su **Save**.

## 6.2.2 Disabilitazione dell'attuazione DHCP per computer noti

Per disabilitare l'attuazione DHCP è necessario cambiare la modalità del criterio ("Policy Mode") da "Enforce" a "Report Only", nei rispettivi criteri. Utilizzare questa funzione quando si effettua l'upgrade dell'attuazione DHCP.

**Importante:** tutti i criteri e le modifiche agli stessi hanno effetto immediato, ma un criterio non viene applicato finché l'agente non lo recupera.

**Nota:** se si utilizza l'attuazione dell'agente invece dell'attuazione DHCP per i computer noti, non è richiesta tale operazione.

### Procedura

1. Accedere a NAC Manager.
2. Cliccare su **Manage > Policies** . Quindi, cliccare sul nome del criterio che si desidera aggiornare.
3. Cliccare sull'elenco **Policy Mode** e selezionare **Report Only**.
  - **Report Only:** la modalità di criterio Report Only indica che i computer sono valutati in base al criterio assegnato e, all'interno di NAC Manager, viene generato un report informativo. Non viene visualizzato alcun messaggio e non viene intrapresa alcuna azione correttiva o di attuazione. la modalità Report Only utilizza il modello di accesso "DHCP - Full Access", per consentire l'accesso alla rete ai computer noti.
4. Cliccare su **Save**.

## 6.3 Disinstallazione del software DHCP Enforcer

Disinstallare il software DHCP Enforcer da tutti i server Microsoft DHCP. Il software DHCP Enforcer include DHCP Enforcer e l'utilità di configurazione di DHCP Enforcer.

1. Dal menu Start, selezionare **Pannello di controllo > Installazione applicazioni** .
2. Selezionare il software **Sophos DHCP Enforcer** e poi cliccare su Rimuovi.
3. Per confermare la rimozione del software DHCP Enforcer, cliccare su **Sì**.

## 6.4 Installazione del software DHCP Enforcer

Installare il software DHCP Enforcer in tutti i server Microsoft DHCP. Il software DHCP Enforcer include DHCP Enforcer e l'utilità di configurazione di DHCP Enforcer. Durante l'installazione viene configurato il server DHCP. Se si desidera modificare le impostazioni del server DHCP specificate durante l'installazione di DHCP Enforcer, utilizzare l'utilità di configurazione di DHCP Enforcer. Per ulteriori informazioni, consultare la sezione [Appendice C: Utilizzo dell'utilità di configurazione di DHCP Enforcer](#) a pagina 40.

1. Andare al sito web di Sophos, scaricare il programma di installazione di Sophos NAC per DHCP Enforcer ed eseguirlo.

In alternativa, inserire il CD Sophos per l'installazione di DHCP Enforcer. Il CD si avvia automaticamente.

2. Viene avviata la procedura guidata di installazione. Nella finestra di dialogo **Benvenuti nella procedura guidata per la protezione dei computer**, cliccare su **Avanti**.
3. Nella finestra di dialogo **Sophos DHCP Enforcer**, inserire l'indirizzo IP del Server NAC, la chiave condivisa del Server NAC e la conferma della chiave condivisa. Cliccare su **Avanti**. Memorizzare la chiave condivisa inserita. La chiave condivisa viene utilizzata per proteggere il traffico tra Server NAC e il server DHCP. Quando si esegue la procedura guidata di configurazione di DHCP tramite NAC Manager, si deve utilizzare la medesima chiave condivisa. Una volta identificato un server DHCP in NAC Manager, è possibile aggiornarne la chiave condivisa nell'area **Configure System > Server Settings**.
4. Nella finestra di dialogo **Pronta per l'installazione del programma**, cliccare su **Installa** per installare DHCP Enforcer.
5. Cliccare su **Fine**.

**Nota:** dopo aver installato il software DHCP Enforcer, è necessario verificare che DHCP Enforcer sia in esecuzione su ciascun server DHCP.

## 6.5 Aggiornamento della chiave condivisa del server DHCP

La chiave condivisa viene utilizzata per proteggere il traffico tra Server NAC e il server DHCP.

Quando si installa la versione 3.5 del software DHCP Enforcer su un server DHCP, è necessario inserire nuovamente una chiave condivisa. Se possibile, utilizzare la stessa chiave condivisa della versione 3.3, poiché in questo modo corrisponderà alla chiave condivisa di NAC Manager per lo stesso server DHCP. Se non si è a conoscenza della chiave condivisa utilizzata nella versione 3.3, è possibile crearne una nuova durante l'installazione del software. Tuttavia, è poi necessario aggiornare anche la chiave condivisa di NAC Manager per il server DHCP in questione, in modo che le chiavi siano identiche.

**Nota:** se, durante l'installazione del software DHCP Enforcer, è stata utilizzata la chiave condivisa della versione 3.3, questa operazione non è richiesta.

### Procedura

1. Cliccare su **Configure System > Server Settings**.
2. Cliccare sul nome del server DHCP per il quale si desidera aggiornare la chiave condivisa.
3. Digitare e confermare la chiave condivisa del server.

**Importante:** la chiave condivisa deve corrispondere a quanto inserito durante l'installazione del software DHCP Enforcer sul server DHCP.

4. Cliccare su **Save**.

## 6.6 Abilitazione dell'attuazione DHCP

È possibile abilitare l'attuazione DHCP sia per computer sconosciuti che noti. Sophos consiglia di utilizzare l'attuazione DHCP per i computer sconosciuti e quella dell'agente per i computer noti. Sophos NAC consente comunque l'utilizzo dell'attuazione DHCP anche per i computer noti.

### 6.6.1 Abilitazione dell'attuazione DHCP per computer sconosciuti

È possibile abilitare l'attuazione DHCP per computer sconosciuti su tutti i server DHCP. Ciò consente di specificare quali server DHCP metteranno in quarantena i computer sconosciuti. Utilizzare questa funzione per svolgere l'attuazione DHCP in fasi.

Prima di abilitare l'attuazione DHCP per computer autonomi, è necessario creare le esenzioni. I computer a cui è assegnato un indirizzo IP in modo dinamico tramite DHCP sono i soli computer a poter essere esentati.

#### Procedura

1. Accedere a NAC Manager.
2. Cliccare su **Configure System** > **Server Settings**.
3. Cliccare sul nome del server DHCP per cui si desidera abilitare l'attuazione DHCP.
4. Cliccare sull'elenco **Unknown Endpoint Mode** e selezionare **Enforce**. La modalità Enforce utilizza il modello di accesso "DHCP - Internet Access" per mettere in quarantena i computer sconosciuti e consentire l'accesso a internet o a server di correzione.

**Nota:** se si è specificato un server proxy durante l'esecuzione della procedura guidata di configurazione di DHCP, i computer possono accedere a internet. Se invece non è stato specificato un server proxy, i computer possono accedere ai server di correzione precedentemente indicati durante la procedura guidata di configurazione di DHCP. È possibile cambiare il modello di accesso nell'area **Configure System** > **Enforcer Settings**.

5. Cliccare su **Save**.

### 6.6.2 Abilitazione dell'attuazione DHCP per computer noti

È possibile abilitare l'attuazione DHCP per i computer noti nei criteri. Se per i computer noti si intende utilizzare l'attuazione DHCP o dell'agente, è necessario cambiare, nei relativi criteri, la modalità del criterio (Policy Mode) da Report Only a Enforce.

**Importante:** tutti i criteri e le modifiche agli stessi hanno effetto immediato, ma un criterio non viene applicato finché l'agente non lo recupera.

#### Procedura

1. Accedere a NAC Manager.
2. Cliccare su **Manage** > **Policies**. Quindi, cliccare sul nome del criterio che si desidera aggiornare.
3. Cliccare sull'elenco **Policy Mode** e selezionare **Enforce**.
  - **Enforce:** la modalità del criterio Enforce indica che i computer sono valutati in base al criterio assegnato e che all'interno di NAC Manager viene generato un report informativo. I messaggi vengono visualizzati e vengono intraprese azioni correttive e di attuazione tramite i modelli di accesso relativi agli adeguati stati di accesso. La modalità Enforce utilizza i modelli di accesso assegnati al punto 5.
4. Cliccare sull'elenco **Agent Enforcement Action** e selezionare **Release Renew**. È necessario selezionare Release Renew quando si utilizza l'attuazione DHCP per computer noti.

5. Nell'area di navigazione Network Access a sinistra, cliccare su **DHCP**. Cliccare sulla scheda **Enforce** e verificare le assegnazioni dei modelli di accesso.

**Nota:** Per impostazione predefinita, ogni criterio viene automaticamente popolato con i modelli di accesso. Assicurarsi che siano applicati i modelli di accesso corretti. Conservare le assegnazioni dei modelli di accesso Report Only e Remediate.

#### Assegnazione dei modelli di DHCP Enforcer predefiniti

- **Policy Retrieval Error:** lo stato di conformità del computer è obsoleto secondo il campo DHCP Policy Update Threshold configurato nell'area **Configure System > Enforcer Settings**. Il modello di accesso DHCP - Remediation Access nega l'accesso alla rete, eccezion fatta per i server di correzione specificati durante l'esecuzione della procedura guidata di configurazione di DHCP.
  - **Compliant:** il computer è conforme. Il modello di accesso DHCP - Full Access consente l'accesso alla rete quando il computer è conforme.
  - **Partially Compliant:** il computer è parzialmente conforme. Il modello di accesso DHCP - Full Access consente l'accesso alla rete quando il computer è parzialmente conforme.
  - **Non-Compliant:** il computer non è conforme. Il modello di accesso DHCP - Remediation Access nega l'accesso alla rete, eccezion fatta per i server di correzione specificati durante l'esecuzione della procedura guidata di configurazione di DHCP.
6. Eventualmente, utilizzare le frecce per ordinare i modelli di accesso di DHCP Enforcer in base alla priorità.  
Se più di un modello è applicabile a un particolare stato, viene utilizzato il primo modello che soddisfa tale stato. Sophos consiglia di dare maggiore priorità ai modelli di accesso più specifici/rigidi e di dare minore priorità a quelli meno specifici/rigidi.
  7. Cliccare su **Save**.

#### 6.6.2.1 Utilizzo dei criteri predefiniti

È possibile utilizzare i criteri predefiniti per supportare la conformità ai criteri di protezione per computer gestiti e non.

- **Default:** questo criterio viene utilizzato se in un computer è installato il Compliance Agent, ma non gli è stato attribuito alcun criterio. Per impostazione predefinita, il criterio è in modalità Report Only. Se il criterio è impostato su Remediate o Enforce, tale criterio svolgerà azioni correttive sul computer.
- **Managed:** questo criterio può essere utilizzato per i computer che sono gestiti da Sophos Enterprise Console e che hanno il Compliance Agent installato. Per impostazione predefinita, il criterio è in modalità Report Only. Se il criterio è impostato su Remediate o Enforce, tale criterio svolgerà azioni correttive sul computer.
- **Unmanaged:** questo criterio può essere utilizzato per i computer esterni all'azienda. Non svolge attività correttive nel computer. Il Dissolvable Agent utilizza il criterio Unmanaged.

**Nota:** se il computer non ha un Compliance Agent installato e non utilizza il Dissolvable Agent, l'accesso alla rete sarà determinato dalle impostazioni di Enforcer.

### 6.6.3 Esperienza dell'utente relativa all'attuazione DHCP

Una volta abilitata l'attuazione DHCP, l'utente può trovarsi in situazioni diverse a seconda che il computer sia sconosciuto o noto. Gli ospiti possono anche eseguire il Compliance Dissolvable Agent per ottenere accesso alla rete.

- **Computer sconosciuti** non sono gestiti dal Compliance Agent, non dispongono del Compliance Agent installato, non sono esenti e non hanno eseguito il Dissolvable Agent.
- **Computer ospiti** possono eseguire il Compliance Dissolvable Agent per il controllo dell'accesso alla rete.
- **Computer noti** sono gestiti da Sophos Enterprise Console e hanno il Compliance Agent installato e operativo.

#### Esperienza dell'utente relativa all'attuazione DHCP in computer sconosciuti

Quando l'attuazione DHCP è abilitata, i computer sconosciuti si troveranno nella seguente situazione:

1. Il computer viene avviato.
2. Quando l'attuazione DHCP per computer sconosciuti è abilitata, tali computer ricevono accesso limitato alla rete. È loro permesso di accedere a internet o a server di correzione. Se si è specificato un server proxy durante l'esecuzione della procedura guidata di configurazione di DHCP, i computer possono accedere a internet. Se invece non è stato specificato un server proxy, i computer possono accedere ai server di correzione precedentemente indicati durante la procedura guidata di configurazione di DHCP.

#### Esperienza dell'utente relativa all'attuazione DHCP in computer ospiti

Quando l'attuazione DHCP è abilitata e ai computer ospiti è richiesto di utilizzare il Compliance Dissolvable Agent, gli utenti ospiti si troveranno nella seguente situazione:

1. Il computer viene avviato.
2. L'utente apre Internet Explorer, inserisce l'URL del Compliance Dissolvable Agent ed esegue il Compliance Dissolvable Agent.
3. Il Compliance Dissolvable Agent conduce una verifica e stabilisce se il computer è conforme, parzialmente conforme o non conforme al criterio di NAC.
4. Quando l'attuazione DHCP è configurata e abilitata, si verifica quanto riportato di seguito:
  - I computer conformi possono accedere alla rete.
  - I computer parzialmente conformi possono accedere alla rete. Il Compliance Dissolvable Agent visualizza messaggi agli utenti in modo tale che possano apportare azioni correttive sui loro computer e renderli conformi. Se il criterio di NAC è configurato in modo tale da apportare automaticamente azioni correttive sul computer, vengono svolte tali azioni. Per impostazione predefinita, l'azione correttiva è disabilitata. Nella maggior parte dei casi, non si desidera apportare azioni correttive su computer ospiti.
  - I computer non conformi non possono accedere alla rete. È loro permesso di accedere a internet o a server di correzione. Se si è specificato un server proxy durante l'esecuzione della procedura guidata di configurazione di DHCP, i computer possono accedere a internet. Se invece non è stato specificato un server proxy, i computer possono accedere ai server di correzione precedentemente indicati durante la procedura guidata di

configurazione di DHCP. Il Compliance Dissolvable Agent visualizza messaggi agli utenti in modo tale che possano apportare azioni correttive sui loro computer e renderli conformi. Se il criterio di NAC è configurato in modo tale da apportare automaticamente azioni correttive sul computer, vengono svolte tali azioni. Per impostazione predefinita, l'azione correttiva è disabilitata. Nella maggior parte dei casi, è meglio non apportare azioni correttive su computer ospiti.

### **Esperienza dell'attuazione DHCP per computer noti**

Quando l'attuazione DHCP è abilitata, i computer noti si troveranno nella seguente situazione concernente DHCP:

1. Il computer viene avviato ed esegue il Compliance Agent.
2. Il Compliance Agent conduce una verifica e stabilisce se il computer è conforme, parzialmente conforme o non conforme al criterio di NAC.
3. Quando l'attuazione DHCP è configurata e abilitata, si verifica quanto riportato di seguito:
  - I computer conformi possono accedere alla rete.
  - I computer parzialmente conformi possono accedere alla rete. Il Compliance Agent visualizza messaggi agli utenti in modo tale che possano apportare azioni correttive sui loro computer e renderli conformi. Se il criterio di NAC è configurato in modo tale da apportare automaticamente azioni correttive sul computer, vengono svolte tali azioni.
  - I computer non conformi non possono accedere alla rete. Possono accedere ai server di correzione specificati durante l'esecuzione della procedura guidata di configurazione di DHCP. Il Compliance Agent visualizza messaggi agli utenti in modo tale che possano apportare azioni correttive sui loro computer e renderli conformi. Se il criterio di NAC è configurato in modo tale da apportare automaticamente azioni correttive sul computer, vengono svolte tali azioni.

## 7 Appendice B: Upgrade dell'attuazione DHCP con riconfigurazione

Per utilizzare l'attuazione DHCP in Sophos NAC versione 3.5, è necessario effettuare l'upgrade del software dell'attuazione DHCP.

- Se si sta effettuando l'upgrade da NAC versione 3.1.2 alla versione 3.5, è necessario riconfigurare l'attuazione DHCP.
- Se l'attuazione DHCP è stata installata per la prima volta in NAC versione 3.3, non è richiesta la riconfigurazione della stessa. In questo caso, durante l'upgrade, l'attuazione DHCP di cui si dispone funzionerà senza alcun problema. Per ulteriori informazioni, consultare la sezione [Appendice A: Upgrade dell'attuazione DHCP senza riconfigurazione](#) a pagina 18.



**Attenzione:** Per eseguire l'upgrade, è necessario disattivare l'attuazione DHCP. Sophos consiglia di svolgere l'upgrade dell'attuazione DHCP ad un orario in cui i rischi ai quali è esposta la propria rete siano minimi.

L'upgrade da NAC versione 3.1.2 alla versione 3.5 influisce sulla configurazione di DHCP nei seguenti modi:

- Rimuove i precedenti modelli di accesso di DHCP Enforcer da tutti i criteri e dalla pagina relativa alle impostazioni di Enforcer in NAC Manager.
- Aggiorna tutti i modelli di accesso di DHCP Enforcer creati e aventi l'opzione DHCP Subnet Override abilitata per limitare l'accesso alla rete.
- Aggiorna tutti i modelli di accesso di DHCP Enforcer creati e aventi l'opzione DHCP Subnet Override disabilitata per consentire l'accesso alla rete.

### 7.1 Checklist per l'upgrade dell'attuazione DHCP con riconfigurazione

La checklist per l'upgrade dell'attuazione DHCP con riconfigurazione fornisce un elenco di operazioni necessarie per l'upgrade dell'attuazione DHCP da Sophos NAC versione 3.1.2 alla versione 3.5. È possibile completare tutte le operazioni seguendo le istruzioni contenute in questo documento, se non diversamente indicato.

Operazione	Descrizione	Completata
<b>Upgrade di Sophos NAC</b>		
1.	Effettuare l'upgrade Sophos NAC. Per ulteriori informazioni, visitare il <b>Centro Upgrade di Endpoint Security and Control 9.5</b> su <a href="http://www.sophos.it/support/upgrades">http://www.sophos.it/support/upgrades</a> .	
<b>Operazioni di Sophos NAC Manager, parte 1</b>		
2.	Disabilitare l'attuazione DHCP (Operazione facoltativa).	
<b>Operazioni del server DHCP, parte 1</b>		

Operazione	Descrizione	Completata
3.	Disinstallare il software DHCP Enforcer attualmente in uso da tutti i server DHCP.	
4.	Installare il nuovo software DHCP Enforcer su tutti i server DHCP.	
<b>Operazioni di Sophos NAC Manager, parte 2</b>		
5.	Utilizzare la procedura guidata di configurazione di DHCP per eseguire la configurazione di proxy, azioni correttive, Dissolvable Agent e server DHCP da utilizzare con l'attuazione DHCP di Sophos NAC.	
6.	Eseguire il report DHCP Enforcer per: <ul style="list-style-type: none"> <li>■ Determinare se, una volta abilitata l'attuazione DHCP, ai computer noti verrà concesso l'adeguato accesso alla rete.</li> <li>■ Identificare i computer che richiedono esenzioni.</li> </ul>	
7.	Assicurarsi che alle attuali esenzioni sia assegnato il giusto modello di DHCP. Durante l'upgrade, alle esenzioni viene assegnato il modello "DHCP - Full Access". Se necessario, è inoltre possibile creare esenzioni aggiuntive.	
8.	Abilitare l'attuazione DHCP.	
<b>Operazioni del server DHCP, parte 2</b>		
9.	Le classi utente non sono necessarie per l'attuazione DHCP in NAC versione 3.5. Una volta eseguiti upgrade, abilitazione e verifica dell'attuazione DHCP, Sophos consiglia quindi di cancellare le classi utente da ciascun server DHCP, le quali erano state create per la versione precedente del software, che è ormai obsoleta.	

## 7.2 Disabilitazione dell'attuazione DHCP per computer noti

Per disabilitare l'attuazione DHCP è necessario cambiare la modalità del criterio ("Policy Mode") da "Enforce" a "Report Only", nei rispettivi criteri. Utilizzare questa funzione quando si effettua l'upgrade dell'attuazione DHCP.

**Importante:** tutti i criteri e le modifiche agli stessi hanno effetto immediato, ma un criterio non viene applicato finché l'agente non lo recupera.

**Nota:** se si utilizza l'attuazione dell'agente invece dell'attuazione DHCP per i computer noti, non è richiesta tale operazione.

### Procedura

1. Accedere a NAC Manager.

2. Cliccare su **Manage > Policies** . Quindi, cliccare sul nome del criterio che si desidera aggiornare.
3. Cliccare sull'elenco **Policy Mode** e selezionare **Report Only**.
  - **Report Only:** la modalità di criterio Report Only indica che i computer sono valutati in base al criterio assegnato e, all'interno di NAC Manager, viene generato un report informativo. Non viene visualizzato alcun messaggio e non viene intrapresa alcuna azione correttiva o di attuazione. la modalità Report Only utilizza il modello di accesso "DHCP - Full Access", per consentire l'accesso alla rete ai computer noti.
4. Cliccare su **Save**.

### 7.3 Disinstallazione del software DHCP Enforcer

Disinstallare il software DHCP Enforcer da tutti i server Microsoft DHCP. Il software DHCP Enforcer include DHCP Enforcer e l'utilità di configurazione di DHCP Enforcer.

1. Dal menu Start, selezionare **Pannello di controllo > Installazione applicazioni** .
2. Selezionare il software **Sophos DHCP Enforcer** e poi cliccare su Rimuovi.
3. Per confermare la rimozione del software DHCP Enforcer, cliccare su **Sì**.

### 7.4 Installazione del software DHCP Enforcer

Installare il software DHCP Enforcer in tutti i server Microsoft DHCP. Il software DHCP Enforcer include DHCP Enforcer e l'utilità di configurazione di DHCP Enforcer. Durante l'installazione viene configurato il server DHCP. Se si desidera modificare le impostazioni del server DHCP specificate durante l'installazione di DHCP Enforcer, utilizzare l'utilità di configurazione di DHCP Enforcer. Per ulteriori informazioni, consultare la sezione [Appendice C: Utilizzo dell'utilità di configurazione di DHCP Enforcer](#) a pagina 40.

1. Andare al sito web di Sophos, scaricare il programma di installazione di Sophos NAC per DHCP Enforcer ed eseguirlo.

In alternativa, inserire il CD Sophos per l'installazione di DHCP Enforcer. Il CD si avvia automaticamente.
2. Viene avviata la procedura guidata di installazione. Nella finestra di dialogo **Benvenuti nella procedura guidata per la protezione dei computer**, cliccare su **Avanti**.
3. Nella finestra di dialogo **Sophos DHCP Enforcer**, inserire l'indirizzo IP del Server NAC, la chiave condivisa del Server NAC e la conferma della chiave condivisa. Cliccare su **Avanti**.

Memorizzare la chiave condivisa inserita. La chiave condivisa viene utilizzata per proteggere il traffico tra Server NAC e il server DHCP. Quando si esegue la procedura guidata di configurazione di DHCP tramite NAC Manager, si deve utilizzare la medesima chiave condivisa. Una volta identificato un server DHCP in NAC Manager, è possibile aggiornarne la chiave condivisa nell'area **Configure System > Server Settings** .
4. Nella finestra di dialogo **Pronta per l'installazione del programma**, cliccare su **Installa** per installare DHCP Enforcer.

5. Cliccare su **Fine**.

**Nota:** dopo aver installato il software DHCP Enforcer, è necessario verificare che DHCP Enforcer sia in esecuzione su ciascun server DHCP.

## 7.5 Completamento delle operazioni di NAC Manager

Una volta terminata l'installazione di DHCP Enforcer in tutti i server DHCP, utilizzare NAC Manager per configurare tali server in modo che possano operare congiuntamente a Sophos NAC. L'attuazione DHCP, eseguita tramite NAC Manager, richiede una configurazione minima. Per impostazione predefinita, l'attuazione DHCP è in modalità Report Only. È necessario abilitare l'attuazione.

- **Computer sconosciuti** non sono gestiti da Sophos Enterprise Console, non dispongono del Compliance Agent installato, non sono esenti e non hanno eseguito il Dissolvable Agent.
- **Computer noti** sono gestiti da Sophos Enterprise Console e hanno il Compliance Agent installato e operativo.

**Nota:** è necessario creare esenzioni per i computer che non possono eseguire il Compliance Agent, quali ad esempio computer con sistemi operativi non Windows. Le esenzioni vengono inoltre applicate ai computer che non richiedono la verifica della conformità, quali server, router e stampanti. I computer a cui è assegnato un indirizzo IP in modo dinamico tramite DHCP sono i soli computer a poter essere esentati.

Le operazioni di NAC Manager comprendono:

1. L'utilizzo della procedura guidata di configurazione di DHCP per eseguire la configurazione di proxy, delle azioni correttive, del Dissolvable Agent e dei server DHCP che si desidera utilizzare con l'attuazione DHCP di Sophos NAC.
2. L'utilizzo del report DHCP Enforcer di NAC Manager per stabilire se i computer riceveranno l'accesso alla rete adeguato una volta abilitata l'attuazione DHCP, e l'identificazione dei computer che richiedono esenzioni.
3. La creazione di esenzioni per i computer che non possono eseguire il Compliance Agent o che non richiedono la verifica della conformità.
4. L'abilitazione dell'attuazione DHCP.

### 7.5.1 Esecuzione della procedura guidata di configurazione di DHCP

La Procedura guidata di configurazione di DHCP aiuta ad identificare i server proxy, di correzione, del Dissolvable Agent e DHCP da utilizzare con le implementazioni di Sophos NAC e per configurare automaticamente i modelli di accesso predefiniti di DHCP in base alle definizioni del proprio server.

#### Procedura

1. Accedere a NAC Manager.
2. Cliccare su **Enforce > DHCP Configuration Wizard** . Cliccare su **Avanti** per continuare.

3. Effettuare una delle seguenti operazioni:

- Se si utilizzano server proxy, cliccare su **Yes** e poi su **Next**. Passare al punto seguente.
- Se **non** si eseguono server proxy, cliccare su **No** e poi su **Next**. Passare al punto 5.

**Importante:** Se non viene definito un server proxy per l'accesso a internet, gli utenti non avranno accesso a internet, e il modello di accesso predefinito DHCP - Internet Access DHCP Enforcer fornirà esclusivamente accesso per azioni correttive.

4. Definire i server proxy necessari per consentire l'accesso a Internet e poi cliccare su **Next**. Eseguire una delle seguenti procedure.

- Deselezionare la casella accanto ai server che **non** si desidera includere come server proxy.
- Cliccare su **Add** per aggiungere nuovi server, inserire i dati relativi al server proxy e cliccare su **OK**. Ripetere eventualmente questo passaggio per aggiungere altri server. Una volta creati, questi server possono essere gestiti dalla pagina **Enforce > Network Resources** .

**Nota:** i server proxy selezionati sostituiranno tutti i server che si trovano correntemente nel modello di accesso predefinito di DHCP - Internet Access DHCP Enforcer.

5. Definire i server di correzione necessari per apportare correzioni all'accesso, quali controller di dominio, e successivamente cliccare su **Next**.

Eseguire una delle seguenti procedure.

- Deselezionare la casella accanto ai server che **non** si desidera includere come server di correzione.
- Cliccare su **Add** per aggiungere nuovi server, inserire i dati relativi al server di correzione e cliccare su **OK**. Ripetere eventualmente questo passaggio per aggiungere altri server. Una volta creati, questi server possono essere gestiti dalla pagina **Enforce > Network Resources** .

**Nota:** i server di correzione selezionati sostituiranno tutti i server che si trovano correntemente nel modello di accesso predefinito di DHCP - Remediation Access DHCP Enforcer.

6. Effettuare una delle seguenti operazioni:

- Se il Dissolvable Agent è installato, cliccare su **Yes** e successivamente su **Next**. Passare al punto seguente.
- Se il Dissolvable Agent **non** è installato, cliccare su **No** e successivamente su **Next**. Passare al punto 8.

**Nota:** se il Dissolvable Agent è stato installato nello stesso server di Sophos NAC, non è necessario creare un server del Dissolvable Agent aggiuntivo.

7. Definire i server che ospitano il Dissolvable Agent in modo tale che DHCP Enforcer ne possa consentire l'accesso. Questo tipo di accesso è necessario per poter consentire ai computer sconosciuti, quali i computer ospiti, di venire riconosciuti all'interno della rete. Cliccare su **Add** per aggiungere nuovi server, inserire i dati relativi al server del Dissolvable Agent e cliccare su **OK**. Quindi cliccare su **Next**. Una volta creati, questi server possono essere gestiti dalla pagina **Configure System > Server Settings** .

8. Definire i server che verranno utilizzati per l'attuazione DHCP. Cliccare su **Add** per aggiungere nuovi server, inserire i dati relativi al server di DHCP Enforcer e cliccare su **OK**. Ripetere eventualmente questo passaggio per aggiungere altri server. Quindi cliccare su **Next**. Una volta creati, questi server possono essere gestiti dalla pagina **Configure System > Server Settings**.

**Nota:** la chiave condivisa deve corrispondere a quanto inserito durante l'installazione di DHCP Enforcer nel server. La chiave condivisa viene utilizzata per proteggere il traffico tra Server NAC e il server DHCP.

9. Cliccare su **Fine**.

## 7.5.2 Esecuzione del report DHCP Enforcer

Prima di abilitare l'attuazione DHCP, eseguire il report DHCP Enforcer di Sophos NAC per determinare lo stato di conformità dei computer. I criteri predefiniti di NAC sono impostati su Report Only. Il report DHCP Enforcer è utilizzabile per stabilire se, una volta abilitata l'attuazione, verranno applicati i modelli di accesso corretti. Dal report DHCP Enforcer è possibile rendere esenti i dispositivi e accedere ai dati di rilevamento.

### Procedura

1. Accedere a NAC Manager.
2. Cliccare su **Report > Troubleshooting**.
3. Cliccare sull'elenco **Report Type** e selezionare **DHCP Enforcer**.
4. Se pertinente, cliccare sul **segno più** accanto a **Report Criteria** e digitare o selezionare le opzioni di ricerca appropriate. È anche possibile cliccare sul link **Custom Sort** per ampliare le opzioni di ordinamento; le opzioni di ordinamento personalizzato vengono modificate temporaneamente durante l'esecuzione del report.

**Nota:** è possibile utilizzare, nella maggior parte dei campi, il simbolo \* o % per eseguire una ricerca con caratteri jolly. Per esempio, se si digita M% nel campo Returned User Class, vengono visualizzate tutte le classi di utenti che iniziano con la lettera M. Se invece si specifica M senza il carattere %, verranno visualizzate solo le classi di utenti con il nome M.

5. Cliccare su **Run**.

### Campi e descrizioni

Campo	Descrizione
<b>Voce del report riepilogativo</b>	
Date/Time	Data e ora del tentativo di accesso alla rete. <b>Nota:</b> la data e l'ora vengono ricavate dal fuso orario del browser web che accede a NAC Manager.

Campo	Descrizione
MAC Address	Indirizzo MAC del dispositivo che sta tentando di connettersi alla rete. L'indirizzo MAC elencato è assegnato al NIC associato alla richiesta del client DHCP.
Computer Name	Nome del dispositivo che sta tentando di connettersi alla rete. Nome del computer ricavato dalla richiesta del client.
Compliance State	Stato di conformità di un computer, assegnato durante la verifica della conformità. Gli stati di conformità disponibili sono Compliant, Partially Compliant e Non-Compliant. Un trattino triplo (---) indica che l'agente non ha registrato alcuno stato di conformità. L'accesso alla rete è determinato dai modelli di accesso di DHCP Enforcer conformi, associati allo stato di conformità del criterio.
Template Name (Version)	<p>Nome e versione del modello di accesso che determina l'azione intrapresa dall'Agent Enforcer. Il modello di accesso utilizzato si basa sul motivo. I modelli di accesso disponibili includono i seguenti modelli predefiniti, oltre che i modelli personalizzati:</p> <ul style="list-style-type: none"> <li>■ <b>DHCP - Full Access:</b> consente pieno accesso alla rete.</li> <li>■ <b>DHCP - Internet Access:</b> consente accesso a Internet, e nega l'accesso agli indirizzi IP privati e alla rete di area locale (LAN).</li> </ul> <p><b>Importante:</b> Se non viene definito un server proxy per l'accesso a internet come risorsa di rete, gli utenti non avranno accesso a internet, e questo modello fornirà esclusivamente accesso per azioni correttive.</p> <ul style="list-style-type: none"> <li>■ <b>DHCP - Remediation Access:</b> nega qualsiasi accesso alla rete, eccezion fatta per i server di correzione specificati, i Sophos Server NAC, e il server del Dissolvable Agent.</li> </ul>
Reason	<p>Motivo per cui un particolare modello di accesso è stato assegnato da DHCP Enforcer. Motivi disponibili:</p> <ul style="list-style-type: none"> <li>■ <b>Assessment:</b> la verifica eseguita dall'agente ha determinato lo stato di conformità. L'accesso alla rete è determinato dai modelli di accesso di DHCP Enforcer conformi, associati allo stato di conformità del criterio. Viene visualizzato un collegamento che dà accesso ai dati della verifica di conformità associata a questa voce di DHCP Enforcer.</li> <li>■ <b>Default Template:</b> il computer può avere un criterio associato oppure essere un'esenzione designata, ma non è stato trovato un modello di accesso associato. L'accesso alla rete è determinato dai modelli di accesso predefiniti designati nell'area <b>Configure System &gt; Enforcer Settings</b> .</li> <li>■ <b>Enforcer Override:</b> l'attuazione non è stata verificata. Se la casella Override DHCP Enforcer nell'area <b>Configure System &gt; Enforcer Settings</b> è spuntata, l'accesso alla rete è determinato dai modelli di accesso Maintenance Mode/Enforcer Override, designati nella medesima area.</li> <li>■ <b>Exempted:</b> il computer è esentato in base ai criteri di esenzione definiti nell'area <b>Enforce &gt; Exemptions</b> . L'accesso alla rete è determinato dai</li> </ul>

Campo	Descrizione
	<p>modelli di accesso associati al criterio di esenzione. I seguenti sottomotivi di Exempted sono visualizzati fra parentesi:</p> <ul style="list-style-type: none"> <li>■ <b>User Class:</b> la classe dell'utente specificata come esenzione.</li> <li>■ <b>Vendor Class:</b> la classe del fornitore specificata come esenzione.</li> <li>■ <b>MAC:</b> l'indirizzo MAC specificato come esenzione.</li> <li>■ <b>IP Scope:</b> l'ambito IP specificato come esenzione.</li> </ul> <ul style="list-style-type: none"> <li>■ <b>Maintenance Mode:</b> il software è in modalità manutenzione. L'accesso alla rete è determinato dai modelli di accesso Maintenance Mode/Enforcer Override designati nell'area <b>Configure System &gt; Enforcer Settings</b> .</li> <li>■ <b>Policy Retrieval Error:</b> lo stato di conformità del computer è obsoleto secondo il campo DHCP Policy Update Threshold configurato nell'area <b>Configure System &gt; Enforcer Settings</b> . L'accesso alla rete è determinato dai modelli di accesso di DHCP Enforcer del criterio e associati allo stato Policy Retrieval Error.</li> <li>■ <b>Remediate:</b> il criterio è in modalità Remediate. L'accesso alla rete è determinato dai modelli di accesso di DHCP Enforcer associati alla modalità Remediate del criterio.</li> <li>■ <b>Report Only:</b> il criterio è in modalità Report Only. L'accesso alla rete è determinato dai modelli di accesso di DHCP Enforcer associati alla modalità Report Only del criterio.</li> <li>■ <b>Reserved:</b> l'indirizzo MAC del dispositivo che richiede accesso alla rete è riservato come dispositivo speciale nel server DHCP.</li> <li>■ <b>System Error:</b> Enforcer ha riscontrato un errore che ha impedito il completamento dell'operazione. L'impostazione del registro SystemErrors del Server NAC nega l'accesso alla rete per impostazione predefinita.</li> <li>■ <b>Template Error:</b> non è stato rilevato alcun modello associato e i modelli di accesso predefiniti designati nell'area <b>Configure System &gt; Enforcer Settings</b> non possono essere utilizzati. Se si riceve questo errore, l'accesso alla rete è determinato dal server DHCP, che non restituirà una classe di utenti e negherà accesso all'utente.</li> <li>■ <b>Unknown Endpoint:</b> non esiste alcun dato relativo alla conformità. L'accesso alla rete è determinato dai modelli di accesso Unknown Endpoint designati nell'area <b>Configure System &gt; Enforcer Settings</b> .</li> </ul>
Returned User Class	Classe dell'utente DHCP restituita al server DHCP dal DHCP Enforcer per l'attuazione.
DHCP Server	Indirizzo IP del server DHCP che ha richiesto l'accesso alla rete da DHCP Enforcer. Si tratta del server DHCP nel quale DHCP Enforcer è installato.
<b>Voce del report nel dettaglio</b>	
Agent Enforcement Action	Azione intrapresa dal computer riguardo l'assegnazione dell'indirizzo IP. Il computer inizia il rilascio e rinnovo degli indirizzi IP in base all'azione

Campo	Descrizione
	<p>dell'Agent Enforcement specificata nel criterio. L'agente ottiene indirizzi IP nuovi: quando si avvia e inizia la verifica della conformità, quando lo stato di conformità del computer cambia, quando la modalità del criterio cambia, quando i modelli di accesso di DHCP Enforcer definiti nel criterio del computer cambiano. Valori disponibili:</p> <ul style="list-style-type: none"> <li>■ <b>None:</b> gli indirizzi IP per il computer non sono né rilasciati né rinnovati.</li> <li>■ <b>Release Renew:</b> gli indirizzi IP per il computer vengono rilasciati e poi rinnovati utilizzando il server DHCP. Gli indirizzi IP correnti vengono abbandonati prima di ottenere quelli nuovi.</li> <li>■ <b>Triple Dash (---):</b> l'agente non ha registrato alcuna azione.</li> </ul>
Vendor Class	Classe del produttore del client DHCP.
DHCP Relay	Indirizzo IP del relay DHCP (se presente nella richiesta DHCP originale) utilizzato da DHCP Enforcer per selezionare un modello di accesso di DHCP Enforcer. Se non si utilizza un relay DHCP viene visualizzato 0.0.0.0.
Transaction ID	Identificativo della transazione che viene restituito dal server DHCP. L'identificativo della transazione associa i messaggi del client DHCP con le risposte del server.

### 7.5.3 Creazione delle esenzioni DHCP

I computer esentati non possono eseguire il Compliance Agent; si tratta per esempio di computer con sistemi operativi non Windows. Le esenzioni vengono inoltre applicate ai computer che non richiedono la verifica della conformità, quali server, router e stampanti. I computer a cui è assegnato un indirizzo IP in modo dinamico tramite DHCP sono i soli computer a poter essere esentati. Per tali computer è necessario creare delle esenzioni DHCP; in caso contrario, una volta abilitata l'attuazione DHCP, sarà loro negato l'accesso alla rete.

Tramite NAC Manager si possono creare due tipi di esenzioni DHCP:

- **Esenzioni per criteri DHCP:** esenzioni create in base a indirizzo MAC, classe dell'utente e del produttore del software
- **Esenzioni per ambito IP:** esenzioni create per segmenti di rete.

#### 7.5.3.1 Creazione di esenzioni per i criteri DHCP

Utilizzare la pagina Exemptions di NAC Manager per creare le esenzioni per i criteri DHCP. Per individuare le esenzioni e designare le azioni, vengono utilizzati congiuntamente i criteri di esenzione e i modelli di accesso di DHCP Enforcer. Una volta soddisfatto il criterio di esenzione definito, il modello di accesso di DHCP Enforcer associato determina l'azione di accesso alla rete più appropriata da intraprendere.

#### Procedura

1. Accedere a NAC Manager.

2. Cliccare su **Enforce > Exemptions** . Quindi, cliccare su **Create Exemption** nella pagina in basso a sinistra.
3. Digitare un nome e una descrizione per l'esenzione.
4. Cliccare sull'elenco **Exemption Type** e selezionare **DHCP Criteria**.
5. In Exemption Criteria, per indicare quale criterio di esenzione si desidera definire: cliccare sul pulsante di opzione **MAC Address**, **User Class** o **Vendor Class**, nel relativo campo digitare l'appropriato indirizzo MAC (o prefisso), classe dell'utente o classe del fornitore e infine cliccare su **Add**.

Ripetere eventualmente questo passaggio per aggiungere altri criteri di esenzione.

**Nota:** per specificare le esenzioni si può utilizzare il carattere \* , purché sia l'ultimo del nome. Per esempio, se si specifica AA\* come indirizzo MAC, verranno esentati tutti gli indirizzi MAC che iniziano con AA. Se si specifica un indirizzo MAC senza il simbolo \* , è necessario indicare l'esatto indirizzo MAC che si desidera esentare.

6. Cliccare su **Select** per aggiungere all'esenzione modelli di accesso di DHCP Enforcer, selezionare il modello di accesso **DHCP - Full Access** e cliccare su **OK**.

In Sophos NAC, il modello di accesso **DHCP - Full Access** è predefinito in modo tale da consentire accesso alla rete. Questa esenzione è così configurata per consentire l'accesso alla rete senza alcuna verifica della conformità da parte di Sophos NAC.

7. Cliccare su **Save**.

### 7.5.3.2 Creazione delle esenzioni per ambito IP

I computer a cui è assegnato un indirizzo IP in modo dinamico tramite DHCP sono i soli computer a poter essere esentati. Utilizzare la pagina Exemptions di NAC Manager per creare le esenzioni per ambito IP. Le esenzioni per ambito IP sono esenzioni create per segmenti di rete. Le esenzioni per ambito IP sono utili per implementare l'attuazione in fasi in tutta l'azienda; è possibile esentare dei segmenti di rete che non si desidera ancora sottoporre all'attuazione dei criteri di sicurezza.

#### Procedura

1. Accedere a NAC Manager.
2. Cliccare su **Enforce > Exemptions** . Quindi, cliccare su **Create Exemption** nella pagina in basso a sinistra.
3. Digitare un nome e una descrizione per l'esenzione.
4. Cliccare sull'elenco **Exemption Type** e selezionare **IP Scope**.
5. Sotto Exempted IP Scopes, cliccare su **Select** per aggiungere uno scope IP all'esenzione, selezionare gli scope appropriati e cliccare su **OK**.

Se non si trova lo scope IP che si sta cercando, è possibile crearlo. Per far ciò è necessario creare un nuovo modello di accesso di DHCP Enforcer o aggiornare uno di quelli predefiniti.

6. Eventualmente, utilizzare le frecce per determinare la priorità degli intervalli.

Se a una particolare esenzione è applicato più di uno scope IP, viene utilizzato il primo di essi. Sophos consiglia di dare maggiore priorità agli scope IP più specifici e di dare minore priorità a quelli meno specifici.

7. Cliccare su **Save**.

**Importante:** una volta create le esenzioni, è possibile ordinarle per priorità nella pagina **Exemptions**. Se a un particolare computer è applicata più di una esenzione, viene utilizzata la prima di esse. Sophos consiglia di dare maggiore priorità alle esenzioni più specifiche e di dare minore priorità a quelle meno specifiche.

## 7.5.4 Abilitazione dell'attuazione DHCP

È possibile abilitare l'attuazione DHCP sia per computer sconosciuti che noti. Sophos consiglia di utilizzare l'attuazione DHCP per i computer sconosciuti e quella dell'agente per i computer noti. Sophos NAC consente comunque l'utilizzo dell'attuazione DHCP anche per i computer noti.

### 7.5.4.1 Abilitazione dell'attuazione DHCP per computer sconosciuti

È possibile abilitare l'attuazione DHCP per computer sconosciuti su tutti i server DHCP. Ciò consente di specificare quali server DHCP metteranno in quarantena i computer sconosciuti. Utilizzare questa funzione per svolgere l'attuazione DHCP in fasi.

Prima di abilitare l'attuazione DHCP per computer autonomi, è necessario creare le esenzioni. I computer a cui è assegnato un indirizzo IP in modo dinamico tramite DHCP sono i soli computer a poter essere esentati.

#### Procedura

1. Accedere a NAC Manager.
2. Cliccare su **Configure System > Server Settings**.
3. Cliccare sul nome del server DHCP per cui si desidera abilitare l'attuazione DHCP.
4. Cliccare sull'elenco **Unknown Endpoint Mode** e selezionare **Enforce**. La modalità Enforce utilizza il modello di accesso "DHCP - Internet Access" per mettere in quarantena i computer sconosciuti e consentire l'accesso a internet o a server di correzione.

**Nota:** se si è specificato un server proxy durante l'esecuzione della procedura guidata di configurazione di DHCP, i computer possono accedere a internet. Se invece non è stato specificato un server proxy, i computer possono accedere ai server di correzione precedentemente indicati durante la procedura guidata di configurazione di DHCP. È possibile cambiare il modello di accesso nell'area **Configure System > Enforcer Settings**.

5. Cliccare su **Save**.

### 7.5.4.2 Abilitazione dell'attuazione DHCP per computer noti

È possibile abilitare l'attuazione DHCP per i computer noti nei criteri. Se per i computer noti si intende utilizzare l'attuazione DHCP o dell'agente, è necessario cambiare, nei relativi criteri, la modalità del criterio (Policy Mode) da Report Only a Enforce.

**Importante:** tutti i criteri e le modifiche agli stessi hanno effetto immediato, ma un criterio non viene applicato finché l'agente non lo recupera.

#### Procedura

1. Accedere a NAC Manager.

2. Cliccare su **Manage > Policies** . Quindi, cliccare sul nome del criterio che si desidera aggiornare.
3. Cliccare sull'elenco **Policy Mode** e selezionare **Enforce**.
  - **Enforce:** la modalità del criterio Enforce indica che i computer sono valutati in base al criterio assegnato e che all'interno di NAC Manager viene generato un report informativo. I messaggi vengono visualizzati e vengono intraprese azioni correttive e di attuazione tramite i modelli di accesso relativi agli adeguati stati di accesso. La modalità Enforce utilizza i modelli di accesso assegnati al punto 5.
4. Cliccare sull'elenco **Agent Enforcement Action** e selezionare **Release Renew**. È **necessario** selezionare Release Renew quando si utilizza l'attuazione DHCP per computer noti.
5. Nell'area di navigazione Network Access a sinistra, cliccare su **DHCP**. Cliccare sulla scheda **Enforce** e verificare le assegnazioni dei modelli di accesso.

**Nota:** Per impostazione predefinita, ogni criterio viene automaticamente popolato con i modelli di accesso. Assicurarsi che siano applicati i modelli di accesso corretti. Conservare le assegnazioni dei modelli di accesso Report Only e Remediate.

#### Assegnazione dei modelli di DHCP Enforcer predefiniti

- **Policy Retrieval Error:** lo stato di conformità del computer è obsoleto secondo il campo DHCP Policy Update Threshold configurato nell'area **Configure System > Enforcer Settings** . Il modello di accesso DHCP - Remediation Access nega l'accesso alla rete, eccezion fatta per i server di correzione specificati durante l'esecuzione della procedura guidata di configurazione di DHCP.
  - **Compliant:** il computer è conforme. Il modello di accesso DHCP - Full Access consente l'accesso alla rete quando il computer è conforme.
  - **Partially Compliant:** il computer è parzialmente conforme. Il modello di accesso DHCP - Full Access consente l'accesso alla rete quando il computer è parzialmente conforme.
  - **Non-Compliant:** il computer non è conforme. Il modello di accesso DHCP - Remediation Access nega l'accesso alla rete, eccezion fatta per i server di correzione specificati durante l'esecuzione della procedura guidata di configurazione di DHCP.
6. Eventualmente, utilizzare le frecce per ordinare i modelli di accesso di DHCP Enforcer in base alla priorità.
 

Se più di un modello è applicabile a un particolare stato, viene utilizzato il primo modello che soddisfa tale stato. Sophos consiglia di dare maggiore priorità ai modelli di accesso più specifici/rigidi e di dare minore priorità a quelli meno specifici/rigidi.
  7. Cliccare su **Save**.

#### 7.5.4.2.1 Utilizzo dei criteri predefiniti

È possibile utilizzare i criteri predefiniti per supportare la conformità ai criteri di protezione per computer gestiti e non.

- **Default:** questo criterio viene utilizzato se in un computer è installato il Compliance Agent, ma non gli è stato attribuito alcun criterio. Per impostazione predefinita, il criterio è in modalità Report Only. Se il criterio è impostato su Remediate o Enforce, tale criterio svolgerà azioni correttive sul computer.

- **Managed:** questo criterio può essere utilizzato per i computer che sono gestiti da Sophos Enterprise Console e che hanno il Compliance Agent installato. Per impostazione predefinita, il criterio è in modalità Report Only. Se il criterio è impostato su Remediate o Enforce, tale criterio svolgerà azioni correttive sul computer.
- **Unmanaged:** questo criterio può essere utilizzato per i computer esterni all'azienda. Non svolge attività correttive nel computer. Il Dissolvable Agent utilizza il criterio Unmanaged.

**Nota:** se il computer non ha un Compliance Agent installato e non utilizza il Dissolvable Agent, l'accesso alla rete sarà determinato dalle impostazioni di Enforcer.

### 7.5.4.3 Esperienza dell'utente relativa all'attuazione DHCP

Una volta abilitata l'attuazione DHCP, l'utente può trovarsi in situazioni diverse a seconda che il computer sia sconosciuto o noto. Gli ospiti possono anche eseguire il Compliance Dissolvable Agent per ottenere accesso alla rete.

- **Computer sconosciuti** non sono gestiti dal Compliance Agent, non dispongono del Compliance Agent installato, non sono esenti e non hanno eseguito il Dissolvable Agent.
- **Computer ospiti** possono eseguire il Compliance Dissolvable Agent per il controllo dell'accesso alla rete.
- **Computer noti** sono gestiti da Sophos Enterprise Console e hanno il Compliance Agent installato e operativo.

#### Esperienza dell'utente relativa all'attuazione DHCP in computer sconosciuti

Quando l'attuazione DHCP è abilitata, i computer sconosciuti si troveranno nella seguente situazione:

1. Il computer viene avviato.
2. Quando l'attuazione DHCP per computer sconosciuti è abilitata, tali computer ricevono accesso limitato alla rete. È loro permesso di accedere a internet o a server di correzione. Se si è specificato un server proxy durante l'esecuzione della procedura guidata di configurazione di DHCP, i computer possono accedere a internet. Se invece non è stato specificato un server proxy, i computer possono accedere ai server di correzione precedentemente indicati durante la procedura guidata di configurazione di DHCP.

#### Esperienza dell'utente relativa all'attuazione DHCP in computer ospiti

Quando l'attuazione DHCP è abilitata e ai computer ospiti è richiesto di utilizzare il Compliance Dissolvable Agent, gli utenti ospiti si troveranno nella seguente situazione:

1. Il computer viene avviato.
2. L'utente apre Internet Explorer, inserisce l'URL del Compliance Dissolvable Agent ed esegue il Compliance Dissolvable Agent.
3. Il Compliance Dissolvable Agent conduce una verifica e stabilisce se il computer è conforme, parzialmente conforme o non conforme al criterio di NAC.
4. Quando l'attuazione DHCP è configurata e abilitata, si verifica quanto riportato di seguito:
  - I computer conformi possono accedere alla rete.
  - I computer parzialmente conformi possono accedere alla rete. Il Compliance Dissolvable Agent visualizza messaggi agli utenti in modo tale che possano apportare azioni correttive

sui loro computer e renderli conformi. Se il criterio di NAC è configurato in modo tale da apportare automaticamente azioni correttive sul computer, vengono svolte tali azioni. Per impostazione predefinita, l'azione correttiva è disabilitata. Nella maggior parte dei casi, non si desidera apportare azioni correttive su computer ospiti.

- I computer non conformi non possono accedere alla rete. È loro permesso di accedere a internet o a server di correzione. Se si è specificato un server proxy durante l'esecuzione della procedura guidata di configurazione di DHCP, i computer possono accedere a internet. Se invece non è stato specificato un server proxy, i computer possono accedere ai server di correzione precedentemente indicati durante la procedura guidata di configurazione di DHCP. Il Compliance Dissolvable Agent visualizza messaggi agli utenti in modo tale che possano apportare azioni correttive sui loro computer e renderli conformi. Se il criterio di NAC è configurato in modo tale da apportare automaticamente azioni correttive sul computer, vengono svolte tali azioni. Per impostazione predefinita, l'azione correttiva è disabilitata. Nella maggior parte dei casi, è meglio non apportare azioni correttive su computer ospiti.

### **Esperienza dell'attuazione DHCP per computer noti**

Quando l'attuazione DHCP è abilitata, i computer noti si troveranno nella seguente situazione concernente DHCP:

1. Il computer viene avviato ed esegue il Compliance Agent.
2. Il Compliance Agent conduce una verifica e stabilisce se il computer è conforme, parzialmente conforme o non conforme al criterio di NAC.
3. Quando l'attuazione DHCP è configurata e abilitata, si verifica quanto riportato di seguito:
  - I computer conformi possono accedere alla rete.
  - I computer parzialmente conformi possono accedere alla rete. Il Compliance Agent visualizza messaggi agli utenti in modo tale che possano apportare azioni correttive sui loro computer e renderli conformi. Se il criterio di NAC è configurato in modo tale da apportare automaticamente azioni correttive sul computer, vengono svolte tali azioni.
  - I computer non conformi non possono accedere alla rete. Possono accedere ai server di correzione specificati durante l'esecuzione della procedura guidata di configurazione di DHCP. Il Compliance Agent visualizza messaggi agli utenti in modo tale che possano apportare azioni correttive sui loro computer e renderli conformi. Se il criterio di NAC è configurato in modo tale da apportare automaticamente azioni correttive sul computer, vengono svolte tali azioni.

## 8 Appendice C: Utilizzo dell'utilità di configurazione di DHCP Enforcer

Se si desidera modificare le impostazioni di DHCP Enforcer specificate durante la sua installazione, utilizzare l'utilità di configurazione di DHCP Enforcer. L'installazione di DHCP Enforcer installa tale utilità nel server DHCP. Se si è in possesso di più di un server DHCP, è necessario modificare le impostazioni di DHCP Enforcer in ciascun server DHCP.

### 8.1 Aggiornamento della chiave condivisa

#### Procedura

La chiave condivisa deve corrispondere a quanto inserito durante l'installazione di DHCP Enforcer nel server. La chiave condivisa viene utilizzata per proteggere il traffico tra Server NAC e il server DHCP.

1. Dal menu Start del server DHCP, selezionare **Sophos > NAC > Support Tools > DHCP Enforcer Configuration Utility**.

La finestra di dialogo **DHCP Enforcer Configuration Utility** viene visualizzata con la scheda **Enforcer** selezionata.

2. Nella finestra di dialogo **DHCP Enforcer Configuration Utility** cliccare su **Edit**.
3. Nella finestra di dialogo **DHCP Enforcer RADIUS Enforcer Server Settings**, inserire e confermare la nuova chiave condivisa, cliccare poi su **OK**.

### 8.2 Aggiornamento delle impostazioni avanzate

Questa sezione descrive come eseguire l'aggiornamento delle impostazioni avanzate di DHCP Enforcer tramite l'utilità di DHCP Enforcer. Nella maggior parte dei casi, queste impostazioni non richiedono aggiornamento.

#### Procedura

1. Dal menu **Start** del server DHCP, selezionare **Sophos > NAC > Support Tools > DHCP Enforcer Configuration Utility**.

La finestra di dialogo **DHCP Enforcer Configuration Utility** viene visualizzata con la scheda **Enforcer** selezionata.

2. Nella finestra di dialogo **DHCP Enforcer Configuration Utility**, cliccare sulla scheda **Advanced**.
3. Cambiare le impostazioni di DHCP Enforcer a seconda delle proprie esigenze.
4. Cliccare su **OK**.

Ripetere queste istruzioni per tutti i server DHCP necessari.

## 8.2.1 Campi e descrizioni dell'utilità di configurazione di DHCP

Campi	Descrizioni
<b>Scheda Enforcer</b>	
Access for Multiple Servers	Questo pulsante di opzione non è applicabile a Sophos Endpoint Security and Control.
<b>Finestra di dialogo DHCP Enforcer RADIUS Enforcer Server Settings</b> Cliccare sull'icona <b>Edit</b> per poter accedere a questa finestra di dialogo. <b>Nota:</b> i campi di questa finestra di dialogo si riferiscono al NAC Server.	
Enable	Indica se il Server NAC è abilitato. Quando abilitato, il Server NAC viene utilizzato per la conformità al criterio e l'attività di reportistica.
IP Address	Indica l'indirizzo IP del Server NAC.
Authentication Port	Indica la porta di autenticazione del Server NAC.
Accounting Port	Indica la porta di accounting del Server NAC.
Shared Key	Identifica la chiave condivisa del server DHCP. La chiave condivisa è la medesima chiave utilizzata durante l'installazione di DHCP Enforcer.
Confirm Shared Key	Conferma la chiave condivisa del server DHCP.
<b>Finestra di dialogo DHCP Enforcer Resolve IP</b>	
Hostname	Quando l'indirizzo IP è sconosciuto, indica il nome host del Server NAC. Quando si inserisce il nome host, è possibile risolvere il nome host in un indirizzo IP.
<b>Scheda Advanced</b>	
Enable Policy Compliance	Quando è selezionata questa opzione, la conformità al criterio e la reportistica per tutti i pacchetti di richiesta DHCP sono abilitate, eccezion fatta per quelli identificati da un codice di opzione riservato.
Attempts	Stabilisce quante volte debba essere iniziata la conformità al criterio per un pacchetto di richiesta DHCP.
Timeout	Stabilisce, in secondi, il tempo di attesa del server DHCP prima di un'altra verifica della conformità al criterio.
Default User Class	Identifica la classe dell'utente da utilizzare nel caso in cui quella definita nel criterio non possa essere ottenuta a causa di un errore durante la verifica della conformità.
Error	Quando selezionato, consente di salvare nel log eventi dell'applicazione i messaggi di errore di Microsoft.

Campi	Descrizioni
Warning	Quando selezionato, consente di salvare nel log eventi dell'applicazione i messaggi di avviso di Microsoft.
Information	Quando selezionato, consente di salvare nel log eventi dell'applicazione i messaggi informativi di Microsoft.
Trace	Quando selezionato, consente di salvare nel log eventi dell'applicazione il log trace di Microsoft.
Subnet Mask Override	Indica la maschera di sottorete a disposizione degli utenti non conformi al criterio; questo campo consente di ignorare la sottorete nel server DHCP al fine di limitare l'accesso alla rete.
Black Hole IP Address	Questo indirizzo IP fittizio viene utilizzato da DHCP Enforcer per scartare/ignorare il traffico delle risorse bloccate.
<b>Finestra di dialogo DHCP Enforcer Informs IP Address</b>	
IP Address	Stabilisce l'indirizzo IP associato al client, quale concentratore di accesso remoto (RAC), per il quale non si desidera eseguire la verifica della conformità al criterio e la reportistica relativa ai pacchetti informativi DHCP. Per impostazione predefinita, per i pacchetti informativi DHCP la verifica della conformità al criterio e la reportistica vengono eseguite. Quando viene indicato un indirizzo IP, da quel client <b>non</b> vengono eseguite la verifica della conformità al criterio né la reportistica per i pacchetti informativi DHCP.
<b>Finestra di dialogo DHCP Enforcer Resolve IP</b>	
Hostname	Quando l'indirizzo IP è sconosciuto, identifica il nome host del client per il quale non si desidera eseguire la verifica della conformità al criterio e la reportistica. Quando si inserisce il nome host, è possibile risolvere il nome host in un indirizzo IP.

## 9 Supporto tecnico

È possibile ricevere supporto tecnico per i prodotti Sophos in ciascuno dei seguenti modi:

- Visitando il forum SophosTalk su <http://community.sophos.com/> e cercando altri utenti con lo stesso problema.
- Visitando il knowledge base del supporto Sophos. <http://www.sophos.it/support/>
- Scaricando la documentazione del prodotto su <http://www.sophos.it/support/docs/>
- Inviando un'e-mail a [support@sophos.com](mailto:support@sophos.com), indicando il o i numeri di versione del software Sophos in vostro possesso, i sistemi operativi e relativi livelli di patch, ed il testo di ogni messaggio di errore.

## **10 Note legali**

Copyright © 2010 Sophos Group. Tutti i diritti riservati. Nessuna parte di questa pubblicazione può essere riprodotta, archiviata in un sistema di recupero, o trasmessa, in alcuna forma o in alcun mezzo, elettronico o meccanico, inclusi fotocopie, registrazione e altri mezzi, salvo che da un licenziatario autorizzato a riprodurre la documentazione in conformità con i termini della licenza, oppure previa autorizzazione scritta del titolare dei diritti d'autore.

Tutti gli altri nomi di società e prodotti sono marchi o marchi registrati dei rispettivi titolari.