

# SOPHOS

## Sophos NAC Advanced Guida all'attuazione dei criteri di sicurezza in DHCP

Versione prodotto: 3.2

Data documento: marzo 2011



# Sommario

1	Contenuti di questo documento.....	3
2	Panoramica sull'attuazione DHCP.....	4
3	Checklist per l'attuazione DHCP.....	5
4	Esenzioni DHCP.....	7
5	Criterio per la richiesta di connessione e client RADIUS per il server DHCP.....	9
6	Installazione del software DHCP Enforcer.....	14
7	Configurazione del server DHCP Microsoft.....	18
8	Operazioni di Compliance Manager.....	25
9	Supporto tecnico.....	36
10	Note legali.....	37

# 1 Contenuti di questo documento

Questo documento fornisce supporto per configurare l'attuazione DHCP, inclusa in Sophos NAC Advanced, in modo tale da identificare i computer non gestiti che si connettono alla rete, verificare il loro livello di sicurezza e controllarne l'accesso alla rete. Spiega come configurare DHCP Enforcer, il server DHCP Microsoft e il Compliance Application Server per una nuova installazione di Sophos NAC Advanced. Questo documento include informazioni relative ai seguenti argomenti:

- Panoramica sull'attuazione DHCP
- Checklist per l'attuazione DHCP
- Esenzioni DHCP
- Impostazioni DHCP nel Sophos Compliance Application Server
- Installazione del software DHCP Enforcer
- Tool di configurazione per DHCP
- Configurazione del server DHCP Microsoft
- Operazioni di Sophos Compliance Manager.

## 1.1 Destinatari della guida

I destinatari di questa guida sono professionisti del settore informatico non specializzati che operano in aziende di piccole e medie dimensioni o specialisti del settore informatico che operano in imprese con un numero di computer superiore a 25.000. Se si gestiscono più di 1000 computer, si consiglia di avvalersi dei Servizi professionali Sophos. I Servizi professionali Sophos collaborano con i dipendenti che si occupano della sicurezza informatica aziendale al fine di progettare e attuare un piano di distribuzione dei software di protezione.

## 1.2 Requisiti del software DHCP Enforcer

Per utilizzare l'attuazione DHCP con Sophos NAC Advanced, è necessario installare il software Sophos DHCP Enforcer nel server DHCP.

Requisiti di DHCP Enforcer	
Sistema operativo	Windows Server 2000, 2003, o 2008
Software DHCP	Software Microsoft® Dynamic Host Configuration Protocol (DHCP)

## 2 Panoramica sull'attuazione DHCP

Sophos NAC Advanced contiene 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 Advanced, 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 l'elenco di operazioni necessarie per implementare l'attuazione DHCP. Per ulteriori informazioni, consultare la sezione [Checklist per l'attuazione DHCP](#) a pagina 5. In questo documento vengono inoltre fornite istruzioni dettagliate relative a ciascun elemento della checklist.

### Sophos NAC Advanced Impostazioni predefinite per l'attuazione DHCP

- Tramite Compliance Manager è necessario abilitare l'attuazione DHCP in ogni criterio che si desidera utilizzare per tale attuazione.
- Quando l'attuazione DHCP è abilitata, ai computer conformi e parzialmente conformi è consentito l'accesso alla rete.
- Quando l'attuazione DHCP è abilitata, ai computer non conformi viene negato l'accesso alla rete.
- Ai computer privi di agente installato e non esenti viene negato l'accesso alla rete.
- Se un computer utilizza il Dissolvable Agent in Windows Vista e deve rilasciare/rinnovare i suoi indirizzi IP, l'agente visualizzerà un messaggio all'utente, richiedendogli le credenziali di amministrazione oppure di riavviare il computer.

### Sophos NAC Advanced Informazioni sull'upgrade

- Se DHCP è stato configurato durante un precedente rilascio del software, l'upgrade di Sophos NAC Advanced mantiene intatta la configurazione di DHCP. Non è richiesta alcuna modifica alla configurazione.

**Nota:** la nuova installazione di Sophos NAC Advanced eseguirà l'installazione di due nuovi template di accesso di DHCP Enforcer. Sophos NAC Advanced durante gli upgrade, i template di accesso di DHCP Enforcer esistenti verranno conservati.

### 3 Checklist per l'attuazione DHCP

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

Op.	Descrizione	Completata
<b>Sophos NAC Advanced Installazione, configurazione e distribuzione del Sophos Compliance Agent</b>		
1.	Installare e configurare Sophos NAC Advanced. Per ulteriori informazioni, consultare la <i>Guida all'installazione</i> di <i>Sophos NAC Advanced</i> .	
2.	Creare le esenzioni DHCP tramite Compliance Manager. Le esenzioni DHCP riguardano i computer esenti che non possono eseguire il Sophos Compliance Agent o che non richiedono la verifica della conformità, quali server, router, stampanti o computer ritenuti sicuri.	
3.	Distribuire il Sophos Compliance Agent nei computer. Per ulteriori informazioni, consultare la <i>Guida all'installazione</i> di <i>Sophos NAC Advanced</i> .	
<b>Impostazioni DHCP nel Sophos Compliance Application Server</b>		
4.	Creare un criterio di richiesta di connessione per DHCP sul Compliance Application Server.	
5.	Aggiungere un client RADIUS per il server DHCP nel Compliance Application Server.	
<b>Impostazioni di DHCP Enforcer nel server DHCP</b>		
6.	Installare il software di DHCP Enforcer nel server DHCP. <b>Nota:</b> dopo aver installato il software DHCP Enforcer, è necessario verificare che DHCP Enforcer sia in esecuzione su ciascun server DHCP.	
7.	Per poter lavorare con il server DHCP, configurare DHCP Enforcer tramite il tool di configurazione di DHCP Enforcer.	
<b>Configurazione del server DHCP</b>		
8.	Configurare il server DHCP in modo tale che operi in concomitanza con DHCP Enforcer.	
<b>Impostazioni di Sophos Compliance Manager</b>		
9.	Creare un criterio.	
10.	Creare un gruppo e assegnarvi un criterio.	
11.	Verificare le impostazioni di DHCP Enforcer.	

Op.	Descrizione	Completata
12.	Prima di abilitare l'attuazione DHCP, eseguire il report DHCP Enforcer per determinare lo stato di conformità dei computer. <b>Nota:</b> utilizzare il report DHCP Enforcer per stabilire se i computer riceveranno l'accesso alla rete adeguato una volta abilitata l'attuazione DHCP	
13.	Verificare i modelli di accesso di DHCP Enforcer e abilitare l'attuazione DHCP.	
<b>Sophos Compliance Dissolvable Agent Distribuzione</b>		
14.	Distribuire gli indirizzi del Sophos Compliance Dissolvable Agent ai computer ospiti. Per ulteriori informazioni, consultare la <i>Guida all'installazione</i> di <i>Sophos NAC Advanced</i> .	

## 4 Esenzioni DHCP

I computer esenti sono quelli che non possono eseguire il Compliance Agent o che non richiedono la verifica della conformità, quali server, router, stampanti o computer ritenuti sicuri. 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 Compliance 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.

### 4.1 Creazione di esenzioni per i criteri DHCP

Utilizzare la pagina Exemptions di Compliance Manager per creare le esenzioni per i criteri DHCP. Le esenzioni per i criteri DHCP sono esenzioni create con un solo valore relativo a indirizzo MAC, classe dell'utente o classe del fornitore, oppure con qualsiasi combinazione di tali valori. Le esenzioni DHCP e i modelli di accesso di DHCP Enforcer vengono utilizzati insieme per identificare un'esenzione e determinarne l'accesso alla rete.

#### Procedura

1. Accedere a Compliance 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 invece si specifica AA senza il carattere \* , verranno esentati solo gli indirizzi MAC con il nome AA.

6. Cliccare su **Select** per aggiungere all'esenzione i modelli di accesso di DHCP Enforcer, selezionare il modello di accesso Default - DHCP Permit (NULL User Class) e cliccare su **OK**.

**Nota:** il modello di accesso Default - DHCP Permit (NULL User Class) è quello predefinito in Sophos NAC Advanced per consentire l'accesso alla rete. Questa esenzione è così configurata per consentire l'accesso alla rete senza alcuna verifica di conformità da parte di Sophos NAC Advanced.

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. Si consiglia di dare maggiore priorità alle esenzioni più specifiche e di dare minore priorità a quelle meno specifiche.

## 4.2 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 Compliance Manager per creare le esenzioni per l'ambito IP. Le esenzioni per scope 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 Compliance 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. Cliccare su **Select** per aggiungere all'esenzione i modelli di accesso di DHCP Enforcer, selezionare il modello di accesso Default - DHCP Permit (NULL User Class) e cliccare su **OK**.

**Nota:** il modello di accesso Default - DHCP Permit (NULL User Class) è quello predefinito in Sophos NAC Advanced per consentire l'accesso alla rete. Questa esenzione è così configurata per consentire l'accesso alla rete senza alcuna verifica di conformità da parte di Sophos NAC Advanced.

6. 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. Si consiglia di dare maggiore priorità alle esenzioni più specifiche e di dare minore priorità a quelle meno specifiche.

## 5 Criterio per la richiesta di connessione e client RADIUS per il server DHCP

Affinché DHCP operi in modo adeguato, è necessario creare un criterio per la richiesta di connessione e un client RADIUS per il server DHCP. Entrambe le operazioni vengono eseguite nel Compliance Application Server. Il criterio per la richiesta di connessione differenzia le richieste di conformità DHCP dalle altre richieste. Il server DHCP deve essere un client RADIUS affinché gli sia consentito di inviare richieste di attuazione a Sophos NAC Advanced.

### 5.1 Creazione di un criterio di richiesta di connessione per DHCP (Windows Server 2003)

Al fine di utilizzare l'attuazione DHCP, è necessario creare un criterio per la richiesta di connessione nel Sophos Compliance Application Server. Il criterio per la richiesta di connessione differenzia le richieste di conformità DHCP dalle altre richieste. Il criterio viene creato in modo tale che il Sophos NAC Advanced possa distinguere questa richiesta da quelle non DHCP e fornire un'attuazione adeguata.

1. Dal menu Start nel Sophos Compliance Application Server, cliccare su **Strumenti di amministrazione Servizio autenticazione Internet**.

Viene aperto IAS.

2. Cliccare su **Elaborazione richiesta di connessione**.
3. Cliccare col tasto destro del mouse su **Criteri di richiesta connessione** e poi cliccare su **Nuovo criterio richiesta di connessione**.

Viene visualizzata la procedura guidata del criterio richiesta di connessione.

4. Cliccare su **Avanti**.
5. Selezionare il pulsante di opzione **Criterio personalizzato**.
6. Digitare **DHCP** come nome del criterio per la richiesta di connessione e successivamente cliccare su **Avanti**.

Il nome **DHCP** indica che questo criterio di richiesta di connessione viene utilizzato per l'attuazione DHCP.

7. Cliccare su **Aggiungi** per aggiungere una condizione al criterio.
8. Selezionare **User-Name** e successivamente cliccare su **Aggiungi**.
9. Digitare  $^{[0-9a-f]{2,32}}$  come nome utente e cliccare su **OK**.

**Nota:** per DHCP, Sophos utilizza un indirizzo MAC come nome utente. Questo valore ha le caratteristiche di una stringa esadecimale contenente da 2 a 32 caratteri.

10. Cliccare su **Aggiungi** per aggiungere un'altra condizione al criterio.
11. Selezionare **Calling-Station-ID** e successivamente cliccare su **Aggiungi**.
12. Digitare  $^{[0-9a-f]{2,32}}$  come ID della stazione chiamante e cliccare su **OK**.

**Nota:** per DHCP, Sophos utilizza un indirizzo MAC come Calling-Station-ID. Questo valore ha le caratteristiche di una stringa esadecimale contenente da 2 a 32 caratteri.

13. Cliccare su **Aggiungi** per aggiungere un'altra condizione al criterio.
14. Selezionare **Tipo di servizio** e successivamente cliccare su **Aggiungi**.
15. Selezionare **Authenticate Only** e cliccare su **Aggiungi** per aggiungere Solo autenticazione all'opzione Tipo servizio.
16. Cliccare su **OK**.
17. Cliccare su **Aggiungi** per aggiungere un'altra condizione al criterio.
18. Selezionare **Nome descrittivo client** e successivamente cliccare su **Aggiungi**.
19. Digitare **DHCP** e poi cliccare su **OK Avanti**.

**Nota:** il nome del client RADIUS deve contenere la dicitura "DHCP" al suo interno per consentire a DHCP di operare in modo adeguato. Il nome del client non distingue fra maiuscole e minuscole.

20. Cliccare su **Modifica profilo**.
21. Cliccare sul pulsante di opzione **Accetta utenti senza la convalida delle credenziali** e successivamente cliccare su **OK**.

**Nota:** il criterio per la richiesta di connessione è impostato in modo tale da non dover richiedere l'autenticazione agli utenti, in quanto questa procedura viene condotta dal Compliance Agent. Sophos NAC Advanced esegue l'autenticazione per tutti i pacchetti di richiesta DHCP. Gli utenti non autenticati dall'agente o non esenti vengono considerati non conformi.

22. Cliccare su **Avanti**.
23. Cliccare su **Fine**.

**Nota:** se si clicca due volte sul criterio appena creato, viene visualizzata una finestra contenente le condizioni del criterio.

## 5.2 Creazione di un criterio di richiesta di connessione per DHCP (Windows Server 2008)

Per utilizzare l'attuazione DHCP, è necessario creare un criterio per la richiesta di connessione nel Sophos Compliance Application Server. Il criterio per la richiesta di connessione differenzia le richieste di conformità DHCP dalle altre richieste. Il criterio viene creato in modo tale che il Sophos NAC Advanced possa distinguere questa richiesta da quelle non DHCP e fornire un'attuazione adeguata.

1. Dal menu Start del Sophos Compliance Application Server, cliccare su **Strumenti di amministrazione Server dei criteri di rete**.  
Viene avviato il Server dei criteri di rete.
2. In "Criteri", cliccare con il tasto destro del mouse su **Criterio richiesta di connessione**, e poi cliccare su **Nuovo**.  
Viene visualizzata la procedura guidata del nuovo criterio di richiesta di connessione.

3. Inserire **DHCP** come nome del criterio di richiesta di connessione, lasciare come metodo di connessione alla rete **Non specificato**, e cliccare su **Avanti**.

Il nome **DHCP** indica che questo criterio di richiesta di connessione viene utilizzato per l'attuazione DHCP.

4. Cliccare su **Aggiungi** per aggiungere una condizione al criterio.
5. Selezionare **Nome utente** e successivamente cliccare su **Aggiungi**.
6. Digitare  $^{[0-9a-f]}_{2,32}$  come nome utente e cliccare su **OK**.

**Nota:** per DHCP, Sophos utilizza un indirizzo MAC come nome utente. Questo valore ha le caratteristiche di una stringa esadecimale contenente da 2 a 32 caratteri.

7. Cliccare su **Aggiungi** per aggiungere un'altra condizione al criterio.
8. Selezionare **ID della stazione chiamante** e successivamente cliccare su **Aggiungi**.
9. Digitare  $^{[0-9a-f]}_{2,32}$  come ID della stazione chiamante e cliccare su **OK**.

**Nota:** per DHCP, Sophos utilizza un indirizzo MAC come Calling Station ID. Questo valore ha le caratteristiche di una stringa esadecimale contenente da 2 a 32 caratteri.

10. Cliccare su **Aggiungi** per aggiungere un'altra condizione al criterio.
11. Selezionare **Tipo di servizio** e successivamente cliccare su **Aggiungi**.
12. Selezionare **Autentica solo**, e cliccare su **Aggiungi**.
13. Cliccare su **OK**.
14. Cliccare su **Aggiungi** per aggiungere un'altra condizione al criterio.
15. Selezionare **Nome descrittivo del client** e successivamente cliccare su **Aggiungi**.
16. Digitare **DHCP** e poi cliccare su **OK Avanti**.

**Nota:** il nome del client RADIUS deve contenere la dicitura "DHCP" al suo interno per consentire a DHCP di operare in modo adeguato. Il nome del client non distingue fra maiuscole e minuscole.

17. Nella sezione **Autenticazione**, selezionare il pulsante di opzione **Accetta utenti senza la convalida delle credenziali**, e cliccare su **Avanti**.

**Nota:** il criterio per la richiesta di connessione è impostato in modo tale da non dover richiedere l'autenticazione agli utenti in quanto tale procedura viene condotta dal Compliance Agent. Sophos NAC Advanced conduce l'autenticazione per tutti i pacchetti di richiesta DHCP. Gli utenti non autenticati dall'agente o non esenti vengono considerati non conformi.

18. Cliccare su **Avanti**. Non è necessario configurare attributi per questo criterio.
19. Cliccare su **Fine**.

**Nota:** se si clicca due volte sul criterio appena creato, viene visualizzata una finestra contenente le condizioni del criterio.

### 5.3 Aggiunta di un client RADIUS per il server DHCP (Windows Server 2003)

Nel Sophos Compliance Application Server, è necessario aggiungere a IAS il server DHCP. Il server DHCP deve essere un client RADIUS affinché possa inviare richieste di attuazione al Sophos NAC Advanced.

1. Dal menu Start nel Sophos Compliance Application Server, cliccare su **Strumenti di amministrazione Servizio autenticazione Internet**.

Viene aperto IAS.

2. Cliccare col tasto destro del mouse su **Client RADIUS** e selezionare **Nuovo client RADIUS**.
3. Digitare **DHCP** nel campo **Nome descrittivo** e poi digitare l'indirizzo IP o il nome DNS del server DHCP nel campo **Indirizzo client**. Cliccare su **Avanti** per continuare.

**Nota:** Per un corretto funzionamento di DHCP, denominare il client RADIUS come **DHCP**. Questo nome corrisponde a quello del criterio per la richiesta di connessione.

4. Digitare, nel campo adeguato, **DHCP** come shared secret (segreto condiviso) del server DHCP e darne conferma. Lo shared secret del DHCP verrà utilizzato successivamente, al momento della configurazione del server DHCP affinché operi con Sophos NAC Advanced.

**Nota:** nel campo Fornitore client, lasciare l'opzione predefinita RADIUS Standard.

5. Verificare che la casella **La richiesta deve contenere l'attributo autenticatore del messaggio** non sia spuntata.
6. Cliccare su **Fine**.

### 5.4 Aggiunta di un client RADIUS per il server DHCP (Windows Server 2008)

Nel Sophos Compliance Application Server, è necessario aggiungere il server DHCP al Server dei criteri di rete. Il server DHCP deve essere un client RADIUS affinché gli sia consentito di inviare richieste di attuazione al Sophos NAC Advanced.

1. Dal menu Start del Sophos Compliance Application Server, cliccare su **Strumenti di amministrazione Server dei criteri di rete**.

Viene avviato il Server dei criteri di rete.

2. In "RADIUS Clients and Servers", cliccare con il tasto destro del mouse su **Client RADIUS**, e poi su **Nuovo client RADIUS**.
3. Digitare **DHCP** nel campo **Nome** e poi digitare l'indirizzo IP o il nome DNS del server DHCP nel campo **Indirizzo (IP o DNS)**.

**Nota:** per un corretto funzionamento di DHCP, denominare il client RADIUS come **DHCP**. Questo nome corrisponde a quello del criterio per la richiesta di connessione.

4. Digitare, nel campo adeguato, **DHCP** come shared secret (segreto condiviso) del server DHCP e darne conferma. Lo shared secret del DHCP verrà utilizzato successivamente, al momento della configurazione del server DHCP affinché operi con Sophos NAC Advanced.

**Nota:** nel campo Nome fornitore, lasciare l'opzione predefinita RADIUS Standard.

5. Verificare che la casella **I messaggi di richiesta di accesso devono contenere l'attributo autenticatore del messaggio non** sia spuntata.
6. Cliccare su **OK**.

## 6 Installazione del software DHCP Enforcer

Installare il software DHCP Enforcer nel server DHCP Microsoft. Il software DHCP Enforcer include DHCP Enforcer e l'utilità di configurazione di DHCP Enforcer.

1. Scaricare il software di DHCP Enforcer dal sito web Sophos.
2. Cliccare due volte sul file di installazione del software di DHCP Enforcer per eseguirne l'installazione.
3. Cliccare su **Avanti**.

Viene visualizzata la procedura guidata dell'installazione di DHCP Enforcer.

4. Selezionare il pulsante di opzione **Completa**. Cliccare su **Avanti**.

**Nota:** l'installazione esegue la scansione del server alla ricerca del server DHCP Microsoft e installa automaticamente i componenti del software DHCP Enforcer.

5. Per installare il software, cliccare su **Installa**.
6. Cliccare su **Fine**.

**Nota:** una volta terminata l'installazione, utilizzare lo strumento di configurazione di DHCP Enforcer per configurare le impostazioni del server DHCP. Per ulteriori informazioni, consultare la sezione [Tool di configurazione per DHCP](#) a pagina 14.

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

### 6.1 Disinstallazione del software Microsoft DHCP Enforcer

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

### 6.2 Tool di configurazione per DHCP

Per poter lavorare con il server DHCP, configurare DHCP Enforcer tramite il tool di configurazione di DHCP Enforcer. Il tool di configurazione di DHCP Enforcer viene installato come parte della procedura di installazione di DHCP Enforcer e supporta i server Windows che eseguono il software Microsoft Dynamic Host Configuration Protocol (DHCP).

#### 6.2.1 Specificazione delle impostazioni di DHCP Enforcer

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

Viene visualizzata la finestra di configurazione del DHCP con la scheda Enforcer selezionata.

2. Lasciare vuoto il campo **Default User Class**.

La classe utente predefinita viene utilizzata solo se il Compliance Application Server non produce una. Per esempio, il Compliance Application Server potrebbe non produrre alcuna classe utente quando il Compliance Application Server è inattivo, quando la connessione tra il server DHCP e il Compliance Application Server è inattiva o quando Sophos NAC Advanced non trova una classe utente per l'ambito. La classe utente NULL è predefinita in Sophos NAC Advanced per consentire l'accesso alla rete.

3. Nella sezione RADIUS Enforcer Servers, cliccare su **Add** per specificare il Compliance Application Server. Il Compliance Application Server deve poter comunicare col server DHCP.
4. Lasciare spuntata la casella **Enable** per tenere attivo il Compliance Application Server.
5. Digitare l'indirizzo IP del Compliance Application Server nel campo **IP Address**. Altrimenti, cliccare su **Resolve IP...**, digitare il nome host nel relativo campo e cliccare su **OK**.
6. A meno che il server DHCP non utilizzi porte differenti, non modificare le impostazioni predefinite relative alle porte di autenticazione e di accounting.
7. Digitare **DHCP** come shared secret e di nuovo **DHCP** per confermare lo shared secret del server DHCP.

DHCP ha il medesimo shared secret utilizzato nella configurazione del server DHCP. Per ulteriori informazioni, consultare la sezione [Aggiunta di un client RADIUS per il server DHCP \(Windows Server 2003\)](#) a pagina 12 o [Aggiunta di un client RADIUS per il server DHCP \(Windows Server 2008\)](#) a pagina 12.

8. Cliccare su **OK**.

**Nota:** non modificare le impostazioni predefinite della scheda Microsoft dal momento che non è necessario alcun cambiamento.

9. Per specificare più di un Compliance Application Server, ripetere i passaggi da 3 a 8.
10. Se si specifica più di un Compliance Application Server, selezionare il pulsante di opzione **Access for Multiple Servers** appropriato.

L'accesso sequenziale consente di accedere a tutti i Compliance Application Server, secondo l'ordine indicato. L'accesso bilanciato fa accedere a tutti i server contemporaneamente tramite il bilanciamento dei carichi.

**Nota:** per l'accesso sequenziale, è possibile ordinare i server secondo la priorità tramite i pulsanti **Move Up** e **Move Down**.

11. Cliccare su **OK**.

## 6.2.2 Campi e descrizioni

Campi	Descrizioni
Scheda Enforcer	

Campi	Descrizioni
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.
Enable Reserved Option Reporting	Quando è selezionata questa opzione, la reportistica è abilitata per identificare i codici delle opzioni riservate.
Attempts	Stabilisce quante volte debba essere iniziata la reportistica per un pacchetto di richiesta DHCP.
Timeout	Stabilisce, in secondi, il tempo di attesa del server DHCP prima di creare un altro report.
Access for Multiple Servers	Stabilisce in che modo i Compliance Application Server multipli eseguono l'accesso. L'accesso sequenziale consente di accedere a tutti i Compliance Application Server, secondo l'ordine indicato. L'accesso bilanciato consente di accedere a tutti i Compliance Application Server contemporaneamente, tramite il bilanciamento dei carichi.  <b>Nota:</b> per l'accesso sequenziale, è possibile ordinare i Compliance Application Server in base alla priorità tramite i pulsanti Move Up e Move Down.
<b>Finestra delle impostazioni del server di DHCP Enforcer RADIUS Enforcer</b>	
<b>Nota:</b> i campi di questa finestra sono relativi al Compliance Application Server.	
Enable	Indica se il Compliance Application Server è abilitato. Quando abilitato, il Compliance Application Server viene utilizzato per la conformità al criterio e l'attività di reportistica.
IP Address	Indica l'indirizzo IP del Compliance Application Server.
Authentication Port	Indica la porta di autenticazione del Compliance Application Server.
Accounting Port	Indica la porta di accounting del Compliance Application Server.
Shared Secret	Indica lo shared secret del server DHCP. Lo shared secret corrisponde a quello utilizzato nella configurazione del server DHCP. Per ulteriori informazioni, consultare la sezione <a href="#">Aggiunta di un client RADIUS per il</a>

Campi	Descrizioni
	<i>server DHCP (Windows Server 2003) a pagina 12 o Aggiunta di un client RADIUS per il server DHCP (Windows Server 2008) a pagina 12.</i>
Confirm Shared Secret	Conferma lo shared secret del server DHCP. Lo shared secret corrisponde a quello utilizzato nella configurazione del server DHCP. Per ulteriori informazioni, consultare la sezione <i>Aggiunta di un client RADIUS per il server DHCP (Windows Server 2003) a pagina 12 o Aggiunta di un client RADIUS per il server DHCP (Windows Server 2008) a pagina 12.</i>
<b>Finestra Resolve IP</b>	
Hostname	Nel caso in cui l'indirizzo IP sia sconosciuto, indica il nome host del Compliance Application Server.

## 7 Configurazione del server DHCP Microsoft

Per configurare il server DHCP Microsoft è necessario creare delle classi di utenti DHCP che corrispondano alle classi utente predefinite in Sophos NAC Advanced. La classe utente NULL si riferisce a computer conformi o parzialmente conformi. Ai computer conformi o parzialmente conformi viene consentito l'accesso alla rete.

La classe utente NACDeny si riferisce a computer non conformi e che non hanno il Compliance Agent installato. I computer non conformi vengono messi in quarantena e hanno accesso limitato alla rete. L'accesso alla rete viene determinato tramite le opzioni di ambito di Microsoft definite. Per ulteriori informazioni, consultare la sezione [Modifica delle opzioni di ambito di Microsoft per poter specificare le classi utenti](#) a pagina 19.

Se nella rete sono presenti stampanti o sistemi operativi non Windows che ricevono un indirizzo IP assegnato in modo dinamico tramite DHCP, è necessario creare esenzioni per tali computer in Compliance Manager. Per ulteriori informazioni, consultare la sezione [Esenzioni DHCP](#) a pagina 7. 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. Quando esentati, i computer possono accedere alla rete. Per ulteriori informazioni, consultare le sezioni [Creazione di esenzioni per i criteri DHCP](#) a pagina 7 e [Creazione delle esenzioni per ambito IP](#) a pagina 8.

**Nota:** questa sezione si riferisce alla classe utente NULL. Microsoft definisce la classe utente NULL come classe predefinita nel server DHCP. In Sophos NAC Advanced, la classe utente NULL è predefinita per consentire l'accesso alla rete.

### 7.1 Definizione delle classi utente di Microsoft DHCP

Per configurare il server DHCP Microsoft è necessario creare delle classi di utenti DHCP che corrispondano alle classi utente predefinite in Sophos NAC Advanced. In Sophos NAC Advanced, la classe utente NULL è predefinita per i computer conformi o parzialmente conformi. Ai computer conformi o parzialmente conformi viene consentito l'accesso alla rete. La classe utente NACDeny è predefinita in Sophos NAC Advanced per i computer non conformi, per quelli su cui non è installato il Compliance Agent, e per quelli in cui il Dissolvable Agent non è in esecuzione. I computer non conformi vengono messi in quarantena e hanno accesso limitato alla rete.

**Nota:** la classe utente NULL è predefinita nel server DHCP Microsoft, di conseguenza non è necessario definire una classe utente per NULL.

1. Nel server DHCP Microsoft, aprire la console di gestione DHCP, cliccare col tasto destro del mouse sul nome del server DHCP e selezionare **Definisci classi utente**.

Viene visualizzata la finestra Classi utente DHCP.

2. Cliccare su **Aggiungi**.

Viene visualizzata la finestra Nuova classe.

3. Digitare **NACDeny** come nome visualizzato e **Sophos NAC Advanced Deny User Class** come descrizione.

4. Posizionare il cursore nella colonna ASCII e digitare **NACDeny** quale classe utente.

**Nota:** questa classe utente distingue tra maiuscole e minuscole, è quindi essenziale digitarne il nome nella forma esatta in cui compare in questo passaggio; in questo modo la classe utente corrisponderà a quella predefinita in Sophos NAC Advanced. La classe utente NACDeny è predefinita nel modello di accesso Default - DHCP Deny (NACDeny User Class).

5. Cliccare su **OK** per creare la classe utente NACDeny.

**Nota:** la classe utente NULL è predefinita nel server DHCP Microsoft, di conseguenza non è necessario definire una classe utente per NULL.

6. Per chiudere la finestra Classi utente DHCP, cliccare su **Chiudi**.

## 7.2 Modifica delle opzioni di ambito di Microsoft per poter specificare le classi utenti

DHCP Enforcer opera abbinando una classe utente a ogni richiesta DHCP. I computer non conformi e non esenti, compresi i computer privi del Compliance Agent e quelli su cui il Dissolvable Agent non è in esecuzione, vengono abbinati alla classe utente NACDeny, predefinita in Sophos NAC Advanced e configurata nel server DHCP. I computer conformi e parzialmente conformi vengono abbinati alla classe utente NULL predefinita in Sophos NAC Advanced e nel server DHCP. La classe utente NULL consente pieno accesso sia alla rete interna che a Internet. La classe utente NACDeny mette in quarantena i computer non conformi. È possibile limitare l'accesso alla rete indicando route statiche per qualsiasi server DNS, server di correzione o altra risorsa di rete alla quale si desidera consentire l'accesso da parte dei computer non conformi.

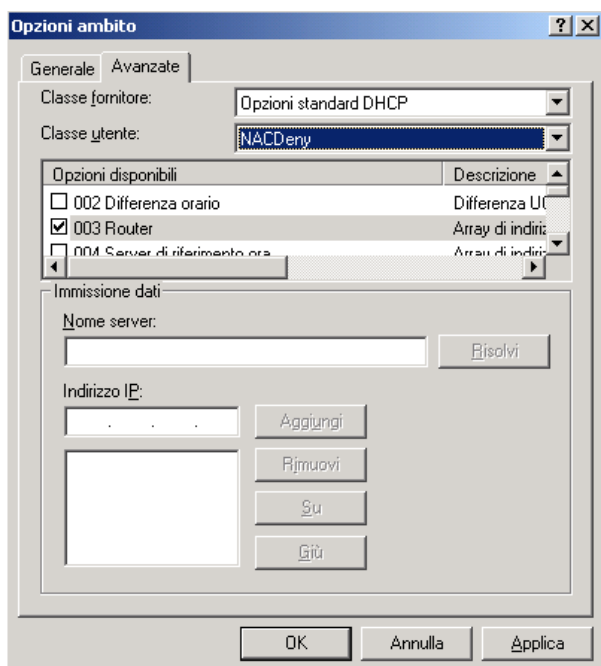
**Importante:** queste istruzioni consentono la modifica di un solo ambito. Per gli ambiti addizionali, è necessario ripetere le istruzioni. Solitamente a un ambito corrisponde un segmento della rete.

1. Nel server DHCP Microsoft, aprire la console di gestione DHCP, espandere la cartella relativa all'ambito appropriato, cliccare col tasto destro del mouse su **Opzioni ambito** e selezionare **Configura opzioni**.
2. Selezionare la scheda **Avanzate** e poi **NACDeny** dall'elenco **Classe utente**.

La classe utente NACDeny viene così definita nel server DHCP. Per ulteriori informazioni, consultare la sezione [Definizione delle classi utente di Microsoft DHCP](#) a pagina 18.

3. Spuntare la casella **003 Router** nell'area Opzioni disponibili.

**Nota:** si sta così configurando la quarantena per i computer non conformi, non esenti, che non hanno installato il Compliance Agent, o su cui il Dissolvable Agent non è in esecuzione. Questa configurazione applica ai computer un gateway vuoto in modo tale che venga loro negato l'accesso alla rete. È possibile limitare l'accesso alla rete indicando route statiche per qualsiasi server DNS, server di correzione, server proxy per l'accesso a Internet o altra risorsa di rete alla quale si desidera consentire l'accesso da parte dei computer non conformi durante la quarantena.



4. Per impostare questa opzione, cliccare su **Applica**.

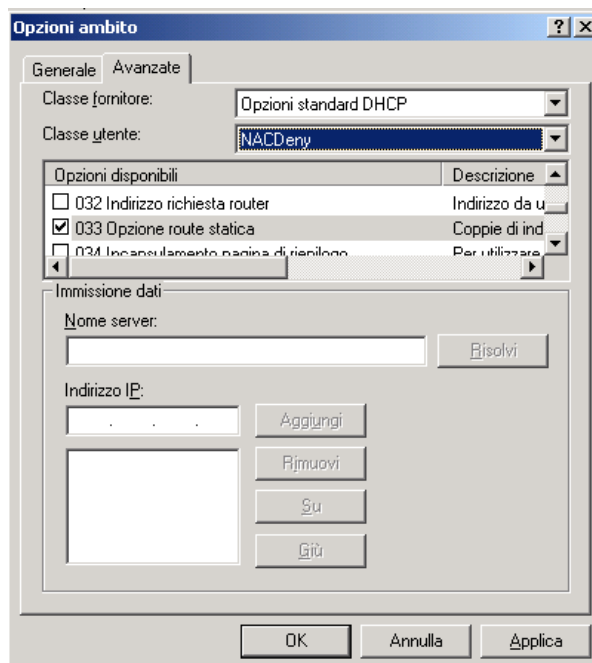
Non aggiungere alcun indirizzo IP per la classe utente del router. Questo passaggio applica ai computer un gateway vuoto in modo tale che venga loro negato l'accesso alla rete.

5. Selezionare **NACDeny** dall'elenco **Classe utente**.

**Nota:** la classe utente NACDeny viene così creata nel server DHCP per gli utenti in quarantena. Per ulteriori informazioni, consultare la sezione [Definizione delle classi utente di Microsoft DHCP](#) a pagina 18.

6. Spuntare la casella **033 Opzione route statica** dall'area Opzioni disponibili.

Ai computer che sono non conformi, non esenti, che non hanno installato il Compliance Agent, o su cui non è in esecuzione il Dissolvable Agent non viene dato alcun gateway. Configurare una route statica per il Compliance Application Server, in modo tale che i computer non conformi possano comunicare con il Compliance Application Server.



7. Digitare il nome del Compliance Application Server nel campo **Nome server** e cliccare su **Risolvi**; oppure, digitare l'indirizzo IP del server nel campo **Indirizzo IP** e cliccare su **Aggiungi**.

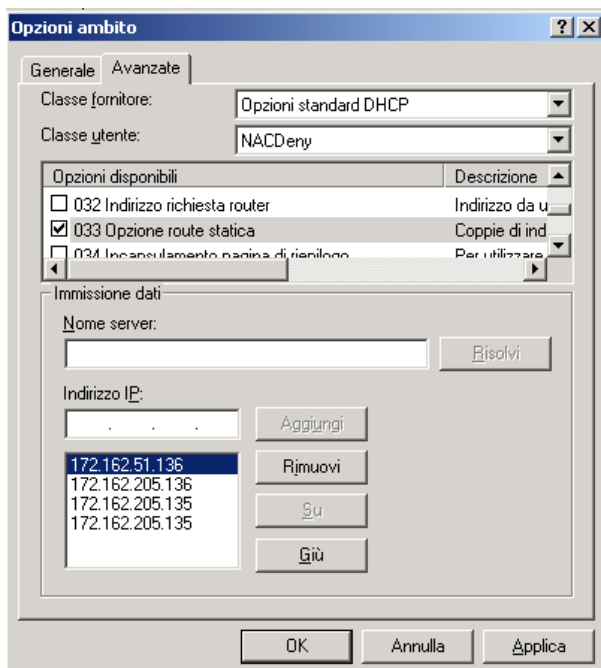
**Nota:** l'opzione relativa alla route statica del DHCP richiede una coppia di indirizzi IP, destinazione e router, per ciascuna route statica. Per gli indirizzi localizzati nello stesso segmento del computer, aggiungere nuovamente tale indirizzo in modo che compaia due volte nell'elenco degli indirizzi IP. Per quanto riguarda gli indirizzi su segmenti diversi, aggiungere l'indirizzo del router attraverso cui il computer raggiunge la destinazione.

8. Digitare il nome del server di correzione nel campo **Nome server** e cliccare su **Risolvi**; oppure, digitare l'indirizzo IP del server di correzione nel campo **Indirizzo IP** e cliccare su **Aggiungi**.

**Nota:** l'opzione relativa alla route statica del DHCP richiede una coppia di indirizzi IP, destinazione e router, per ciascuna route statica. Per gli indirizzi localizzati nello stesso segmento del computer, aggiungere nuovamente tale indirizzo in modo che compaia due volte nell'elenco degli indirizzi IP. Per quanto riguarda gli indirizzi su segmenti diversi, aggiungere l'indirizzo del router attraverso cui il computer raggiunge la destinazione.

9. Ripetere il passaggio 8 per aggiungere indirizzi IP aggiuntivi a qualsiasi server DNS, server di correzione, server proxy per l'accesso a Internet o altra risorsa di rete alla quale si desidera consentire l'accesso da parte dei computer non conformi durante la quarantena.

**Nota:** permettendo l'accesso esclusivamente a queste route statiche, si mettono in quarantena i computer non conformi. L'accesso alla rete viene limitato agli indirizzi IP statici che sono stati definiti e a Internet. Gli indirizzi IP interni non sono raggiungibili. I seguenti indirizzi hanno scopo esclusivamente illustrativo.



10. Per terminare cliccare su **OK**.

**Importante:** queste istruzioni consentono la modifica di un solo ambito. Per gli ambiti aggiuntivi, è necessario ripetere le istruzioni. Solitamente a un ambito corrisponde un segmento della rete.

### 7.3 Panoramica sulla modalità bypass di DHCP Enforcement

DHCP Enforcer include la modalità bypass che ha lo scopo di sospendere, solo temporaneamente, l'attuazione della conformità quando si verifica un carico eccessivo del backend. Il carico eccessivo del backend può essere dovuto a interruzioni della rete, elevata latenza della rete, conflitti tra database o sovraccarico del RADIUS Enforcer.

Quando attivata, la modalità bypass registra lo stato finale di richiesta di conformità relativo a ogni transazione DHCP. Lo stato viene registrato per tutte le transazioni DHCP, ma non per quelle di attuazione (RADIUS). Per esempio, se DHCP Enforcer è configurato in modo tale da eseguire più tentativi di attuazione, ma nessuno di questi tentativi ha esito positivo, viene registrato un solo insuccesso, invece che più fallimenti. Se lo stato finale di una sessione rileva un errore di rete o un timeout di attivazione, il contatore aumenta di uno. Quando si

verifica una sessione positiva, il contatore viene azzerato. Se il contatore raggiunge un limite prefissato, si attiva la modalità bypass per un periodo di tempo limitato.

**Nota:** è possibile scegliere sia il limite massimo per il contatore che il periodo di tempo in cui la modalità bypass sarà attiva.

Durante il periodo di tempo in cui la modalità bypass è attiva, tutte le transazioni DHCP gestite da DHCP Enforcer vengono assegnate a una classe utente DHCP specificata in precedenza. Per impostazione predefinita, DHCP Enforcer utilizza la classe utente NULL. A seconda della configurazione del DHCP server, la classe utente DHCP in modalità bypass può essere utilizzata per limitare o consentire l'accesso ai computer endpoint che richiedono indirizzi.

### 7.3.1 Impostazioni di registro della modalità bypass di DHCP Enforcement

L'attivazione della modalità bypass di DHCP è assolutamente opzionale. Le impostazioni della modalità bypass devono essere specificate nel registro di tutti i DHCP server, una volta eseguita l'installazione di DHCP Enforcer. Per attivare la modalità bypass, DHCP Enforcer deve essere installato e tale modalità deve essere abilitata.

Dal momento che la funzione bypass supervisiona le transazioni DHCP, ma non quelle di attuazione, è necessario scegliere con attenzione la combinazione di impostazioni adeguata per il proprio DHCP Enforcer.

**Importante:** è necessario specificare tutte le impostazioni della modalità bypass per tutti i DHCP server, nel seguente percorso di registro:

HKLM\SOFTWARE\Sophos\NAC\ServerExtensions\DHCP\Microsoft. Tutte le impostazioni sono REG\_DWORD, ad eccezione della classe utente, che è invece REG\_SZ.

Impostazioni registro modalità bypass	Descrizione	Valore predefinito
BypassModeEnabled	Indica se la modalità bypass è abilitata o meno.	BypassModeEnabled ha un valore predefinito di 0 (disabilitata).  Per abilitare la modalità bypass, impostare tale valore su 1 e riavviare il DHCP server.
BypassErrorLimit	Il numero di errori ricevuti prima che la modalità bypass venga attivata.	BypassErrorLimit ha un valore predefinito di 3. È possibile specificare un valore minimo di 1 e uno massimo di 60.  È possibile modificare questa impostazione senza riavviare il DHCP server.
BypassErrorTimeoutSeconds	Il periodo di tempo, in secondi, in cui la modalità bypass resterà attiva.	BypassErrorTimeoutSecond ha un valore predefinito di 300 (5 minuti). È possibile specificare un valore minimo di 15 e uno massimo di 900 (15 minuti).

Impostazioni registro modalità bypass	Descrizione	Valore predefinito
		È possibile modificare questa impostazione senza riavviare il DHCP server.
BypassUserClass	La classe utente DHCP che viene assegnata quando DHCP Enforcer è in modalità bypass.	Il valore predefinito è NULL. Questo valore indica che nella richiesta DHCP non è presente alcuna classe utente. <b>Nota:</b> si tratta di un comportamento predefinito della piattaforma del sistema operativo client di Windows. È possibile modificare questa impostazione senza riavviare il DHCP server.

### 7.3.2 Messaggi in modalità bypass del log eventi del DHCP Server

La modalità bypass scrive messaggi nel log degli eventi del DHCP Server, quando InfoLogging è abilitato in DHCP Enforcer. I messaggi sono i seguenti:

Evento	ID evento
Modalità bypass attiva	10224
Modalità bypass scaduta e quindi disattivata	10225

## 7.4 Abilitazione della reportistica relativa ai messaggi informativi di DHCP

Per impostazione predefinita i messaggi informativi di DHCP vengono attuati, ma non costituiscono oggetto di report. È possibile abilitare la reportistica relativa ai messaggi informativi aggiungendo un valore alla chiave di registro Microsoft esistente. Se in possesso di una vasta implementazione DHCP, si consiglia di non attivare la reportistica relativa ai messaggi informativi dal momento che potrebbe compromettere il rendimento di Sophos NAC Advanced.

1. Trovare la seguente chiave di registro nel DHCP server:  
HKLM\SOFTWARE\Sophos\NAC\ServerExtensions\DHCP\Microsoft.
2. Aggiungere il valore di registro **DWORD**.
3. Digitare **ReportInforms** come **Nome valore**.
4. Digitare **1** come **Dati valore**.
5. Cliccare su **OK** per salvare il valore.

La reportistica relativa ai messaggi informativi è ora abilitata.

## 8 Operazioni di Compliance Manager

Se si esegue il Compliance Manager, l'attuazione DHCP dovrebbe funzionare con cambiamenti minimi o nulli. Come minimo, è necessario creare un criterio e un gruppo a cui assegnare tale criterio. È poi possibile abilitare l'attuazione DHCP.

Compliance Manager Le operazioni comprendono:

- Creare un criterio.
- Creare un gruppo e assegnarvi un criterio.
- Verificare che le impostazioni predefinite di DHCP Enforcer siano adeguate all'implementazione di DHCP.
- Eseguire il report DHCP Enforcer di Compliance Manager per visualizzare le informazioni del report del DHCP.

**Nota:** Utilizzare il report DHCP Enforcer per stabilire se i computer riceveranno l'accesso alla rete adeguato una volta abilitata l'attuazione DHCP

- Verificare i modelli di accesso di DHCP Enforcer e abilitare l'attuazione DHCP.

### 8.1 Creazione di un criterio

I criteri controllano l'accesso alle risorse di rete aziendali affidandosi alla valutazione del profilo del computer. I criteri gestiscono la configurazione che determina lo stato di conformità del computer, la visualizzazione dei messaggi, le azioni correttive intraprese e quelle di attuazione. I criteri includono le impostazioni dell'agente, i profili e le assegnazioni dei modelli di accesso.

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

#### Procedura

1. Accedere a Compliance Manager.
2. Cliccare su **Manage > Policies** . Quindi, cliccare su **Create Policy** in basso a sinistra nella pagina.
3. Digitare un nome e una descrizione per il criterio.
4. Uscire dall'impostazione Policy Mode.

5. Specificare le impostazioni di DHCP Agent. Queste impostazioni sono valide solo se si implementa l'attuazione DHCP:
  - **Agent Enforcement Action:** stabilisce il metodo utilizzato per ottenere i nuovi indirizzi IP per il computer. L'agente ottiene degli 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:
    - **None:** gli indirizzi IP per il computer non sono né rilasciati né rinnovati. Selezionare **None** quando non si applica l'attuazione DHCP.
    - **Release Renew:** 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. Quando si utilizza l'attuazione DHCP, è **necessario** selezionare Release Renew.

**Nota:** se un computer utilizza il Dissolvable Agent in Windows Vista e deve rilasciare rinnovare i suoi indirizzi IP, l'agente visualizzerà un messaggio all'utente, richiedendogli le credenziali di amministrazione oppure di riavviare il computer.
6. Cliccare su **Add Profiles**.

7. Spuntare le caselle accanto ai profili dei sistemi operativi che si desidera aggiungere al criterio, poi cliccare su **OK**.

Se si selezionano più profili di sistema operativo, è possibile dare loro differenti priorità ai fini della valutazione. Il comportamento del criterio viene valutato come segue.

- **Required - Use Best Profile:** il profilo del sistema operativo è necessario e viene valutato come il profilo più probabile. Nel caso in cui nel computer non sia installato uno dei sistemi operativi necessari, lo stato di conformità della condizione Else del profilo del sistema operativo con priorità massima viene utilizzato per determinare lo stato e le azioni di conformità del tipo di profilo del sistema operativo e, per questo criterio, non verrà valutato nessun altro profilo.
- **Use Best Profile:** sul computer viene valutato ciascun profilo del criterio appartenente a una determinata tipologia, viene stabilita la migliore corrispondenza e infine vengono condotte esclusivamente le azioni di garanzia relative la profilo che meglio corrisponde. Il comportamento Best utilizza il profilo **più** conforme presente nel computer per determinare lo stato di conformità del tipo di profilo nel criterio. I profili delle applicazioni, se non contrariamente diagnosticato, vengono valutati in questo modo. Se nel computer non è installato nessuno dei profili valutati, lo stato di conformità della condizione Else del profilo con priorità massima viene utilizzato per determinare lo stato e le azioni di conformità del tipo di profilo del criterio.
- **Use All Profiles:** sul computer vengono valutati tutti i profili del criterio appartenenti a una determinata tipologia e condotte le azioni di garanzia rivolte a tutti i profili. Il comportamento All utilizza il profilo **meno** conforme presente nel computer per determinare lo stato di conformità del tipo di profilo nel criterio. I profili delle patch vengono valutati in questo modo. I profili dell'applicazione che si desidera escludere dal computer possono essere valutati in questo modo.

**Importante:** per prima cosa è necessario aggiungere al criterio un profilo del sistema operativo per poi aggiungerne altri di diverso tipo. Al criterio è possibile aggiungere un numero illimitato di profili. Come minimo, almeno un profilo di sistema operativo deve essere aggiunto a un criterio. I criteri devono comprendere i profili di tutti i sistemi operativi che si desidera valutare nei computer.

8. Se necessario, cliccare su **Add Profiles** per aggiungere profili di altro tipo al criterio, cliccare sull'elenco **Profile Type** per selezionare il tipo di profilo, spuntare la casella accanto ai profili da aggiungere al criterio, quindi cliccare su **OK**.

Ripetere eventualmente questo passaggio per aggiungere altri profili al criterio.

9. Dopo aver selezionato un qualsiasi profilo di applicazione o patch, è possibile specificare i sistemi operativi nei quali l'applicazione o patch verrà valutata. Inoltre, se si selezionano più profili di applicazioni, ai fini della valutazione è possibile ordinarli per priorità. Deselezionare le caselle di spunta per i sistemi operativi nei quali non si desidera valutare le applicazioni o patch. Eventualmente, utilizzare le frecce per determinare la priorità delle valutazioni delle applicazioni. Le caselle in grigio indicano che la valutazione dell'applicazione in un particolare sistema operativo non è disponibile o supportata.

10. Cliccare su **Save**.

Una volta creato un criterio, assegnarlo al gruppo. A un gruppo può essere assegnato solo un criterio; al contrario, un singolo criterio può essere assegnato ad un numero illimitato di gruppi.

## 8.2 Creazione di un gruppo e assegnazione del relativo criterio

Creando un gruppo si stabilisce un nome che mappa un gruppo di utenti o di computer all'interno di un archivio utenti e si assegna un criterio a tale gruppo.

Ai gruppi devono essere assegnati dei criteri tali per cui i computer che si registrano a Sophos NAC Advanced possano essere verificati in base a un criterio di conformità. L'appartenenza a un gruppo viene determinata quando un computer accede a Sophos NAC Advanced utilizzando l'agente. Il criterio viene recuperato con la frequenza dell'intervallo di aggiornamento del criterio specificato.

È possibile assegnare un criterio a un gruppo quando si crea il gruppo oppure nell'elenco della pagina Groups. A un gruppo può essere assegnato solo un criterio; al contrario, un singolo criterio può essere assegnato ad un numero illimitato di gruppi. Una volta creati i gruppi, è possibile ordinarli per priorità nell'elenco della pagina Groups.

### Procedura

1. Accedere a Compliance Manager.
2. Cliccare su **Manage > Groups**. Quindi, cliccare su **Create Group** in basso a sinistra nella pagina.
3. Digitare un nome e una descrizione per il gruppo.

### Importante:

- Se si utilizza Sophos NAC Advanced come proxy RADIUS (configurando il software in modalità proxy in presenza di un altro server RADIUS), affinché l'utente riceva il criterio corretto il nome del gruppo deve corrispondere al valore generato dal server RADIUS. Se il nome del gruppo non corrisponde al valore del server RADIUS oppure nessun nome di gruppo viene generato dal server RADIUS, l'utente riceve il criterio predefinito, se ne è assegnato uno.
  - Se si utilizza Active Directory, il nome del gruppo deve corrispondere a quello di un gruppo di sicurezza nell'archivio utenti. Se il nome del gruppo non corrisponde a quello del gruppo di sicurezza nell'archivio utenti, l'utente riceve il criterio predefinito, se ne è assegnato uno.
4. Cliccare sull'elenco **Policy** per selezionare il criterio al quale il gruppo sarà associato.

**Importante:** se non viene selezionato nessun criterio e non viene assegnato un criterio predefinito, il computer non viene verificato ai fini della conformità. In questo caso, al computer viene assegnato il seguente modello di accesso. Si consiglia di assegnare sempre un criterio predefinito.

- **DHCP Enforcer:** al computer viene assegnato il modello di accesso di DHCP Enforcer associato allo stato di accesso Default, nell'area relativa a **Configure System > Enforcer Settings**.
5. Cliccare su **Save**.

**Importante:** una volta creati i gruppi, è possibile ordinarli per priorità nell'elenco della pagina Groups. Se a un particolare computer è associato più di un gruppo, viene utilizzato il primo di essi. Si consiglia di dare maggiore priorità ai gruppi più specifici/rigidi e di dare minore priorità a quelli meno specifici/rigidi.

## 8.3 Verifica delle impostazioni di Enforcer

La pagina Enforcer Settings di Compliance Manager consente di configurare le impostazioni che specificano la modalità di attuazione da parte di Sophos NAC Advanced. Verificare che le impostazioni predefinite siano adeguate all'implementazione di DHCP. Nella maggior parte dei casi, non sarà necessario apportare modifiche alle impostazioni di Enforcer.

### Procedura

1. Accedere a Compliance Manager.
2. Cliccare su **Configure System > Enforcer Settings**.
3. Non modificare i valori predefiniti in Policy Threshold Settings.
4. Non modificare i valori predefiniti in DHCP Enforcer Server Settings.
5. Cliccare sulla scheda **DHCP Enforcer**.
6. Verificare che i modelli di accesso siano corretti per ciascun stato di accesso. Sono disponibili i seguenti stati di accesso:
  - **Unknown Endpoint:** determina l'accesso alla rete in mancanza di dati sulla conformità. I computer sconosciuti sono non gestiti e non esenti. I modelli di accesso assegnati negano l'accesso alla rete ai computer sconosciuti.
  - **Maintenance Mode/Enforcer Override:** determina l'accesso alla rete quando il sistema si trova in modalità di manutenzione o l'attuazione in DHCP Enforcer è stata disabilitata tramite la casella Override Enforcers. Il modello di accesso assegnato consente ai computer di accedere alla rete.
  - **Default:** determina l'accesso alla rete nel caso in cui è stato designato un criterio predefinito o non è possibile trovare un modello di accesso associato. Il modello di accesso assegnato consente ai computer di accedere alla rete.
7. Per aggiungere o modificare i modelli di accesso per un determinato stato di accesso, cliccare su **Select**, spuntare le caselle accanto ai modelli e ai relativi stati di accesso e poi cliccare su **OK**.
8. Eventualmente, utilizzare le frecce per determinare la priorità dei modelli di accesso.

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

## 8.4 Esecuzione del report DHCP Enforcer

Prima di abilitare l'attuazione DHCP, eseguire il report DHCP Enforcer del Compliance Manager per determinare lo stato di conformità dei computer. Il report DHCP Enforcer è utilizzabile per stabilire se, una volta abilitata l'attuazione, verranno applicati i modelli di accesso corretti.

Il report DHCP Enforcer è utilizzabile sia con dati correnti che archiviati. Le impostazioni del server stabiliscono per quanto tempo i dati vengono tenuti correnti e quando vengono archiviati. Le impostazioni predefinite mantengono i dati correnti per due giorni e li archiviano

una volta al giorno. La data e ora dell'ultima archiviazione dei dati viene visualizzata accanto alla casella di spunta Use Data from Last Archive.

- **DHCP Enforcer:** questo report fornisce dettagli in merito allo stato di conformità dei computer, al modello di accesso associato e al motivo per cui un particolare modello di accesso è stato applicato. Prima di abilitare l'attuazione DHCP, dal report DHCP Enforcer è possibile accedere alla pagina Exemptions al fine di creare delle esenzioni per i computer che ne hanno bisogno.

**Nota:** in alcuni casi, per il fatto che i dati in tempo reale devono essere uniti da più fonti, i dati correnti possono essere incompleti.

### Procedura

1. Accedere a Compliance Manager.
2. Cliccare su **Report > Troubleshooting**.
3. Cliccare sull'elenco **Report Type** e selezionare **DHCP Enforcer**.
4. Se si desidera utilizzare dati archiviati, spuntare la casella **Use Data from Last Archive**.
5. 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 **Ordinamento personalizzato** per ampliare le opzioni di ordinamento; le opzioni di ordinamento personalizzato vengono modificate temporaneamente durante l'esecuzione del report.

Per ulteriori informazioni sugli specifici campi, v. la tabella Descrizioni dei campi.

**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.

6. 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 Compliance 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.

Campo	Descrizione
Compliance State	<p>Stato di conformità di un computer, assegnato durante la verifica della conformità. Stati di conformità disponibili:</p> <ul style="list-style-type: none"> <li>■ <b>Compliant:</b> la verifica ha stabilito che il computer è conforme al criterio. L'accesso alla rete è determinato dal modello di accesso di DHCP Enforcer conforme associato al criterio.</li> <li>■ <b>Partially Compliant:</b> la verifica ha stabilito che il computer è parzialmente conforme al criterio. L'accesso alla rete è determinato dal modello di accesso di DHCP Enforcer parzialmente conforme associato al criterio.</li> <li>■ <b>Non-Compliant:</b> la verifica ha stabilito che il computer non è conforme al criterio. L'accesso alla rete è determinato dal modello di accesso di DHCP Enforcer non conforme associato al criterio.</li> </ul> <p><b>Importante:</b> lo stato di conformità del computer viene determinato tramite la valutazione delle condizioni del profilo del computer stesso ed il comportamento del criterio assegnato a quel determinato profilo. Ogni stato di conformità della condizione viene innalzato a livello del profilo e i profili multipli vengono innalzati a livello del criterio per determinare, in questo modo, lo stato generale di conformità. Lo stato di conformità più basso indica lo stato di conformità generale. Una volta determinato lo stato di conformità, l'accesso alla rete basato sullo stato di conformità può essere garantito utilizzando i template di accesso assegnati dal criterio.</p>
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, insieme a modelli specifici dell'azienda.</p> <ul style="list-style-type: none"> <li>■ <b>Default - DHCP Deny (NULL User Class):</b> modello di accesso di DHCP Enforcer utilizzato per generare la classe di utente NULL e consentire l'accesso alla rete.</li> <li>■ <b>Default - DHCP Deny (NACDeny User Class):</b> modello di accesso di DHCP Enforcer utilizzato per generare la classe di utente NACDeny e negare l'accesso alla rete.</li> </ul>
Motivo	<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.</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 Enforcer nell'area <b>Configure System &gt; Enforcer Settings</b> è spuntata,</li> </ul>

Campo	Descrizione
	<p>l'accesso alla rete è determinato dai modelli di accesso Maintenance Mode/Enforcer Override, designati nella medesima area.</p> <ul style="list-style-type: none"> <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 di 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 nel Compliance Application Server 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.
Username	Nome utente della persona che ha tentato l'accesso alla rete.

Campo	Descrizione
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.
Exempt	Icona che dà accesso alla pagina Exemptions per creare un'esenzione basata sul criterio DHCP in questa voce del report. L'icona viene visualizzata solo se il motivo è diverso da Exempted.
<b>Voce del report dettagliato</b>	
Agent Enforcement Action	Azione intrapresa dal computer. Il computer inizia il rilascio e rinnovo degli indirizzi IP in base all'azione dell'Agent Enforcement specificata nel criterio. L'agente ottiene degli indirizzi IP nuovi al momento dell'avvio e inizia la verifica della conformità quando lo stato di conformità del computer e il modello di accesso di DHCP Enforcer definito nel criterio dell'utente cambiano. Valori disponibili: <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>Trattino triplo (---):</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.

## 8.5 Verifica dei modelli di accesso e abilitazione dell'attuazione DHCP

Per abilitare l'attuazione DHCP è necessario cambiare la modalità del criterio da Report Only a Enforce, nei criteri appropriati. Mentre si abilita l'attuazione, verificare che i modelli di accesso predefiniti assegnati siano adeguati per l'implementazione 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.

### Procedura

1. Accedere a Compliance Manager.
2. Cliccare su **Manage > Policies** . Quindi, cliccare sul nome del criterio che si desidera aggiornare.

3. Cliccare sull'elenco **Policy Mode** per modificare la modalità del criterio ed impostarla su Enforce. Sono disponibili le seguenti modalità:
  - **Report Only:** i computer vengono valutati in base ai profili nel criterio e, all'interno del Compliance Manager, viene generato un report informativo; tuttavia, nessun messaggio viene visualizzato, nessuna azione correttiva e di attuazione viene svolta nel computer. la modalità Report Only utilizza i modelli di accesso assegnati al punto 5.
  - **Remediate:** i computer vengono valutati in base ai profili nel criterio e, all'interno del Compliance Manager, viene generato un report informativo; tuttavia, nessun messaggio viene visualizzato, nessuna azione correttiva e di attuazione viene svolta nel computer. la modalità Remediate utilizza i modelli di accesso assegnati al punto 5.
  - **Enforce:** i computer vengono verificati in base ai profili inclusi nel criterio, le informazioni dei report sono generate nel Compliance Manager; sul computer vengono visualizzati messaggi, intraprese azioni correttive e i modelli di accesso vengono applicati agli appropriati stati di accesso o conformità. la modalità Enforce utilizza i modelli di accesso assegnati al punto 5.
  
4. Specificare le impostazioni di DHCP Agent.
  - **Agent Enforcement Action:** stabilisce il metodo utilizzato per ottenere i nuovi indirizzi IP per il computer. L'agente ottiene degli indirizzi IP nuovi al momento dell'avvio e inizia la verifica della conformità quando lo stato di conformità del computer e il modello di accesso di DHCP Enforcer definito nel criterio del computer cambiano. Valori disponibili:
    - **None:** gli indirizzi IP per il computer non sono né rilasciati né rinnovati. Selezionare **None** quando **non** si applica l'attuazione DHCP.
    - **Release Renew:** 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. Per l'attuazione DHCP, è **necessario** selezionare **Release Renew**.

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

**Nota:** per impostazione predefinita, ogni criterio viene automaticamente popolato con i modelli di accesso predefiniti. Assicurarsi che siano applicati i modelli di accesso corretti. Conservare le assegnazioni dei modelli di accesso Report Only e Remediate predefiniti. Le assegnazioni predefinite per Report Only e Remediate consentono l'accesso alla rete.

#### **Modelli di accesso predefiniti per DHCP Enforcer**

- **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 predefinito Default - DHCP Deny (NACDeny User Class) mette in quarantena il computer e consente l'accesso limitato alla rete quando si verifica un errore nel recupero di un criterio.
  - **Compliant:** il computer è conforme. Il modello di accesso predefinito Default - DHCP Permit (NULL User Class) consente l'accesso alla rete quando il computer è conforme.
  - **Partially Compliant:** il computer è parzialmente conforme. Il modello di accesso predefinito Default - DHCP Permit (NULL User Class) consente l'accesso alla rete quando il computer è parzialmente conforme.
  - **Non-Compliant:** il computer non è conforme. Il modello di accesso predefinito Default - DHCP Deny (NACDeny User Class) mette in quarantena il computer e consente l'accesso limitato alla rete quando il computer non è conforme.
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. Si 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**.

## 9 Supporto tecnico

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

- Visitando la community SophosTalk su <http://community.sophos.com/> e cercando altri utenti con lo stesso problema.
- Visitando la knowledge base del supporto Sophos su <http://www.sophos.com/support/>.
- Scaricando la documentazione del prodotto su <http://www.sophos.com/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 Limited. Tutti i diritti riservati. Nessuna parte di questa pubblicazione può essere riprodotta, memorizzata in un sistema di recupero informazioni, o trasmessa, in qualsiasi forma o con qualsiasi mezzo, elettronico o meccanico, inclusi le fotocopie, la 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.

Sophos e Sophos Anti-Virus sono marchi registrati di Sophos Limited. Tutti gli altri nomi citati di società e prodotti sono marchi o marchi registrati dei rispettivi titolari.