

Sophos NAC Manager Guida in linea

Versione prodotto: 3.9

Data documento: dicembre 2011



Sommario

- 1 Panoramica di NAC Manager.....3
- 2 Panoramica dell'area Manage.....12
- 3 Panoramica dell'area Enforce.....43
- 4 Panoramica dell'area Report.....56
- 5 Panoramica dell'area Configure System.....75
- 6 Tool di log.....82
- 7 Tool della modalità di manutenzione86
- 8 Glossario.....88
- 9 Supporto tecnico.....94
- 10 Note legali.....95

1 Panoramica di NAC Manager

Questa della Guida in linea fornisce istruzioni e informazioni su come utilizzare NAC Manager.

Restrizione: L'utilizzo dei pulsanti del browser web per navigare in NAC Manager **non** è supportato. La navigazione e le diverse funzioni devono essere svolte utilizzando le voci del menu, i collegamenti e i pulsanti a disposizione in ciascuna pagina.

1.1 Distribuzione di Network Access Control

Questa sezione fornisce le migliori pratiche per l'utilizzo di Network Access Control.

Processi	Passaggi
Utilizzare Sophos Enterprise Console per proteggere i computer con Sophos NAC.	<ol style="list-style-type: none"> Da Sophos Enterprise Console, eseguire la procedura guidata Protezione dei computer.
Controllare i report di NAC Manager per stabilire lo stato di conformità corrente.	<ol style="list-style-type: none"> Utilizzare i report in NAC Manager per stabilire lo stato di conformità degli utenti. Nota: I report di NAC Manager offrono una rappresentazione realistica di quanto gli utenti siano conformi al criterio Managed. Utilizzare i report in NAC Manager per stabilire se i messaggi ricevuti dagli utenti sono appropriati. Nota: Finché la modalità del criterio non viene cambiata in Remediate o Enforce, gli utenti non visualizzano i messaggi. Questa operazione viene descritta nei passaggi di seguito.
Se necessario, aggiornare i profili di NAC Manager .	<ol style="list-style-type: none"> Aggiornare Sophos Anti-Virus e/o i profili di Sophos Client Firewall. Verificare che comprendano i corretti sistemi operativi, messaggi e azioni correttive. Utilizzare i report in NAC Manager per stabilire se gli aggiornamenti dei profili sono appropriati.
Implementare il criterio di correzione.	<ol style="list-style-type: none"> Aggiornare il criterio Managed. Cambiare la modalità del criterio da Report Only a Remediation. Utilizzare i report in NAC Manager per stabilire lo stato di conformità corrente. Nota: Col passare del tempo, i computer non conformi o parzialmente conformi ricevono azioni correttive per diventare conformi.

Processi	Passaggi
Se necessario creare o aggiornare i modelli di accesso.	<ol style="list-style-type: none"> 1. Creare o aggiornare i modelli di accesso. Nota: Se si desidera attuare l'accesso alla rete tramite l'agente, creare o aggiornare i modelli di accesso di Agent Enforcer. Se si desidera attuare l'accesso alla rete tramite l'attuazione DHCP, creare o aggiornare i modelli di accesso di DHCP Enforcer. Per ulteriori informazioni, consultare la sezione Migliori pratiche relative ai modelli di accesso a pagina 44. 2. Utilizzare i report in NAC Manager per stabilire se i modelli di accesso forniscano a tutti i computer un corretto accesso alla rete.
Implementare il criterio di attuazione.	<ol style="list-style-type: none"> 1. Aggiornare il criterio Managed. Cambiare la modalità del criterio da Remediation a Enforce. 2. Utilizzare i report in NAC Manager per stabilire lo stato di conformità corrente. Nota: Col passare del tempo, i computer che non sono conformi devono essere corretti; in caso contrario a tali utenti verrà negato l'accesso alla rete.

1.2 Nome e password dell'account di NAC Manager

Per accedere a NAC Manager sono necessari un nome account ed una password.

Per accedere per la prima volta a NAC Manager, utilizzare i seguenti nome account e password:

- **Nome account** = admin
- **Password** = una password a scelta

La prima volta che si accede a NAC Manager verrà richiesto di cambiare la password. Memorizzare questa password dal momento che rappresenta l'unico accesso a NAC Manager finché non vengono creati altri account utente. Per ulteriori informazioni, consultare la sezione [Creazione degli account](#) a pagina 76.

1.3 Visualizzazione della home page










I seguenti comandi sono disponibili nella home page.

















- **Current Compliance:** Rappresentazione grafica degli stati di conformità correnti per tutti gli agenti del computer riportati negli ultimi sette giorni. Per ulteriori informazioni, consultare la sezione [Esecuzione di report Compliance](#) a pagina 57.
- **Compliance Trend:** Rappresentazione grafica degli stati di conformità negli ultimi sette giorni. Per ulteriori informazioni, consultare la sezione [Esecuzione di report Compliance](#) a pagina 57.















- **Server Task Status:** Stato di ogni operazione del loader ordinata per server. Se un'operazione non è riuscita, cliccare sul collegamento **Error** per visualizzare informazioni dettagliate sull'errore. Operazioni del loader:
 - **Current Definition Loader:** recupera da Sophos le date più recenti delle firme per le applicazioni antivirus e antispyware.
 - **Report Warehouse Loader:** controlla quando vengono eliminati i dati dei report.

1.4 Icone di NAC Manager

In NAC Manager, le icone rappresentano una possibile azione o indicano un significato. Per ulteriori informazioni sull'utilizzo e il significato di tutte le icone, consultare la tabella Icone e descrizioni.

Icona	Descrizione
Funzioni comuni	
	Aumenta il livello di priorità di un elemento della lista.
	Diminuisce il livello di priorità di un elemento della lista.
	Cancella un elemento. È necessario confermare la cancellazione degli elementi di una lista, quali profili. Non è invece necessario confermare la cancellazione delle impostazioni di un elemento, quali le sue funzioni.
	Contrassegna un elemento o una procedura come obbligatorio; ciò significa che tale procedura deve essere completata prima di poter passare ad un'altra o salvare i dati contenuti in quella determinata pagina.
	Indica che un elemento non è bloccato. Se si clicca sull'icona l'elemento viene bloccato. Gli amministratori e gli amministratori di sistema possono bloccare gli elementi.
	Indica che un elemento è bloccato. Se si clicca sull'icona l'elemento verrà sbloccato. Gli amministratori di sistema possono sbloccare tutti gli elementi. Gli amministratori possono sbloccare solo gli elementi che hanno personalmente bloccato.
	Indica che un elemento è bloccato e non può essere sbloccato dall'utente corrente dell'account, per es. le risorse di rete personalizzate bloccate da un altro utente dell'account.
	Indica la presenza di un errore nella pagina che deve essere corretto prima di passare ad un'altra procedura o di salvare i dati contenuti in quella determinata pagina.
	Indica la presenza di un messaggio informativo che conferma la corretta esecuzione o il salvataggio di una procedura.

Icona	Descrizione
	Indica la presenza di un collegamento esterno a NAC Manager.
	Rappresenta un elemento predefinito che non può essere modificato, per esempio un'applicazione o risorsa di rete standard. È tuttavia possibile salvare un elemento standard come nuovo per poterlo modificare.
Stati di conformità del modello	
	Indica che il modello di accesso viene utilizzato per i computer conformi.
	Indica che il modello di accesso viene utilizzato per i computer parzialmente conformi.
	Indica che il modello di accesso viene utilizzato per i computer non conformi.
Account	
	Indica che un account è attivo. Cliccando sull'icona è possibile disattivare l'account.
	Indica che un account è inattivo. Cliccando sull'icona è possibile attivare l'account.
Profili e criteri	
	Indica che un profilo, un'applicazione, o una funzione sono supportati nel Quarantine Agent.
	Indica che un profilo, un'applicazione, o una funzione sono supportati nel Dissolvable Agent.
	Indica che un profilo, un'applicazione, o una funzione sono supportati da Windows 7.
	Indica che un profilo, un'applicazione, o una funzione sono supportati da Windows Vista.
	Indica che un profilo, un'applicazione, o una funzione sono supportati da Windows XP.
	Indica che un profilo, un'applicazione, o una funzione sono supportati su Windows 2000.
	Indica che un profilo, un'applicazione, o una funzione sono supportati da Windows 2008.
	Indica che un profilo, un'applicazione, o una funzione sono supportati da Windows Server 2003.
	Indica che un'azione correttiva non è supportata da determinati sistemi operativi. Clicca l'icona per visualizzare i sistemi operativi non supportati.

Icona	Descrizione
	Indica che, sebbene questa funzione sia supportata da Windows 7, l'azione correttiva associata non lo è.
	Indica che, sebbene questa funzione sia supportata da Windows Vista, l'azione correttiva associata non lo è.
	Indica che, sebbene questa funzione sia supportata da Windows XP, l'azione correttiva associata non lo è.
	Indica che, sebbene questa funzione sia supportata da Windows 2000, l'azione correttiva associata non lo è.
	Indica che, sebbene questa funzione sia supportata da Windows Server 2008, l'azione correttiva associata non lo è.
	Indica che, sebbene questa funzione sia supportata da Windows Server 2003, l'azione correttiva associata non lo è.
Profili delle applicazioni	
	Indica che un messaggio è stato identificato relativo alla condizione. Il messaggio viene visualizzato nel computer solo se la condizione viene soddisfatta.
Esenzioni	
	Rappresenta un indirizzo MAC nell'esenzione DHCP.
	Rappresenta una classe fornitore nell'esenzione DHCP.
	Rappresenta una classe utente nell'esenzione DHCP.
	Rappresenta un ambito IP nell'esenzione DHCP.
Report	
	Accede al record del report di Agent Enforcer associato alla voce selezionata del report relativa a Agent Session.
	Accede al record del report di DHCP Enforcer associato alla voce selezionata del report relativa a Agent Session.
	Accede ai dati relativi alla verifica della conformità associati a una determinata voce del report relativa a Compliance Detail, Agent Session o Non-Compliance Detail.

1.5 Quando utilizzare la funzione Save As New

Questa sezione descrive le migliori pratiche per l'utilizzo del pulsante Save As New.

Migliore pratica	Descrizione
Utilizzare la funzione Save As New per salvare un profilo o modello di accesso esistente con un nuovo nome e aggiornarlo.	La funzione Save as new permette di duplicare un profilo o modello di accesso senza alterarlo.
Utilizzare la funzione Save as New per aggiornare un profilo o un modello di accesso già applicato ai criteri, a meno che non si desideri che le modifiche siano immediatamente efficaci.	Se si aggiorna un profilo o modello di accesso esistente che è già applicato ai criteri, le modifiche sono immediatamente efficaci e vengono applicate durante il successivo recupero del criterio da parte dell'agente. Utilizzare pertanto la funzione Save As New a meno che non si desideri che le modifiche siano immediatamente efficaci.

1.6 Salvataggio di un oggetto come nuovo oggetto in NAC Manager

È possibile salvare un oggetto come nuovo per poterne riutilizzare le impostazioni esistenti.

Si consiglia di salvare l'elemento come nuovo prima di aggiornarne le impostazioni. Gli elementi che possono essere salvati come nuovi sono: modelli di configurazione dell'agente, profili, modelli di accesso, risorse di rete ed esenzioni.

Procedura

1. Cliccare sul nome dell'area appropriato: **Manage**, **Enforce** o **Configure System**.
2. Cliccare sul nome dell'area dell'oggetto che si desidera riutilizzare.
3. Cliccare sul nome dell'oggetto nell'elenco.
4. Cliccare su **Save As New**. Nella finestra di dialogo, digitare un nuovo nome per l'oggetto, quindi cliccare su **OK**.

Per informazioni sulla creazione o l'aggiornamento delle impostazioni di un oggetto, v. l'argomento *Creating* appropriato.

1.7 Visualizzazione o ricerca di oggetti elencati in NAC Manager

In NAC Manager, è possibile visualizzare una lista di elementi o ricercarne degli specifici.

In ogni area di NAC Manager, è possibile visualizzare la lista di elementi creati o aggiunti, avere accesso ai dati relativi ad uno di essi, aggiornare o cancellare un elemento. È inoltre possibile, utilizzando le opzioni di ricerca presenti in aree specifiche, accorciare liste potenzialmente molto estese.

Procedura

1. Cliccare sul nome dell'area appropriato: **Manage**, **Enforce** o **Configure System**.
2. Cliccare sul nome dell'area degli oggetti che si desidera visualizzare.

Nota: Perché tutti i nomi delle applicazioni vengano visualizzati correttamente nell'elenco della pagina **Applications**, è necessario installare i file per il supporto delle lingue orientali (tramite **Pannello di controllo > Opzioni internazionali e della lingua**) nel computer in cui si visualizza NAC Manager.

- Se ci si trova in **Manage > Profiles or Applications**, si possono cercare oggetti specifici nell'elenco tramite l'operazione Search Criteria. Digitare o selezionare le opzioni di ricerca appropriate e cliccare su **Search**.

Nota: i valori di ricerca per gli oggetti degli elenchi **non** corrispondono precisamente e **non** distinguono fra maiuscole e minuscole. Inoltre, nella maggior parte dei campi è possibile utilizzare i simboli * e % per eseguire le ricerche con i caratteri jolly. Per esempio, se si digita M% nel campo Name, vengono visualizzati tutti i nomi che iniziano con la lettera M. Se invece si specifica M senza il carattere %, verranno visualizzati solo i nomi come M.

- Effettuare una delle seguenti operazioni:
 - Per ordinare l'elenco, cliccare sull'intestazione di colonna appropriata.
 - Per visualizzare i dati relativi a un oggetto o per aggiornarlo, cliccare sul nome dell'oggetto.
 - Per cancellare un oggetto, spuntare la casella accanto a ogni oggetto che si desidera cancellare e cliccare su **Delete**. Nella finestra di dialogo, confermare l'elenco di oggetti da cancellare e cliccare su **OK**.

1.8 Cancellazione di oggetti in NAC Manager

In NAC Manager, la cancellazione di alcuni elementi implica la loro completa rimozione dal software. Possono essere cancellati solo gli oggetti non utilizzati da altri componenti. Non è possibile, per esempio, cancellare una risorsa di rete che faccia parte del modello di accesso di Agent Enforcer. È inoltre possibile utilizzare l'icona cestino per cancellare gli oggetti di una pagina.

Procedura

- Cliccare sul nome dell'area appropriato: **Manage**, **Enforce** o **Configure System**.
- Cliccare sul nome dell'area dell'oggetto che si desidera cancellare.
- Spuntare la casella accanto a ogni oggetto che si desidera cancellare.
- Cliccare su **Delete**.
- Nella finestra di dialogo, cliccare su **OK** per confermare la cancellazione.

1.9 Quando utilizzare la funzione Lock

Questa sezione descrive le migliori pratiche per l'utilizzo della funzione Lock.

Migliore pratica	Descrizione
Blocco di criteri, profili, modelli di accesso e risorse di rete per prevenire modifiche accidentali.	<p>Il blocco di questi elementi di NAC Manager ne previene la modifica accidentale. Gli amministratori possono sbloccare solo gli elementi che hanno personalmente bloccato. Gli amministratori di sistema possono sbloccare tutti gli elementi.</p> <p>Nota: Per garantire la protezione di un intero criterio, è necessario bloccare tutti i profili, i modelli di accesso e le risorse di rete legati al criterio, oltre che il criterio stesso.</p>

1.10 Blocco e sblocco di oggetti in NAC Manager

Il blocco di un elemento del software impedisce che altri amministratori ne eseguano l'aggiornamento.

Gli amministratori di sistema possono sbloccare tutti gli elementi. Gli amministratori possono sbloccare solo gli elementi che hanno personalmente bloccato.

Procedura

1. Cliccare sul nome dell'area appropriato: **Manage**, **Enforce** o **Configure System**.
2. Cliccare sul nome dell'area degli oggetti che si desidera bloccare o sbloccare.
3. Cliccare sull'icona **Lock** o **Unlock** accanto all'oggetto che si desidera bloccare o sbloccare.

L'icona visualizza lo stato corrente.

Nota: Alcuni oggetti standard, come applicazioni e risorse di rete, non possono essere bloccati e sbloccati.

1.11 Utilizzo delle funzioni del tasto destro del mouse in NAC Manager

Le funzioni che compaiono cliccando col tasto destro del mouse sono disponibili in tutte le pagine degli elenchi e in altre aree.

Procedura

1. Cliccare sul nome dell'area appropriato: **Manage**, **Enforce** o **Configure System**.
2. Cliccare sul nome dell'area dell'oggetto che si desidera gestire.
3. Cliccare con il tasto destro del mouse sul nome del collegamento e selezionare la funzione appropriata. Per informazioni su aree e funzioni, consultare la tabella Funzioni del tasto destro del mouse.

Funzioni del tasto destro del mouse

Area NAC Manager	Descrizione
Funzioni standard per tutte le aree	Tutte le pagine con elenchi includono le seguenti funzioni standard: Edit, View (a disposizione di oggetti standard che non possono essere modificati), Copy, Rename, Delete, Lock/Unlock e View Audit Data. Nota: alcune funzioni possono non essere disponibili per tutte le voci di un elenco.
Agent Configuration Templates, Profiles, Applications, Agent Enforcer Access Templates, DHCP Enforcer Access Templates e Network Resources list pages	Specifiche pagine con elenchi presentano tutte le funzioni standard e in più View Usage Details, che visualizza i dati relativi a criteri, profili o modelli di accesso in cui è incluso l'oggetto selezionato.

Area NAC Manager	Descrizione
Elenco pagina Accounts	La pagina Accounts presenta tutte le funzioni standard, eccetto Copy e Lock/Unlock, oltre che Enable/Disable.

2 Panoramica dell'area Manage

L'area di gestione include tutti i componenti richiesti per la gestione dei criteri. Dal menu Manage è possibile accedere alle seguenti aree:

Area e azione	Descrizione
Applicazioni	
Utilizzare tipi di applicazione standard.	I tipi di applicazione categorizzano le applicazioni e stabiliscono i comportamenti dei criteri predefiniti per tutte le applicazioni associate a un determinato tipo. I tipi di applicazioni standard sono già presenti nel software.
Utilizzare le applicazioni standard.	Le applicazioni sono le applicazioni del software supportate da Sophos NAC. Le applicazioni standard sono già presenti nel software. Sono legate a un determinato tipo di applicazione, che stabilisce come debbano essere valutate quando il loro profilo viene aggiunto a un criterio.
Agent configuration templates	
Creare i modelli di configurazione dell'agente.	Modelli di configurazione dell'agente definiscono le impostazioni opzionali che controllano il funzionamento dell'agente nel computer.
Profiles	
Creare profili per sistemi operativi, patch, e/o applicazioni, oppure utilizzare i profili campione predefiniti nel sistema.	<p>I profili consentono di definire quali elementi dei computer devono essere valutati (per es. sistemi operativi e applicazioni). Una volta creati possono essere organizzati e ordinati per priorità all'interno dei criteri.</p> <p>Consigli</p> <ul style="list-style-type: none"> ■ Utilizzare come riferimento i profili predefiniti. È possibile salvare come nuovi i profili predefiniti per personalizzarne i messaggi, aggiungere altre condizioni, modificare gli stati di conformità, attivare azioni correttive ecc., o più semplicemente utilizzare tali profili come modello per crearne di nuovi. ■ Utilizzare i profili predefiniti di Patch Manager per supportare la verifica della patch per computer gestiti e non. Per ulteriori informazioni, consultare la sezione Utilizzo dei profili predefiniti di Patch Manager a pagina 28.
Criteri	
Aggiornare i criteri.	<p>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.</p> <p>Consigli</p> <ul style="list-style-type: none"> ■ Al criterio è possibile aggiungere un numero illimitato di profili. ■ In un criterio deve essere incluso almeno un profilo di sistema operativo.

Area e azione	Descrizione
	<ul style="list-style-type: none"> ■ I criteri devono comprendere i profili di tutti i sistemi operativi che si desidera valutare nei computer. ■ Utilizzare i criteri predefiniti per supportare la conformità ai criteri di protezione per computer gestiti e non. Per ulteriori informazioni, consultare la sezione Utilizzo dei criteri predefiniti a pagina 15.

2.1 Migliori pratiche relative ai criteri

Questa sezione fornisce le migliori pratiche relative ai criteri.

Specificazione della modalità del criterio appropriata

Importante: È necessario verificare che al criterio siano associati gli adeguati modelli di accesso per le modalità Report Only e Remediate. se si applica un modello di accesso di Enforcer che impedisce l'accesso alla rete nelle modalità Report Only o Remediate, a tutti i computer verrà negato l'accesso a prescindere dal loro effettivo stato di conformità. Per attuare uno stato di conformità, è necessario modificare la modalità del criterio e selezionare Enforce.

Migliore pratica	Descrizione
Utilizzare la modalità Report Only per verificare il livello di conformità aziendale.	La modalità Report Only consente di raccogliere informazioni sullo stato di conformità aziendale da inserire nei report. Questa modalità è la meno intrusiva per gli utenti.
Utilizzare la modalità Remediate per generare report relativi agli utenti ed eseguire azioni correttive per renderli conformi ai criteri definiti.	La modalità Remediate fornisce alle imprese la possibilità di generare report relativi agli utenti ed eseguire azioni correttive per renderli conformi ai criteri definiti. Questa modalità consente inoltre di ottenere la conformità al criterio prima di avviare l'attuazione.
Utilizzare la modalità Enforce per generare report, svolgere azioni correttive e attuare la conformità della rete. Se gli utenti non sono conformi al criterio, viene loro negato l'accesso alla rete.	La modalità Enforce fornisce alle aziende la possibilità di generare report, svolgere azioni correttive e attuare la conformità della rete. L'accesso alla rete è determinato dai modelli di accesso (Agent e/o DHCP) selezionati. Se più di un modello di accesso è applicabile a un particolare stato, viene utilizzato il primo modello che soddisfa tale stato.

Utilizzo di Quarantine Override quando l'accesso alla rete è imperativo

Migliore pratica	Descrizione
Impostare quarantine override su true solo quando l'accesso alla rete è indispensabile per il lavoro e i	Impostando quarantine override su true gli utenti possono rimuovere il computer dalla quarantena anche se il computer non è conforme.

Migliore pratica	Descrizione
rischi per la sicurezza sono minimi o inesistenti.	

Mantenimento dei soli criteri contenenti profili necessari

Migliore pratica	Descrizione
Mantenere solo i criteri che contengono profili necessari. Rimuovere i profili scaduti da tutti i criteri.	Mantenere solo i criteri che comprendono i profili antivirus, firewall, antispyware, e dei sistemi operativi necessari, in modo tale da semplificarne la manutenzione e il supporto.

Aggiunta e diversificazione della priorità dei profili nei criteri

Migliore pratica	Descrizione
Aggiungere al criterio i profili dei sistemi operativi , quindi ordinarli per priorità.	<p>I criteri devono comprendere i profili di tutti i sistemi operativi che si desidera valutare. Dare la priorità ai sistemi operativi più importanti.</p> <p>Se uno di questi sistemi non è installato nel computer, per determinare lo stato di conformità e le azioni viene utilizzato il profilo del sistema operativo a più alta priorità, e per tale criterio non vengono valutati altri profili.</p> <p>Per esempio, se Windows XP e Windows 2000 sono sistemi operativi necessari e Windows XP è quello preferito, aggiungere al criterio entrambi i profili dando priorità maggiore a Windows XP e assicurarsi che la condizione Else nel profilo di Windows XP sia impostata su Non-Compliant e includa un messaggio per gli utenti non conformi. In questo scenario, se il computer non ha uno dei sistemi operativi necessari installato risulta non conforme, un messaggio viene visualizzato all'utente e non vengono valutati altri profili del criterio.</p>
Aggiungere al criterio i profili delle applicazioni appropriate, quindi ordinarli per priorità.	Per esempio, se un criterio contiene più di un profilo antivirus, dare priorità al profilo più importante.

Verifica del modello di accesso assegnato al criterio

Migliore pratica	Descrizione
Cancellare da tutti i criteri i modelli di accesso scaduti o inutilizzati.	Mantenere solo i criteri che contengono i modelli di accesso relativi ai tipi di attuazione implementati. Questa migliore pratica semplifica la risoluzione dei problemi di accesso alla rete, a prescindere dalla modalità del criterio.
Verificare che al criterio siano assegnati gli adeguati modelli di accesso.	<p>Per impostazione predefinita, ogni criterio viene automaticamente popolato con i modelli di accesso. Assicurarsi che a ciascuno stato di accesso siano applicati i modelli di accesso corretti.</p> <p>Se necessario, modificare l'ordine di priorità o cancellare i modelli di accesso presenti nel criterio. Se più di un modello è applicabile a un particolare stato, viene utilizzato il primo modello che soddisfa tale stato.</p> <p>Importante:</p> <ul style="list-style-type: none"> ■ se si applica un modello di accesso di Enforcer che impedisce l'accesso alla rete nelle modalità Report Only o Remediate, a tutti i computer verrà negato l'accesso a prescindere dal loro effettivo stato di conformità. Per attuare uno stato di conformità, è necessario modificare la modalità del criterio e selezionare Enforce. ■ Se si cancellano i modelli di accesso di Agent Enforcer da un particolare stato di accesso, per quello stato viene consentito tutto il traffico in uscita.

2.2 Utilizzo dei criteri predefiniti

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

Durante la verifica della conformità del computer, l'agente recupererà il criterio relativo al gruppo a cui appartiene il computer stesso in Sophos Enterprise Console. Per ulteriori informazioni, consultare la sezione [Aggiornamento dei criteri](#) a pagina 16.

- **Default:** questo criterio viene utilizzato se in un computer è installato Sophos 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 viene utilizzato per i computer gestiti con Sophos Enterprise Console che hanno Sophos 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 agente installato e non utilizza Dissolvable Agent, l'accesso alla rete sarà determinato dalle impostazioni di Enforcer. Per ulteriori informazioni, consultare la sezione [Specificazione delle impostazioni di Enforcer](#) a pagina 77.

2.3 Aggiornamento dei criteri

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.

Importante: tutti i criteri e le modifiche agli stessi hanno effetto immediato nella rete; tuttavia un criterio non viene applicato in un computer finché l'agente non lo recupera.

Procedura

1. Cliccare su **Manage > Policies** . Quindi, cliccare sul nome del criterio che si desidera aggiornare. Per ulteriori informazioni sui criteri predefiniti, consultare la sezione [Utilizzo dei criteri predefiniti](#) a pagina 15.
2. Cliccare sull'elenco **Policy Mode** per scegliere la modalità del criterio.
Le modalità del criterio determinano quali modelli di accesso utilizzare durante la verifica della conformità. Le modalità del criterio possono essere Report Only, Remediate e Enforce. Per ulteriori informazioni, consultare la sezione [Glossario](#) a pagina 88.
3. Nell'area di navigazione Agent a sinistra, cliccare su **Settings**.
4. Se applicabili, specificare le impostazioni del Continuous Agent. Queste impostazioni sono valide solo per i computer che eseguono il Quarantine Agent:
 - **Policy Refresh Interval:** specifica la frequenza di recupero del criterio da parte dell'agente. Il valore predefinito è 4 ore.
 - **Assess and Enforce Interval:** specifica la frequenza con cui l'agente verifica la conformità del computer. Il valore predefinito è 4 ore.
 - **Report Interval:** specifica la frequenza con cui l'agente invia i dati del report al server. Il valore predefinito è 8 ore.
5. Se applicabile, selezionare il modello di configurazione dell'agente nella sezione Configuration.
Se non è stato selezionato alcun modello di configurazione, l'agente utilizzerà le impostazioni predefinite. Queste impostazioni sono valide solo per i computer che eseguono il Quarantine Agent. Per ulteriori informazioni, consultare le sezioni [Creazione dei modelli di configurazione dell'agente](#) a pagina 20 e [Impostazioni dell'agente](#) a pagina 20.
6. Se applicabili, specificare le impostazioni del Quarantine Agent. Queste impostazioni sono valide solo per i computer che eseguono il Quarantine Agent:
 - **Quarantine Override:** specifica se l'utente può ignorare la quarantena nel computer. Se il Quarantine override è impostato su True, allora l'utente può ignorare la quarantena dell'agente. Questa opzione consente agli utenti di rimuovere un computer dalla quarantena anche se non conforme. Se l'override è impostato su False, l'utente non può ignorare la quarantena dell'agente ed il computer resta in quarantena finché non conforme al criterio.

7. Se applicabili, specificare le impostazioni del 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 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. Quando si utilizza l'attuazione DHCP, è **necessario** selezionare Release Renew.

Nota: se un computer utilizza il Dissolvable Agent in Windows Vista o Windows 7 e deve rilasciare/rinnovare i suoi indirizzi IP, l'agente visualizzerà un messaggio per l'utente, richiedendo le credenziali di amministrazione oppure il riavvio del computer.
8. Effettuare una delle seguenti operazioni:
 - Per aggiungere profili al criterio, cliccare su **Add Profiles** in basso a sinistra nella pagina, cliccare sull'elenco **Profile Type** per selezionare il tipo di profilo, spuntare le caselle accanto ai profili che si desidera aggiungere al criteri e cliccare su **OK**. Ripetere eventualmente questo passaggio per aggiungere altri profili al criterio.

Importante: Al criterio è possibile aggiungere un numero illimitato di profili. In un criterio deve essere incluso almeno un profilo del sistema operativo. I criteri devono comprendere i profili di tutti i sistemi operativi che si desidera valutare nei computer.
 - Per rimuovere i profili dal criterio, cliccare sull'adeguato tipo di profilo nell'area di navigazione Profiles a sinistra, quindi cliccare sull'icona **cestino** accanto ai rispettivi profili, per rimuoverli dal criterio.
9. Se si possiedono più profili di sistema operativo, è possibile dare loro differenti priorità ai fini della valutazione.

I comportamenti dei criteri possono essere Required, Best e All. Per ulteriori informazioni, consultare la sezione [Glossario](#) a pagina 88.

10. Nell'area di navigazione Network Access a sinistra, cliccare sul tipo di attuazione per il quale si desidera verificare o modificare i modelli di accesso. Per aggiungere i modelli di accesso relativi a un particolare stato di accesso, cliccare sulla scheda della modalità del criterio appropriata, cliccare su **Select**, selezionare i modelli di accesso e agli stati di accesso cui si applicano i modelli e cliccare su **OK**. È possibile anche uscire o cancellare il modello di accesso corrente.

A seconda della configurazione di rete, può essere necessario specificare più di un tipo di attuazione. Per ulteriori informazioni sui tipi di attuazione, consultare la sezione [Modalità e stati di accesso di un criterio](#) a pagina 18.

Nota: per impostazione predefinita, tutti i criteri vengono popolati automaticamente con i modelli di accesso corrispondenti a ciascuno stato di accesso, in base ai modelli di accesso predefiniti in NAC Manager e ai relativi modelli di conformità. Assicurarsi che a ciascuno stato di accesso siano applicati i modelli di accesso corretti. È inoltre possibile aggiornare le impostazioni dei modelli di accesso predefiniti o creare nuovi modelli di accesso e aggiungerli ai criteri, in alternativa ai modelli di accesso predefiniti. Si osservi che se si rimuovono tutti i modelli di accesso di Agent Enforcer da un determinato stato di accesso, viene consentito tutto il traffico in uscita. per ulteriori informazioni, consultare le sezioni [Creazione dei modelli di accesso di Agent Enforcer](#) a pagina 46 e [Creazione dei modelli di accesso di DHCP Enforcer](#) a pagina 47.

11. 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.

12. Cliccare su **Save**.

2.4 Modalità e stati di accesso di un criterio

La seguente tabella indica gli stati di accesso a disposizione di ciascuna modalità di un criterio, ordinati per tipo di attuazione.

Per ulteriori informazioni, consultare la sezione [Aggiornamento dei criteri](#) a pagina 16.

Modalità del criterio	Descrizione e stati di accesso
Report Only	<p>I computer vengono valutati in base al criterio e, all'interno di NAC Manager, viene generato un report informativo. Non viene visualizzato nessun messaggio e non viene intrapresa alcuna azione correttiva e di attuazione. Selezionare il modello di accesso di Enforcer che consente l'accesso al traffico proveniente dal computer.</p> <p>Importante: se si applica un modello di accesso di Enforcer che impedisce l'accesso alla rete nelle modalità Report Only o Remediate, a tutti i computer verrà negato l'accesso a prescindere dal loro effettivo stato di conformità. Per attuare uno stato di conformità, è necessario modificare la modalità del criterio e selezionare Enforce.</p>

Modalità del criterio	Descrizione e stati di accesso
Remediate	<p>I computer vengono valutati in base al criterio e, all'interno del NAC Manager, viene generato un report informativo. I messaggi vengono visualizzati e vengono intraprese azioni correttive; non viene tuttavia svolta alcuna azione di attuazione. Selezionare il modello di accesso di Enforcer che consente l'accesso al traffico proveniente dal computer.</p> <p>Importante: se si applica un modello di accesso di Enforcer che impedisce l'accesso alla rete nelle modalità Report Only o Remediate, a tutti i computer verrà negato l'accesso a prescindere dal loro effettivo stato di conformità. Per attuare uno stato di conformità, è necessario modificare la modalità del criterio e selezionare Enforce.</p>
Enforce	<p>I computer vengono valutati in base al criterio e, all'interno del 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. Quando il computer si trova in uno dei seguenti stati nel criterio assegnato, i modelli di accesso associati a quello stato determinano l'accesso alla rete.</p> <p>Stati dell'agente:</p> <ul style="list-style-type: none"> ■ No Agent Tray: l'agente non è attualmente in esecuzione nel computer. Questo stato viene segnalato da Agent Enforcer nel caso in cui l'utente non sia connesso a Windows oppure l'applicazione dell'agente nell'area di notifica non sia più in esecuzione. ■ User Override: nel computer, l'utente ha ignorato la quarantena dell'agente. ■ Policy Retrieval Error: non è stato possibile recuperare un criterio per il computer. Questo stato può esistere se l'agente non riesce a recuperare il criterio da NAC Server; oppure lo stato di conformità del computer non è aggiornato secondo il campo Agent Policy Update Threshold configurato nell'area Configure System > Enforcer Settings . <p>Enforcer State:</p> <ul style="list-style-type: none"> ■ 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 . <p>Stati di conformità:</p> <ul style="list-style-type: none"> ■ Compliant: la verifica ha stabilito che il computer è conforme al criterio. ■ Partially Compliant: la verifica ha stabilito che il computer è parzialmente conforme al criterio. ■ Non-Compliant: la verifica ha stabilito che il computer non è conforme al criterio.

2.5 Creazione dei modelli di configurazione dell'agente

I modelli di configurazione dell'agente consentono agli amministratori di definire le impostazioni opzionali che controllano il funzionamento dell'agente nel computer. I modelli di accesso di Agent Enforcer vengono applicati solo ai computer che utilizzano il Quarantine Agent.

Una volta creati i modelli di configurazione dell'agente, è possibile aggiungerli ai criteri. Gli agenti sono così in grado, durante la successiva verifica, di recuperare il criterio assegnato e di applicare contestualmente le impostazioni al computer. Per ulteriori informazioni, consultare la sezione [Aggiornamento dei criteri](#) a pagina 16.

Procedura

1. Cliccare su **Manage > Agent Configuration Templates**. Cliccare poi su **Create Agent Configuration Template** in basso a sinistra nella pagina.
2. Digitare un nome e una descrizione per il modello di configurazione dell'agente.
3. Per specificare le impostazioni dell'agente, cliccare su **Select**, spuntare le caselle accanto alle impostazioni che si desidera aggiungere al modello di configurazione dell'agente, cliccare su **OK** e specificare i valori appropriati.

Le impostazioni dell'agente ne definiscono le funzioni quando è in esecuzione nel computer. Per ulteriori informazioni su specifiche impostazioni dell'agente e valori disponibili, consultare la sezione [Impostazioni dell'agente](#) a pagina 20.

4. Cliccare su **Save**.

Nota: una volta creato il modello di configurazione dell'agente, è possibile visualizzare i criteri che utilizzano questo modello cliccando sulla relativa opzione del menu del tasto destro del mouse nella pagina **Agent Configuration Templates** o durante la modifica del modello cliccando sul collegamento **View Usage Details**.

2.6 Impostazioni dell'agente

La tabella seguente descrive le impostazioni dell'agente disponibili.

Per ulteriori informazioni sulla creazione dei modelli di configurazione dell'agente, consultare la sezione [Creazione dei modelli di configurazione dell'agente](#) a pagina 20.

Impostazione dell'agente	Descrizione e valori disponibili	Valore predefinito
Log Lifetime	<p>Tempo, espresso in ore, entro cui i log dell'agente sono conservati nel computer prima di essere cancellati e il computer riavviato. Quando la sessione di un agente ha inizio, tutti i file di log con una data precedente alla durata consentita vengono cancellati.</p> <p>Nota: La registrazione ha ripercussioni sulle prestazioni; si consiglia quindi di abilitarla esclusivamente per la risoluzione di un problema e di disabilitarla a problema risolto. I file di log per Windows 2000 e Windows XP si trovano nella cartella <code><unità>:\Documents and Settings\All Users\Application Data\Sophos\Sophos Compliance</code></p>	24

Impostazione dell'agente	Descrizione e valori disponibili	Valore predefinito
	Agent\Logs, mentre i file di log per Windows Vista e Windows 7 si trovano nella directory <unità>:\ProgramData\Sophos\Sophos Compliance Agent\Logs.	
Logging	<p>Imposta i livelli di log per l'agente. I valori disponibili sono:</p> <ul style="list-style-type: none"> ■ Log Error e Warning: comprende messaggi di errore e di avviso. ■ Log All Messages: comprende messaggi di errore, di avviso e informativi. ■ Log All Messages and Brief Trace: comprende messaggi di errore, di avviso, informativi e brief trace. <p>Nota: La registrazione ha ripercussioni sulle prestazioni; si consiglia quindi di abilitarla esclusivamente per la risoluzione di un problema e di disabilitarla a problema risolto. I file di log per Windows 2000 e Windows XP si trovano nella cartella <unità>:\Documents and Settings\All Users\Application Data\Sophos\Sophos Compliance Agent\Logs, mentre i file di log per Windows Vista e Windows 7 si trovano nella directory <unità>:\ProgramData\Sophos\Sophos Compliance Agent\Logs.</p>	Log Error and Warning
Max Attempts	Numero massimo di tentativi dell'agente di comunicare col NAC Server per una data operazione (vale a dire: recuperare un criterio, verificare/attuare/correggere e creare un report). L'agente tenta nuovamente di instaurare la comunicazione durante il suo avvio iniziale e durante gli intervalli della verifica; non lo fa durante i controlli di conformità condotti dall'utente.	10
Retry Delay	Indica il tempo, in secondi, che l'agente attenderà prima di dare inizio a un nuovo tentativo di comunicazione col NAC Server. L'agente tenta nuovamente di instaurare la comunicazione durante il suo avvio iniziale e durante gli intervalli della verifica; non lo fa durante i controlli di conformità condotti dall'utente.	15
Save Proxy Password	Salva la password di proxy utilizzata per richieste di autenticazione proxy successive. I valori disponibili sono Save e Do Not Save .	Save
Save Proxy Username	Salva il nome utente di proxy utilizzato per richieste di autenticazione proxy successive. I valori disponibili sono Save e Do Not Save .	Save
Show Errors In Results	<p>Mostra/nasconde i messaggi di errore nella finestra di dialogo Risultati. I valori disponibili sono Show e Hide.</p> <p>Se il valore prescelto è Show, i messaggi di errore vengono visualizzati nella finestra di dialogo Risultati e registrati nel file errors.htm situato nel computer. Se il valore prescelto è Hide, i messaggi di errore vengono solo registrati nel file errors.htm. Il file per Windows 2000 e Windows XP si trova nella cartella <unità>:\Documents and Settings\All Users\Application Data\Sophos\Sophos Compliance Agent\Data, mentre il file per Windows Vista e Windows 7 si trova nella cartella <unità>:\ProgramData\Sophos\Sophos Compliance Agent\Data.</p>	Show

Impostazione dell'agente	Descrizione e valori disponibili	Valore predefinito
Show Exit	Mostra/nasconde l'opzione di menu Exit. I valori disponibili sono Show e Hide .	Hide
Show Extended Errors	Mostra/nasconde, nella finestra di dialogo Risultati, i messaggi di errore dettagliati relativi agli errori di comunicazione del NAC Server. I valori disponibili sono Show e Hide . Se il valore prescelto è Show, i messaggi di errore dettagliati vengono visualizzati nella finestra di dialogo Risultati e registrati nel file errors.htm situato nel computer. Il file per Windows 2000 e Windows XP si trova nella cartella <unità>:\Documents and Settings\All Users\Application Data\Sophos\Sophos Compliance Agent\Data, mentre il file per Windows Vista e Windows 7 si trova nella cartella <unità>:\ProgramData\Sophos\Sophos Compliance Agent\Data.	Show
Show Logging	Stabilisce se visualizzare la casella Abilita registrazione nella finestra di dialogo About. I valori disponibili sono Show e Hide .	Show

2.7 Migliori pratiche relative ai profili

Questa sezione fornisce le migliori pratiche per i profili.

Utilizzo di profili predefiniti per creare i profili pronti per la produzione

Migliore pratica	Descrizione
Utilizzare come riferimento i profili predefiniti.	Utilizzare i profili predefiniti: <ul style="list-style-type: none"> ■ Per dimostrazioni, applicazioni pilota o test proof-of-concept, è possibile utilizzare i profili predefiniti senza modificarli. ■ Per la distribuzione in produzione, è possibile copiare (salvare come nuovi) i profili predefiniti e personalizzare la messaggistica, aggiungere altre condizioni, modificare le azioni ecc., o semplicemente utilizzare i profili come modello per crearne di nuovi.

Aggiunta di funzioni ai profili

Le capability sono funzioni di un'applicazione che possono essere valutate ai fini della conformità. Sophos NAC per prima cosa, utilizzando la funzione Installed, verifica che un determinato sistema operativo o applicazione sia installato. Una volta che il software ha verificato l'installazione di un'applicazione, valuta le altre eventuali funzioni nel computer.

Nota: le funzioni dell'applicazione dipendono da come è stato progettato il software dell'applicazione. Alcune funzioni non possono essere disponibili in determinati sistemi operativi che supportano l'applicazione o per tutte le sue versioni. Se una funzione non è

supportata non verrà visualizzata. Se una funzione è supportata da determinati sistemi operativi, ma non da altri, verrà visualizzata solo da quelli supportati.

Migliore pratica	Descrizione
<p>Aggiungere funzioni che testano l'applicazione al fine di verificare che si stia proteggendo il computer in modo adeguato.</p>	<p>Il fatto che un'applicazione sia installata non garantisce che quest'ultima stia proteggendo il computer. Si consiglia di aggiungere funzioni, come Last Scan Grace Period o Signature Grace Period, che testino l'applicazione per verificare che quest'ultima stia proteggendo il computer in modo adeguato.</p>
<p>Utilizzare le funzioni che supportano i criteri di sicurezza aziendali.</p>	<p>Per esempio, si può possedere un criterio che richiede settimanalmente la scansione del sistema da parte dell'applicazione antivirus oppure un criterio che considera la scansione in tempo reale una forma di protezione adeguata. Nel primo caso è consigliabile aggiungere nel profilo la funzione Scan, mentre nel secondo non è necessario.</p>
<p>Utilizzare le funzioni Grace Period (Last Scan Grace Period e Signature Grace Period) invece che le funzioni Date (Last Scan Date e Signature Date).</p>	<p>Grace period consente di impostare il profilo una volta sola richiedendo così una manutenzione minima.</p> <p>Le funzioni Grace Period e Date non devono essere utilizzate contemporaneamente, a meno che le condizioni non siano state accuratamente testate. Il risultato potrebbe essere imprevedibile.</p>
<p>Utilizzare tutte le funzioni disponibili per una più sicura valutazione del computer.</p>	<p>Quando possibile, utilizzare tutte le funzioni a disposizione (eccetto Grace Period e Date) per una più sicura valutazione del computer. Rimuovere dal profilo solo le funzioni che possono incidere sulla distribuzione di Sophos NAC o sui processi aziendali.</p>

Specificazione di condizioni e stati di conformità

Migliore pratica	Descrizione
<p>Assegnare gli stati di conformità alle condizioni in base all'accesso alla rete desiderato.</p>	<ul style="list-style-type: none"> ■ Utilizzare lo stato Compliant per consentire l'accesso alla rete. ■ Utilizzare lo stato Partially Compliant per limitare l'accesso alla rete o per attuare la quarantena; tale stato può essere anche utilizzato per consentire l'accesso completo alla rete visualizzando però messaggi e svolgendo azioni correttive. ■ Utilizzare lo stato Non-Compliant per negare o limitare l'accesso alla rete, visualizzare messaggi e svolgere azioni correttive. <p>lo stato di conformità del computer viene determinato dai profili contenuti nel criterio. Lo stato di conformità più basso indica lo stato di conformità generale. Se Sophos NAC determina che un computer è conforme al profilo antivirus, ma non conforme al profilo firewall, lo stato di conformità complessivo è non conforme.</p>
<p>Aggiungere una nuova condizione per testare più di un valore, per impostare un diverso stato di conformità oppure per specificare un messaggio o azione correttiva differente a seconda dello stato di conformità.</p>	<p>Per esempio, con Grace Period si può determinare quando un file della firma di un computer è obsoleto di 5 giorni, ma negare l'accesso alla rete quando lo stesso file è obsoleto di 10 giorni. In questo caso è necessario aggiungere una nuova condizione per cui il computer risulti conforme entro 5 giorni, l'utente riceva un messaggio di avviso ma continui ad avere accesso alla rete. Aggiungere un'altra condizione per cui il computer risulti parzialmente conforme entro 10 giorni, l'utente riceva un messaggio di avviso ma continui ad avere accesso alla rete. Se il file della firma del computer è obsoleto di oltre 10 giorni, l'utente riceve un messaggio di avviso e gli viene negato l'accesso alla rete.</p>
<p>Stabilire l'ordine di valutazione per condizioni multiple.</p>	<p>Una volta rispettata una condizione, vengono utilizzati stato di conformità, messaggio e azione correttiva associati, ma non verrà valutata nessun'altra condizione relativa a tale funzione.</p> <p>Per esempio, dando a una condizione Partially Compliant priorità maggiore della condizione Non-Compliant, ci si assicura che venga verificata innanzitutto la prima condizione e solo i computer non conformi non abbiano accesso alla rete.</p>
<p>Assicurarsi che stati di conformità, messaggi e azioni correttive corrispondano alla condizione selezionata.</p>	<p>Tutte le funzioni visualizzano condizioni e stati di conformità nell'ordine predefinito. Se si modifica una condizione, assicurarsi che gli stati di conformità corrispondano a ciò che si desidera valutare. Inoltre, se si cambiano le condizioni e gli stati di conformità, è consigliabile fare in modo che l'utente visualizzi messaggi differenti o che nel computer vengano eseguite azioni correttive diverse.</p>

Migliore pratica	Descrizione
	Per esempio, l'ordine predefinito può stabilire che se il firewall è Enabled, il computer sarà Compliant; la condizione Else (indicante in questo caso che il firewall è Not Enabled), comporta che il computer sia Non-Compliant. Di conseguenza, se si cambia la condizione in Not Enabled, è necessario cambiare anche gli stati di conformità associati per stabilire che, se il firewall è Not Enabled, il computer è Non-Compliant; la condizione Else (indicante in questo caso che il firewall è Enabled), comporta che il computer è Compliant.
Utilizzare condizioni e stati di conformità che supportano i propri criteri di sicurezza.	Per esempio, si può possedere un criterio di sicurezza che considera un computer come non conforme nel caso in cui la protezione in tempo reale non sia abilitata oppure se un criterio lo considera solo parzialmente conforme. Nel primo caso, ci si deve assicurare che il computer sia considerato non conforme e non abbia l'accesso alla rete. Nel secondo caso, si deve correggere il computer parzialmente conforme senza intervenire sull'accesso alla rete.
Per quanto concerne le funzioni Version, assicurarsi che il numero della versione contenga il numero corretto di cifre significative.	Per esempio, se si crea una condizione che specifica == 8 e la versione nel computer è la 8.1, il software confronta 8.1 con 8 (una sola cifra significativa) e la condizione risulta rispettata. Tuttavia, se si crea una condizione che specifica == 8.0 e la versione nel computer è la 8.1, il software confronta 8.1 con 8.0 (due cifre significative) e la condizione risulta non rispettata.
Per le applicazioni antivirus e antispyware, testare l'utilizzo dell'operatore == nelle funzioni Date.	Se si definisce un profilo per un'applicazione antivirus o antispyware e si specifica una funzione Date (Last Scan Date o Signature Date) tramite l'operatore == (uguale a), accertarsi che la data sia generata dal computer nel formato MM/GG/AAAA. Se l'applicazione genera una data nel formato MM/GG/AAAA HH:MM:SS, il rilevamento può dare esito negativo anche se la data nel computer è identica al valore specificato nella condizione. Per evitare questo problema, durante la definizione delle date si può utilizzare l'operatore >= (maggiore o uguale a) o <= (minore o uguale a) invece di ==. Un criterio va testato prima della distribuzione, per assicurare che l'operatore == non sbaglia il rilevamento.

Creazione di messaggi

I messaggi vengono visualizzati solo quando le condizioni vengono soddisfatte. A seconda del criterio, gli utenti possono visualizzare messaggi multipli. Testare i messaggi per verificare che siano accurati, informativi e adeguati.

Importante: tenere in considerazione l'eventuale presenza di computer non appartenenti all'impresa ma connessi alla sua rete. Se si verifica questa situazione, i messaggi di avviso

devono essere adeguatamente formulati, dal momento che tali computer possono eseguire applicazioni di sicurezza differenti o non supportate. Il criterio predefinito Unmanaged viene utilizzato specificamente per i computer non gestiti. Aggiornare questo criterio e i profili e messaggi associati in modo che comunichi correttamente con i computer non gestiti.

Migliore pratica	Descrizione
Creare ed eliminare messaggi tramite la modalità Report Only del criterio.	Creare un profilo per il quale la messaggistica sia la più simile possibile a quella della produzione. I messaggi sono eliminabili selezionando Report Only come modalità del criterio. Quando si desidera visualizzare i messaggi ed eseguire azioni correttive, ma non attuare la conformità, è possibile passare alla modalità Remediate. Se si desidera anche attuare la conformità, è possibile passare alla modalità Enforce. Per ulteriori informazioni, consultare la sezione Distribuzione di Network Access Control a pagina 3.
Utilizzare i messaggi per notificare che si è verificata una determinata condizione.	Per esempio, creare un messaggio che indichi che la firma antivirus è obsoleta e che Sophos NAC la aggiornerà immediatamente.
Creare tutti i messaggi in inglese e poi creare i corrispondenti in ogni altra lingua.	L'agente sceglie la lingua più appropriata per visualizzare i messaggi. Il messaggio in inglese compare se non può essere visualizzato quello nell'altra lingua. Se un messaggio in inglese non esiste e il messaggio nell'altra lingua non può essere visualizzato, all'utente verrà visualizzata una finestra con un messaggio vuoto. I report di NAC Manager visualizzano i messaggi in inglese. Se non esistono messaggi in inglese, il campo dei messaggi rimane vuoto.

Utilizzo delle azioni correttive

Le azioni correttive a disposizione dipendono da come è stato progettato il software dell'applicazione. Alcune azioni correttive possono non essere disponibili in determinati sistemi operativi che supportano l'applicazione oppure per tutte le sue versioni. Se un'azione correttiva è supportata da determinati sistemi operativi, ma non da altri, quelli non supportati verranno visualizzati come sistemi operativi non supportati.

Migliore pratica	Descrizione
Selezionare le azioni correttive e bloccarle tramite la modalità Report Only del criterio.	Creare un profilo per il quale le azioni correttive siano le più simili possibile a quelle della produzione. Le azioni correttive sono eliminabili selezionando Report Only come modalità del criterio. Quando si desidera visualizzare i messaggi ed eseguire azioni correttive, ma non attuare la conformità, è possibile passare alla modalità Remediate. Se si desidera anche attuare la conformità, è possibile passare alla modalità Enforce.

Migliore pratica	Descrizione
	Per ulteriori informazioni, consultare la sezione Distribuzione di Network Access Control a pagina 3.
Quando si eseguono azioni correttive, creare una condizione con stato di accesso Partially Compliant.	Se si creano solo condizioni con stati di conformità Compliant e Non-Compliant, perché le azioni correttive abbiano luogo il computer deve risultare non conforme. Se si crea una condizione con lo stato di conformità Partially Compliant, è possibile intraprendere azioni correttive che assicurino che i computer siano aggiornati e vengano considerati Non-Compliant solo se molto indietro negli aggiornamenti.
Quando possibile, per una più sicura valutazione del computer, utilizzare tutte le azioni correttive a disposizione.	Rimuovere dal profilo solo le azioni correttive che possono causare problemi durante la distribuzione.
Evitare di applicare azioni correttive se possono compromettere un'operazione critica nel computer.	Per evitarne azioni correttive, è possibile creare, per utenti specifici, profili separati che non comprendano azioni correttive; deselezionare temporaneamente le azioni correttive nei profili esistenti o cambiare la modalità del criterio dell'utente in Report Only. In conclusione, è necessario valutare l'impatto di un'azione correttiva sul lavoro degli utenti e il rischio comportato dal non eseguirla rispetto a quello causato dalla mancata esecuzione di un'attività critica.

2.8 Creazione di profili

I profili consentono di definire quali elementi dei computer devono essere valutati, quali sistemi operativi e applicazioni. I profili definiscono condizioni, stati di conformità, messaggi e azioni correttive. Una volta creati possono essere organizzati e ordinati per priorità all'interno dei criteri.

È possibile creare un profilo relativo a un determinato elemento, cui successivamente associare i service pack o le funzioni dell'applicazione per quell'elemento (a seconda del tipo di elemento). Se, per un determinato elemento, si desiderano definire differenti stati di conformità, messaggi o azioni correttive, è possibile creare profili multipli per uno stesso sistema operativo o applicazione.

2.9 Linee guida sui profili

Le istruzioni relative ai profili includono quanto riportato di seguito:

- Al criterio è possibile aggiungere un numero illimitato di profili.
- In un criterio deve essere incluso almeno un profilo del sistema operativo.
- I criteri devono comprendere i profili di tutti i sistemi operativi che si desidera valutare nei computer.

- A un profilo può appartenere un solo sistema operativo o applicazione.
- Un sistema operativo o applicazione può appartenere a più profili.

2.10 Utilizzo dei profili predefiniti di Patch Manager

È possibile utilizzare i profili predefiniti di Patch Manager per supportare la conformità della patch per computer gestiti e non.

Se si sta eseguendo l'agente delle patch con Enterprise Console, è possibile includere i risultati della verifica delle patch come parte della verifiche di NAC. Il profilo predefinito del Sophos Patch Agent è disponibile per l'applicazione ai criteri di NAC. Se non si utilizza questa funzione, è ancora possibile cercare gli aggiornamenti del sistema operativo Windows utilizzando i profili di Windows Update.

Criteri Default and Managed

Il seguente profilo viene automaticamente aggiunto ai criteri Default e Managed. e va utilizzato con il Quarantine Agent e gli utenti conosciuti.

- **Profilo di Windows Update:** questo profilo è utilizzabile per assicurarsi che nei computer **gestiti** sia installato lo strumento Windows Update e gli aggiornamenti automatici siano abilitati. Se in un computer non sono abilitati gli Automatic Update, l'azione correttiva di Windows Update li abilita comunque nel computer.

Nota: Il profilo del Sophos Patch Agent non viene aggiunto automaticamente a questi criteri. Quando i criteri hanno il parametro Behavior impostato su Best, inclusi i profili di Windows Update e del Sophos Patch Agent, il computer può essere considerato conforme anche se non in possesso di tutte le patch, se è installato il tool di Windows Update e gli Automatic Update sono abilitati. Se si desidera aggiungere il profilo del Sophos Patch Agent a questi criteri, rimuovere il profilo di Windows Update o impostare Behavior su All.

Criterio Unmanaged

Il seguente profilo viene automaticamente aggiunto al criterio non gestito e va utilizzato con il Dissolvable Agent e gli utenti ospiti.

- **Profilo di Windows Update per computer non gestiti:** questo profilo è utilizzabile per accertare che nei computer non gestiti sia installato il tool di Windows Update e gli aggiornamenti automatici siano abilitati. Se in un computer non sono abilitati gli aggiornamenti automatici, viene visualizzato un messaggio che indica di abilitarli in modo tale da rendere il computer conforme.

2.11 Creazione dei profili dei sistemi operativi

La pagina Profiles consente di creare i profili dei sistemi operativi da utilizzare nei criteri. I profili dei sistemi operativi sono un mezzo per organizzare e dare priorità ai sistemi operativi e ai service pack associati che si desidera valutare nel computer. Nei profili è possibile definire le condizioni che determinano lo stato di conformità di un computer e i messaggi da visualizzare.

Procedura

1. Cliccare su **Manage > Profiles**. Quindi, cliccare su **Create Profile** in basso a sinistra nella pagina.

2. Digitare un nome e una descrizione per il profilo.
3. Cliccare su **Select Profile Item**.
4. Nell'elenco **Profile Type**, selezionare **Operating System**, quindi scegliere il sistema operativo per il quale si desidera creare questo profilo e cliccare su **OK**.

Importante: i profili dei sistemi operativi sono necessari nei criteri. 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.

5. Se del caso, cliccare sugli elenchi della colonna **Compliance State** per cambiare gli stati di conformità per le seguenti condizioni dei sistemi operativi. Per ulteriori informazioni, consultare la sezione [Determinazione dello stato di conformità del computer](#) a pagina 42.

- **Installata:** se questo sistema operativo è installato, questo stato di conformità viene applicato alla valutazione del criterio nel computer e a qualsiasi configurazione dei messaggi visualizzati.
- **Else:** se nessuno dei sistemi operativi è installato, lo stato di conformità associato al profilo del sistema operativo a più alta priorità nel criterio viene applicato alla valutazione del criterio nel computer e a qualsiasi configurazione dei messaggi visualizzati.

6. Se del caso, cliccare sugli elenchi della colonna **Message** e selezionare **Show Message** per aggiungere un messaggio a una condizione. Quindi, cliccare sull'icona **Message**, digitare il messaggio in tutte le lingue necessarie (ne sono supportate otto) e cliccare su **OK**.

Il messaggio viene visualizzato nel computer solo se la condizione viene soddisfatta.

Nota: l'agente sceglie la lingua più appropriata per visualizzare i messaggi in un computer. Si consiglia di creare un messaggio in inglese (lingua predefinita) in modo tale che, se non può essere visualizzato un messaggio in un'altra lingua, all'utente ne compaia comunque uno. Le versioni precedenti dell'agente visualizzano i messaggi solo in inglese (lingua predefinita). Per ulteriori informazioni sui messaggi, consultare la *Sophos Compliance Agent di Guida alla configurazione*.

7. Cliccare su **Add Service Packs**.

Nota: i service pack vengono valutati solo se il sistema operativo è installato nel computer.

8. Selezionare i service pack che si desidera aggiungere al profilo e cliccare su **OK**.
9. Se del caso, cliccare sugli elenchi della colonna **Compliance State** per cambiare gli stati di conformità per ogni condizione dei service pack.

- **Installata:** se è installato un particolare service pack, lo stato di conformità associato viene applicato alla valutazione del criterio del computer e a qualsiasi configurazione dei messaggi visualizzati.
- **Else:** se nessuno dei service pack è installato, lo stato di conformità associato al service pack a più alta priorità (il più recente) viene applicato alla valutazione del criterio del computer e a qualsiasi configurazione dei messaggi visualizzati.

10. Se del caso, cliccare sugli elenchi della colonna **Message** e selezionare **Show Message** per aggiungere un messaggio a una condizione. Quindi, cliccare sull'icona **Message**, digitare il messaggio in tutte le lingue necessarie (ne sono supportate otto) e cliccare su **OK**.

Il messaggio viene visualizzato nel computer solo se la condizione viene soddisfatta.

11. Cliccare su **Save**.

Nota: una volta creato il profilo, è possibile visualizzare i criteri che lo utilizzano cliccando sulla relativa opzione del menu del tasto destro del mouse nella pagina **Profiles** o, durante la modifica del profilo, cliccando sul collegamento **View Usage Details**.

2.12 Creazione dei profili delle applicazioni

La pagina Profiles consente di creare i profili delle applicazioni da utilizzare nei criteri. I profili delle applicazioni sono un mezzo per organizzare e dare priorità alle applicazioni e funzioni associate che si desidera valutare nel computer. Nei profili è possibile definire le condizioni che determinano lo stato di conformità del computer, insieme ai messaggi da visualizzare e alle azioni correttive da eseguire.

Procedura

1. Cliccare su **Manage > Profiles**. Quindi, cliccare su **Create Profile** in basso a sinistra nella pagina.
2. Digitare un nome e una descrizione per il profilo.
3. Cliccare su **Select Profile Item**.
4. Scegliere un tipo di profilo dall'elenco **Profile Type**, digitare o selezionare le opzioni di ricerca appropriate e cliccare su **Search**.
5. Selezionare l'applicazione per cui si desidera creare questo profilo e cliccare su **OK**.

Nota: Perché tutti i nomi delle applicazioni vengano visualizzati correttamente, è necessario installare i file per il supporto delle lingue orientali (tramite **Pannello di controllo > Opzioni internazionali e della lingua**) nel computer in cui si visualizza NAC Manager.

6. Se del caso, cliccare sugli elenchi della colonna **Compliance State** per cambiare gli stati di conformità per le seguenti condizioni delle applicazioni. Per ulteriori informazioni, consultare la sezione [Determinazione dello stato di conformità del computer](#) a pagina 42.
 - **Installed:** se l'applicazione è installata, durante la valutazione del criterio del computer e a qualsiasi visualizzazione di messaggio configurata viene applicato questo stato di conformità.
 - **Else:** se l'applicazione è installata, questo stato di conformità viene applicato alla valutazione del criterio del computer e tutti i messaggi configurati vengono visualizzati.

7. Se del caso, cliccare sugli elenchi della colonna **Message** e selezionare **Show Message** per aggiungere un messaggio a una condizione. Quindi, cliccare sull'icona **Message**, digitare il messaggio in tutte le lingue necessarie (ne sono supportate otto) e cliccare su **OK**.

Il messaggio viene visualizzato nel computer solo se la condizione viene soddisfatta.

Nota: l'agente sceglie la lingua più appropriata per visualizzare i messaggi in un computer. Si consiglia di creare un messaggio in inglese (lingua predefinita) in modo tale che, se non può essere visualizzato un messaggio in un'altra lingua, all'utente ne compaia comunque uno. Le versioni precedenti dell'agente visualizzano i messaggi solo in inglese (lingua predefinita). Per ulteriori informazioni sui messaggi, consultare la Guida alla configurazione di Sophos Compliance Agent.

8. Cliccare su **Add Capabilities**.

Si intendono le funzioni di un'applicazione che possono essere testate durante una verifica di conformità. Le Capability contengono le regole utilizzate per la verifica, costituite da un insieme di condizioni, stati di conformità, messaggi e azioni correttive (se disponibili).

Le funzioni vengono valutate solo se l'applicazione è installata nel computer.

9. Selezionare le funzioni che si desidera aggiungere al profilo e cliccare su **OK**.

Per ulteriori informazioni sulle funzioni, consultare la sezione [Funzioni e condizioni di un'applicazione](#) a pagina 33.

10. Per ciascuna funzione, seguire una delle seguenti procedure:

- a) Per selezionare le condizioni oppure digitare i parametri della condizione nei campi a disposizione, cliccare sulla colonna **Condition**.

Per ulteriori informazioni sulle condizioni specifiche di una funzione dell'applicazione, consultare la sezione *Funzioni e condizioni di un'applicazione* a pagina 33.

- b) Cliccare sulla colonna **Compliance State** per modificare lo stato di conformità di ciascuna condizione.
- c) Cliccare sugli elenchi della colonna **Message** e selezionare **Show Message** per aggiungere un messaggio a una condizione. Quindi, cliccare sull'icona **Message**, digitare il messaggio in tutte le lingue necessarie (ne sono supportate otto) e cliccare su **OK**.

Il messaggio viene visualizzato nel computer solo se la condizione viene soddisfatta.

- d) Selezionare la casella di spunta appropriata dalla colonna **Remediation Action** per applicare un'azione correttiva a una condizione.

L'azione viene eseguita nel computer solo se la condizione viene soddisfatta. Le azioni correttive non sono disponibili per tutti i criteri o tutte le funzioni di un'applicazione. Sono disponibili le seguenti azioni correttive:

- **Enable:** nel computer, abilita la protezione in tempo reale per le applicazioni antivirus o antispyware, il firewall per le applicazioni firewall oppure gli aggiornamenti automatici per le applicazioni Patch Manager. Questa azione è disponibile sia per la funzione Real-Time Protection che Enabled.
- **Update:** aggiorna il file della firma nel computer. Questa azione è disponibile sia per la funzione Signature Date che Signature Grace Period.
- **Scan:** inizia una scansione nel computer. Questa azione è disponibile per la funzione Scan Date o Scan Grace Period.
- **Apply:** applica il criterio di Sophos Enterprise Console per l'applicazione di Sophos Anti-Virus sul computer endpoint. Questa azione è disponibile per la funzione dell'applicazione di SEC Policy.

- e) Cliccare su **New Condition** per aggiungere ulteriori condizioni alla funzione dell'applicazione.

Le condizioni disponibili dipendono dalle funzioni selezionate al punto 9; se non si seleziona una funzione avente ulteriori condizioni, tale pulsante non viene visualizzato. Se si aggiungono ulteriori condizioni, è possibile utilizzare le frecce su e giù per riordinare le priorità delle condizioni ai fini della valutazione del computer.

11. Cliccare su **Salva**.

Nota: una volta creato il profilo, è possibile visualizzare i criteri che lo utilizzano cliccando sulla relativa opzione del menu del tasto destro del mouse nella pagina **Profiles** o, durante la modifica del profilo, cliccando sul collegamento **View Usage Details**.

2.13 Funzioni e condizioni di un'applicazione

Le seguenti tabelle indicano le condizioni a disposizione di ciascuna funzione dell'applicazione, ordinate in base al tipo di profilo:

Per ulteriori informazioni sulla creazione dei profili dell'applicazione, consultare la sezione [Creazione dei profili delle applicazioni](#) a pagina 30.

Nota: le funzioni dell'applicazione e le azioni correttive dipendono da come è stato progettato il software dell'applicazione. Alcune funzioni e azioni correttive possono non essere disponibili in determinati sistemi operativi che supportano l'applicazione oppure in tutte le versioni dell'applicazione. Se una funzione non è supportata non verrà visualizzata. Se una funzione è supportata solo da alcuni sistemi operativi, verranno visualizzati solo quelli che la supportano. Se un'azione correttiva è supportata solo su determinati sistemi operativi, quelli non supportati verranno visualizzati come sistemi operativi non supportati.

Sophos Anti-Virus

Nota: Sophos Anti-Virus supporta queste funzioni oltre alle funzioni standard antivirus, antispyware, HIPS e IDS. Le funzioni disponibili dipendono dalla versione del software.

Funzione dell'applicazione	Descrizione e condizioni disponibili
Adware/PUA	Determina se adware o applicazioni potenzialmente indesiderate (PUA) vengono rilevate nel computer. Condizioni disponibili: <ul style="list-style-type: none"> ■ Detected/Not Detected: specifica se adware o PUA vengano rilevate o meno e i relativi stato di conformità e messaggio, nel caso in cui la condizione sia rispettata. ■ Else: specifica i relativi stato di conformità e messaggio se la condizione Detected/Not Detected non è rispettata.
Controlled Applications	Determina se un'applicazione controllata viene rilevata nel computer. Le applicazioni controllate vengono definite all'interno del criterio di Sophos Enterprise Console. Condizioni disponibili: <ul style="list-style-type: none"> ■ Detected/Not Detected: specifica se un'applicazione controllata viene rilevata o meno e i relativi stato di conformità e messaggio, nel caso in cui la condizione sia rispettata. ■ Else: specifica i relativi stato di conformità e messaggio se la condizione Detected/Not Detected non è rispettata.
Managed by SEC	Determina se Sophos Anti-Virus è gestito da Sophos Enterprise Console o è installato come prodotto autonomo. Condizioni disponibili: <ul style="list-style-type: none"> ■ Yes/No: specifica se Sophos Anti-Virus è gestito da Sophos Enterprise Console e i relativi stato di conformità e messaggio, nel caso in cui la condizione sia rispettata. ■ Else: specifica i relativi stato di conformità e messaggio se la condizione Yes/No Detected non è rispettata.

Funzione dell'applicazione	Descrizione e condizioni disponibili
SEC Policy	<p>Determina se Sophos Anti-Virus è conforme al criterio in Sophos Enterprise Console. Condizioni disponibili:</p> <ul style="list-style-type: none"> ■ Conforms/Does Not Conform: specifica se Sophos Anti-Virus è conforme al criterio di Sophos Enterprise Console e i relativi stato di conformità e messaggio, nel caso in cui la condizione sia rispettata. ■ Else: specifica i relativi stato di conformità, messaggio e azione se la condizione Conforms/Does Not Conform non è rispettata.
Suspicious Behavior	<p>Determina se nel computer viene rilevato un comportamento sospetto. Condizioni disponibili:</p> <ul style="list-style-type: none"> ■ Detected/Not Detected: specifica se nel computer viene rilevato un comportamento sospetto o meno e i relativi stato di conformità e messaggio, nel caso in cui la condizione sia rispettata. ■ Else: specifica i relativi stato di conformità e messaggio se la condizione Detected/Not Detected non è rispettata.
Suspicious File	<p>Determina se nel computer viene rilevato un file sospetto. Condizioni disponibili:</p> <ul style="list-style-type: none"> ■ Detected/Not Detected: specifica se un'applicazione controllata viene rilevata o meno e i relativi stato di conformità e messaggio, nel caso in cui la condizione sia rispettata. ■ Else: specifica i relativi stato di conformità e messaggio se la condizione Detected/Not Detected non è rispettata.
Virus/Spyware	<p>Determina se nel computer viene rilevato un virus o spyware. Condizioni disponibili:</p> <ul style="list-style-type: none"> ■ Detected/Not Detected: specifica se virus e spyware vengono rilevati o meno e i relativi stato di conformità e messaggio, nel caso in cui la condizione sia rispettata. ■ Else: specifica i relativi stato di conformità e messaggio se la condizione Detected/Not Detected non è rispettata.

Anti-Spyware o Anti-Virus

Funzione dell'applicazione	Descrizione e condizioni disponibili
Last Scan Date	<p>Determina se la data dell'ultima scansione dell'applicazione corrisponde alla data indicata nella condizione. La funzione Last Scan Date può essere utilizzata al posto di quella Last Scan Grace Period. Condizioni disponibili:</p> <ul style="list-style-type: none"> ■ Date: specifica la data dell'ultima scansione del computer e i relativi stato di conformità, messaggio e azione, nel caso in cui la condizione sia rispettata. Operatori: == (uguale a), != (diverso da), < (minore di), <= (minore o uguale a), > (maggiore di), >= (maggiore o uguale a). ■ Else: specifica i relativi stato di conformità, messaggio e azione se la condizione Date non è rispettata.
Last Scan Grace Period	<p>Determina se la data dell'ultima scansione dell'applicazione è valida rispetto alla data indicata nella condizione. La funzione Last Scan Grace Period può essere utilizzata al posto di quella Last Scan Date. Condizioni disponibili:</p> <ul style="list-style-type: none"> ■ Within: specifica il numero di giorni entro cui deve rientrare la data dell'ultima scansione del computer per poter essere considerata valida e i relativi stato di conformità, messaggio e azione, nel caso in cui la condizione sia rispettata. ■ Else: specifica i relativi stato di conformità, messaggio e azione se la condizione Within non è rispettata.
Real-Time Protection	<p>Determina se l'applicazione sta attivamente proteggendo il computer. Condizioni disponibili:</p> <ul style="list-style-type: none"> ■ Enabled/Disabled: specifica se la protezione in tempo reale dell'applicazione è abilitata o meno e i relativi stato di conformità, messaggio e azione, nel caso in cui la condizione sia rispettata. ■ Else: specifica i relativi stato di conformità e messaggio se la condizione Enabled/Disabled non è rispettata.
Signature Date	<p>Determina se la data del file della firma dell'applicazione corrisponde alla data indicata nella condizione. La funzione Signature Date può essere utilizzata al posto della Signature Grace Period. Condizioni disponibili:</p> <ul style="list-style-type: none"> ■ Date: specifica la data del file della firma nel computer e i relativi stato di conformità, messaggio e azione, nel caso in cui la condizione sia rispettata. Operatori: == (uguale a), != (diverso da), < (minore di), <= (minore o uguale a), > (maggiore di), >= (maggiore o uguale a). ■ Else: specifica i relativi stato di conformità, messaggio e azione se la condizione Date non è rispettata.

Funzione dell'applicazione	Descrizione e condizioni disponibili
Signature Grace Period	<p>Determina se il file della firma dell'applicazione è valido rispetto alla data indicata nella condizione. La funzione Signature Grace Period può essere utilizzata al posto di quella Signature Date. Condizioni disponibili:</p> <ul style="list-style-type: none"> ■ Within: specifica il numero di giorni entro cui deve rientrare la data dell'ultima scansione del computer per poter essere considerata valida e i relativi stato di conformità, messaggio e azione, nel caso in cui la condizione sia rispettata. ■ Else: specifica i relativi stato di conformità, messaggio e azione se la condizione Within non è rispettata.
Versione	<p>Determina se la versione dell'applicazione nel computer rispetta la condizione.</p> <p>Nota: nel computer la versione viene valutata utilizzando il numero di cifre significative indicate nella condizione. Per esempio, se si crea una condizione che specifica == 8 e la versione nel computer è la 8.1, il software confronta 8.1 con 8 (una sola cifra significativa) e la condizione risulta rispettata. Tuttavia, se si crea una condizione che specifica == 8.0 e la versione nel computer è la 8.1, il software confronta 8.1 con 8.0 (due cifre significative) e la condizione risulta non rispettata.</p> <ul style="list-style-type: none"> ■ Se l'applicazione è stata definita specificandone la versione nel profilo, le condizioni disponibili all'interno di tale profilo sono: <ul style="list-style-type: none"> ■ Version: specifica la versione dell'applicazione nel computer e i relativi stato di conformità e messaggio, nel caso in cui la condizione sia rispettata. Operatori: == (uguale a), != (diverso da), < (minore di), <= (minore o uguale a), > (maggiore di), >= (maggiore o uguale a). La versione deve essere espressa nel formato N.n.n.n. ed è limitata a quattro cifre significative. ■ Else: specifica i relativi stato di conformità e messaggio se la condizione Version non è rispettata. ■ Se l'applicazione fosse definita specificandone la versione nelle regole di rilevamento, le condizioni disponibili all'interno di tale profilo sarebbero: <ul style="list-style-type: none"> ■ Pass/Fail: specifica l'esito della valutazione nel computer se la versione dell'applicazione del computer corrisponde a quella specificata all'interno delle regole di rilevamento dell'applicazione stessa, e i relativi stato di conformità e messaggio, nel caso in cui la condizione sia rispettata. ■ Else: specifica i relativi stato di conformità e messaggio se la condizione Pass/Fail non è rispettata.

Verifica, HIPS o IDS

Funzione dell'applicazione	Descrizione e condizioni disponibili
Running	<p>Determina se i servizi eseguibili sono in esecuzione nel computer. Condizioni disponibili:</p> <ul style="list-style-type: none"> ■ Running/Not Running: specifica se i servizi eseguibili sono o meno in esecuzione nel computer e i relativi stato di conformità, messaggio e azione, nel caso in cui la condizione sia rispettata. ■ Else: specifica i relativi stato di conformità e messaggio se la condizione Running/Not Running non è rispettata.
Versione	<p>Determina se la versione dell'applicazione nel computer rispetta la condizione.</p> <p>Nota: nel computer la versione viene valutata utilizzando il numero di cifre significative indicate nella condizione. Per esempio, se si crea una condizione che specifica == 8 e la versione nel computer è la 8.1, il software confronta 8.1 con 8 (una sola cifra significativa) e la condizione risulta rispettata. Tuttavia, se si crea una condizione che specifica == 8.0 e la versione nel computer è la 8.1, il software confronta 8.1 con 8.0 (due cifre significative) e la condizione risulta non rispettata.</p> <ul style="list-style-type: none"> ■ Se l'applicazione è stata definita specificandone la versione nel profilo, le condizioni disponibili all'interno di tale profilo sono: <ul style="list-style-type: none"> ■ Version: specifica la versione dell'applicazione nel computer e i relativi stato di conformità e messaggio, nel caso in cui la condizione sia rispettata. Operatori: == (uguale a), != (diverso da), < (minore di), <= (minore o uguale a), > (maggiore di), >= (maggiore o uguale a). La versione deve essere espressa nel formato N.n.n.n. ed è limitata a quattro cifre significative. ■ Else: specifica i relativi stato di conformità e messaggio se la condizione Version non è rispettata. ■ Se l'applicazione fosse definita specificandone la versione nelle regole di rilevamento, le condizioni disponibili all'interno di tale profilo sarebbero: <ul style="list-style-type: none"> ■ Pass/Fail: specifica l'esito della valutazione nel computer se la versione dell'applicazione del computer corrisponde a quella specificata all'interno delle regole di rilevamento dell'applicazione stessa, e i relativi stato di conformità e messaggio, nel caso in cui la condizione sia rispettata. ■ Else: specifica i relativi stato di conformità e messaggio se la condizione Pass/Fail non è rispettata.

Firewall

Funzione dell'applicazione	Descrizione e condizioni disponibili
Enabled	<p>Determina se l'applicazione sta attivamente proteggendo il computer. Condizioni disponibili:</p> <ul style="list-style-type: none"> ■ Enabled/Disabled: specifica se il firewall nel computer è attivo o meno e i relativi stato di conformità, messaggio e azione, nel caso in cui la condizione sia rispettata. ■ Else: specifica i relativi stato di conformità e messaggio se la condizione Enabled/Disabled non è rispettata.
Running	<p>Determina se i servizi eseguibili sono in esecuzione nel computer. Condizioni disponibili:</p> <ul style="list-style-type: none"> ■ Running/Not Running: specifica se i servizi eseguibili sono o meno in esecuzione nel computer e i relativi stato di conformità, messaggio e azione, nel caso in cui la condizione sia rispettata. ■ Else: specifica i relativi stato di conformità e messaggio se la condizione Running/Not Running non è rispettata.
Versione	<p>Determina se la versione dell'applicazione nel computer rispetta la condizione.</p> <p>Nota: nel computer la versione viene valutata utilizzando il numero di cifre significative indicate nella condizione. Per esempio, se si crea una condizione che specifica == 8 e la versione nel computer è la 8.1, il software confronta 8.1 con 8 (una sola cifra significativa) e la condizione risulta rispettata. Tuttavia, se si crea una condizione che specifica == 8.0 e la versione nel computer è la 8.1, il software confronta 8.1 con 8.0 (due cifre significative) e la condizione risulta non rispettata.</p> <ul style="list-style-type: none"> ■ Se l'applicazione è stata definita specificandone la versione nel profilo, le condizioni disponibili all'interno di tale profilo sono: <ul style="list-style-type: none"> ■ Version: specifica la versione dell'applicazione nel computer e i relativi stato di conformità e messaggio, nel caso in cui la condizione sia rispettata. Operatori: == (uguale a), != (diverso da), < (minore di), <= (minore o uguale a), > (maggiore di), >= (maggiore o uguale a). La versione deve essere espressa nel formato N.n.n.n. ed è limitata a quattro cifre significative. ■ Else: specifica i relativi stato di conformità e messaggio se la condizione Version non è rispettata. ■ Se l'applicazione fosse definita specificandone la versione nelle regole di rilevamento, le condizioni disponibili all'interno di tale profilo sarebbero: <ul style="list-style-type: none"> ■ Pass/Fail: specifica l'esito della valutazione nel computer se la versione dell'applicazione del computer corrisponde a quella

Funzione dell'applicazione	Descrizione e condizioni disponibili
	<p>specificata all'interno delle regole di rilevamento dell'applicazione stessa, e i relativi stato di conformità e messaggio, nel caso in cui la condizione sia rispettata.</p> <ul style="list-style-type: none"> ■ Else: specifica i relativi stato di conformità e messaggio se la condizione Pass/Fail non è rispettata.

Cifratura di dispositivi fissi

Funzione dell'applicazione	Descrizione e condizioni disponibili
Full Disk Encryption	<p>Stabilisce se le unità hard disk nel computer sono criptate. Condizioni disponibili:</p> <ul style="list-style-type: none"> ■ All Drives/At Least 1 Drive/No Drives: indica se tutte le unità, almeno una, o nessuna unità del computer sono criptate e il relativo stato di conformità e messaggio se tale condizione è rispettata. ■ Else: specifica i relativi stato di conformità e messaggio se le altre condizioni non sono rispettate.
Pre-boot Authentication	<p>Indica se l'applicazione è abilitata all'autenticazione dell'utente prima prima dell'avvio del computer. Condizioni disponibili:</p> <ul style="list-style-type: none"> ■ Enabled/Temporarily Disabled/Disabled: indica se nel computer l'autenticazione precedente all'avvio è abilitata, temporaneamente disabilitata o disabilitata completamente; indica inoltre i relativi stato di conformità e azione se la condizione è rispettata. ■ Else: specifica i relativi stato di conformità e azione se le altre condizioni non sono rispettate.
Versione	<p>Determina se la versione dell'applicazione nel computer rispetta la condizione.</p> <p>Nota: nel computer la versione viene valutata utilizzando il numero di cifre significative indicate nella condizione. Per esempio, se si crea una condizione che specifica == 8 e la versione nel computer è la 8.1, il software confronta 8.1 con 8 (una sola cifra significativa) e la condizione risulta rispettata. Tuttavia, se si crea una condizione che specifica == 8.0 e la versione nel computer è la 8.1, il software confronta 8.1 con 8.0 (due cifre significative) e la condizione risulta non rispettata.</p> <ul style="list-style-type: none"> ■ Se l'applicazione è stata definita specificandone la versione nel profilo, le condizioni disponibili all'interno di tale profilo sono: <ul style="list-style-type: none"> ■ Version: specifica la versione dell'applicazione nel computer e i relativi stato di conformità e messaggio, nel caso in cui la condizione sia rispettata. Operatori: == (uguale a), != (diverso da), < (minore di),

Funzione dell'applicazione	Descrizione e condizioni disponibili
	<p><= (minore o uguale a), > (maggiore di), >= (maggiore o uguale a). La versione deve essere espressa nel formato N.n.n.n. ed è limitata a quattro cifre significative.</p> <ul style="list-style-type: none"> ■ Else: specifica i relativi stato di conformità e messaggio se la condizione Version non è rispettata. ■ Se l'applicazione fosse definita specificandone la versione nelle regole di rilevamento, le condizioni disponibili all'interno di tale profilo sarebbero: <ul style="list-style-type: none"> ■ Pass/Fail: specifica l'esito della valutazione nel computer se la versione dell'applicazione del computer corrisponde a quella specificata all'interno delle regole di rilevamento dell'applicazione stessa, e i relativi stato di conformità e messaggio, nel caso in cui la condizione sia rispettata. ■ Else: specifica i relativi stato di conformità e messaggio se la condizione Pass/Fail non è rispettata.

Patch Manager

Funzione dell'applicazione	Descrizione e condizioni disponibili
Enabled	<p>Determina se l'applicazione sta attivamente proteggendo il computer. Questa funzione è disponibile per l'agente delle patch e i tool di Windows Update. Condizioni disponibili:</p> <ul style="list-style-type: none"> ■ Enabled/Disabled: indica se nel computer l'autenticazione delle patch è abilitata o disabilitata, oltre che il relativo stato di conformità e messaggio se la condizione è rispettata. Specifica se gli aggiornamenti automatici per lo strumento Windows Update sono attivi o meno nel computer e i relativi stato di conformità, messaggio e azione, nel caso in cui la condizione sia rispettata. ■ Else: specifica i relativi stato di conformità e messaggio se la condizione Enabled/Disabled non è rispettata.
Patch applicata	<p>Stabilisce se la patch sia stata applicata Condizioni disponibili:</p> <ul style="list-style-type: none"> ■ Patched/Not Patched: specifica se al computer sia stata applicata una patch o meno e i relativi stato di conformità e messaggio, nel caso in cui la condizione sia rispettata. ■ Else: specifica i relativi stato di conformità e messaggio se la condizione Patched/Not Patched non è rispettata.

Funzione dell'applicazione	Descrizione e condizioni disponibili
Versione	<p>Determina se la versione dell'applicazione nel computer rispetta la condizione.</p> <p>Nota: nel computer la versione viene valutata utilizzando il numero di cifre significative indicate nella condizione. Per esempio, se si crea una condizione che specifica == 8 e la versione nel computer è la 8.1, il software confronta 8.1 con 8 (una sola cifra significativa) e la condizione risulta rispettata. Tuttavia, se si crea una condizione che specifica == 8.0 e la versione nel computer è la 8.1, il software confronta 8.1 con 8.0 (due cifre significative) e la condizione risulta non rispettata.</p> <ul style="list-style-type: none"> ■ Version: specifica la versione dell'applicazione nel computer e i relativi stato di conformità e messaggio, nel caso in cui la condizione sia rispettata. Operatori: == (uguale a), != (diverso da), < (minore di), <= (minore o uguale a), > (maggiore di), >= (maggiore o uguale a). La versione deve essere espressa nel formato N.n.n.n. ed è limitata a quattro cifre significative. ■ Else: specifica i relativi stato di conformità e messaggio se la condizione Version non è rispettata.

Cifratura di dispositivi rimovibili

Funzione dell'applicazione	Descrizione e condizioni disponibili
Versione	<p>Determina se la versione dell'applicazione nel computer rispetta la condizione.</p> <p>Nota: nel computer la versione viene valutata utilizzando il numero di cifre significative indicate nella condizione. Per esempio, se si crea una condizione che specifica == 8 e la versione nel computer è la 8.1, il software confronta 8.1 con 8 (una sola cifra significativa) e la condizione risulta rispettata. Tuttavia, se si crea una condizione che specifica == 8.0 e la versione nel computer è la 8.1, il software confronta 8.1 con 8.0 (due cifre significative) e la condizione risulta non rispettata.</p> <ul style="list-style-type: none"> ■ Se l'applicazione è stata definita specificandone la versione nel profilo, le condizioni disponibili all'interno di tale profilo sono: <ul style="list-style-type: none"> ■ Version: specifica la versione dell'applicazione nel computer e i relativi stato di conformità e messaggio, nel caso in cui la condizione sia rispettata. Operatori: == (uguale a), != (diverso da), < (minore di), <= (minore o uguale a), > (maggiore di), >= (maggiore o uguale a). La versione deve essere espressa nel formato N.n.n.n. ed è limitata a quattro cifre significative. ■ Else: specifica i relativi stato di conformità e messaggio se la condizione Version non è rispettata.

Funzione dell'applicazione	Descrizione e condizioni disponibili
	<ul style="list-style-type: none"> ■ Se l'applicazione fosse definita specificandone la versione nelle regole di rilevamento, le condizioni disponibili all'interno di tale profilo sarebbero: <ul style="list-style-type: none"> ■ Pass/Fail: specifica l'esito della valutazione nel computer se la versione dell'applicazione del computer corrisponde a quella specificata all'interno delle regole di rilevamento dell'applicazione stessa, e i relativi stato di conformità e messaggio, nel caso in cui la condizione sia rispettata. ■ Else: specifica i relativi stato di conformità e messaggio se la condizione Pass/Fail non è rispettata.

2.14 Determinazione dello stato di conformità del computer

Lo stato di conformità viene stabilito secondo la conformità o meno del computer ai profili contenuti nel criterio. Il software verifica le condizioni del profilo secondo il comportamento del criterio assegnato a quel tipo di profilo. Innalza poi tutte le informazioni relative all'attuazione di NAC al livello del criterio ed assegna loro lo stato di conformità a partire da quella meno conforme. Una volta determinato lo stato di conformità, l'accesso alla rete basato su tale stato può essere concesso utilizzando i modelli di accesso assegnati nel criterio.

- **Compliant:** se la condizione è rispettata durante la fase di verifica, il computer viene riconosciuto come conforme.
- **Partially Compliant:** se la condizione è rispettata durante la fase di verifica, il computer viene riconosciuto come parzialmente conforme.
- **Non-Compliant:** se la condizione è rispettata durante la fase di verifica, il computer viene riconosciuto come non conforme.

3 Panoramica dell'area Enforce

L'area Enforce include tutti i componenti richiesti per impostare le risorse della rete, le impostazioni dell'accesso a Internet e le esenzioni. Dal menu Enforce è possibile accedere alle seguenti aree:

Area e azione	Descrizione
DHCP Configuration Wizard	
Eseguire la procedura guidata di configurazione di DHCP	La Procedura guidata di configurazione di DHCP aiuta ad identificare i server proxy web, di correzione e di DHCP Enforcer da utilizzare con le implementazioni di DHCP di Sophos NAC e a configurare automaticamente i modelli di accesso predefiniti di DHCP in base alle definizioni del proprio server.
Risorse di rete	
Creare risorse di rete.	Le risorse di rete sono applicazioni o dispositivi necessari per la correzione dei computer o responsabili della negazione dell'accesso alla rete dei computer messi in quarantena. Le risorse di rete possono essere aggiunte sia ai modelli di accesso di Agent Enforcer che a quelli di DHCP Enforcer. Nota: le risorse di rete vengono utilizzate per l'attuazione della quarantena basata sul client tramite Quarantine Agent o l'attuazione di DHCP.
Modelli di accesso di Agent Enforcer	
Creare modelli di accesso di Agent Enforcer.	I modelli di accesso di Agent Enforcer identificano le risorse di rete a cui i computer possono o non possono accedere durante l'applicazione della quarantena basata sul client. Una volta creati, i modelli di accesso di Agent Enforcer possono essere assegnati ai criteri per consentire l'accesso in base all'agente o allo stato di conformità del computer. Nota: I modelli di accesso di Agent Enforcer vengono applicati solo ai computer che utilizzano il Quarantine Agent.
Modelli di accesso di DHCP Enforcer	
Creare modelli di accesso di DHCP Enforcer.	I modelli di accesso di DHCP Enforcer specificano le impostazioni di accesso necessarie per supportare l'attuazione DHCP. Una volta creati, i modelli di accesso di DHCP Enforcer possono essere assegnati a criteri, esenzioni e impostazioni di Enforcer. Nota: I modelli di accesso di DHCP Enforcer vengono utilizzati solo con l'attuazione di DHCP in Sophos NAC.
Exemptions	
Creare esenzioni.	le esenzioni identificano, in base a vari criteri, i computer che non devono essere valutati ai fini della conformità quando si connettono alla rete. Tra i computer esenti si includono quelli che non possono eseguire l'agente (computer che utilizzano sistemi operativi non Windows) o quelli che non richiedono la verifica della conformità, quali server, router o stampanti.

Area e azione	Descrizione
	Nota: le esenzioni vengono utilizzate solo con l'attuazione di DHCP.
Abilitare o disabilitare le esenzioni.	Le esenzioni possono essere disabilitate o abilitate dall'amministratore di sistema. La disabilitazione di un'esenzione consente ai computer di essere valutati in base alla conformità. Se l'esenzione è disabilitata e il computer non ha Sophos Compliance Agent installato, il computer viene considerato sconosciuto. Abilitando un'esenzione si evita che la conformità del computer venga valutata.

3.1 Migliori pratiche relative ai modelli di accesso

Questa sezione descrive le migliori pratiche relative ai modelli di accesso. I modelli di accesso determinano come concedere ai computer l'accesso alla rete. Sophos NAC supporta l'attuazione dell'agente e di DHCP. Quando i modelli di accesso vengono applicati agli stati di accesso compliant, partially compliant o non-compliant in NAC Manager, l'accesso alla rete può essere attuato congiuntamente alla verifica della conformità del computer.

Creazione di un modello di accesso per la produzione

Migliore pratica	Descrizione
Creazione di un modello di accesso che si avvicini alla forma definitiva per la produzione.	Nel criterio, utilizzare l'impostazione Policy Mode per aumentare gradualmente l'impatto sugli utenti. L'attuazione è attivabile tramite questa semplice impostazione, apportando solo cambiamenti minimi ai modelli di accesso. Per ulteriori informazioni, consultare la sezione Migliori pratiche relative ai criteri a pagina 13.

Utilizzo di modelli di accesso predefiniti come riferimento

Migliore pratica	Descrizione
Utilizzo di modelli di accesso predefiniti come riferimento.	Utilizzare i modelli predefiniti di accesso: <ul style="list-style-type: none"> ■ Per dimostrazioni, applicazioni pilota o test proof-of-concept, è possibile utilizzare i modelli di accesso predefiniti senza modificarli. ■ Per la distribuzione in produzione, si possono copiare (salvare come nuovi) i modelli di accesso predefiniti e personalizzarne le impostazioni.

Diversificazione del livello di priorità di risorse di rete, modelli di accesso ed esenzioni

Utilizzare la priorità per implementare l'adeguato tipo di accesso alla rete.

Migliore pratica	Descrizione
Dare maggiore priorità alle risorse di rete, alle esenzioni e ai modelli di accesso più specifici/rigidi e minore priorità a quelli meno specifici/rigidi.	<ul style="list-style-type: none"> ■ Risorse di rete: se a un computer è applicabile più di una risorsa di rete, la prima di esse che corrisponde al computer ne determina l'accesso alla rete. Le risorse di rete eseguibili vengono valutate prima delle risorse di rete porta/protocollo. ■ Access Templates: se a un particolare stato è applicabile più di un modello di accesso, viene utilizzato il primo modello di accesso che lo soddisfa. I modelli di accesso più specifici/rigidi forniscono un indirizzo IP specifico o un intervallo IP più limitato, mentre quelli meno specifici/rigidi forniscono un intervallo più ampio. ■ Exemptions: se a un computer si applica più di un'esenzione, la prima di tali esenzioni che corrisponde al computer ne determina l'accesso. Inoltre, se una particolare esenzione contiene più di un modello di accesso, verrà utilizzato il primo modello contenente l'indirizzo IP del server DHCP o del relay DHCP.

Specificazione degli stati di conformità del modello

Migliore pratica	Descrizione
Non selezionare stati di conformità del modello in conflitto fra loro.	Per esempio, se si seleziona Compliant, è consigliabile creare un modello che permetta l'accesso alla rete. Se invece si seleziona Non-Compliant, si dovrà creare un modello che limiti l'accesso ai soli server di correzione.

Specificazione dei modelli di accesso per lo stato di accesso Default

Migliore pratica	Descrizione
Specificare i modelli di accesso per lo stato di accesso Default. Questa migliore pratica è applicabile solo all'attuazione DHCP.	<p>Se si utilizza l'attuazione di DHCP, specificare i modelli di accesso appropriati per lo stato di accesso Default dalla pagina Configure System > Enforcer Settings di NAC Manager.</p> <p>Il modello di accesso Default costituisce fondamentalmente l'ultima risorsa per l'assegnazione dei modelli di accesso. Di conseguenza, si consiglia di assicurarsi che tutti i possibili indirizzi IP siano inclusi nei modelli di accesso assegnati allo</p>

Migliore pratica	Descrizione
	stato di accesso Default. Dare innanzitutto maggiore priorità ai modelli di accesso più specifici/rigidi e identificare il modello di accesso con priorità più bassa tramite le impostazioni ANY - Deny All.

Test dei modelli di accesso per impostare accuratamente l'attuazione

Migliore pratica	Descrizione
<p>Aggiungere modelli di accesso a un criterio per verificare che al computer sia stato assegnato l'adeguato modello di accesso.</p> <p>Per ulteriori informazioni sul test dei criteri o sulla successiva distribuzione di Sophos NAC, consultare la sezione Distribuzione di Network Access Control a pagina 3.</p>	<p>Assicurarsi che per ogni modello di accesso vengano eseguite le corrette azioni di attuazione relative agli stati di accesso. Verificare che le esenzioni siano effettivamente esenti. Visualizzare i report di Agent Enforcer, DHCP Enforcer, o DHCP Exemption in NAC Manager per verificare quale modello di accesso è stato applicato al computer, la ragione per cui il modello di accesso è stato applicato e i dati relativi all'azione di attuazione.</p>

3.2 Creazione dei modelli di accesso di Agent Enforcer

La pagina Agent Enforcer Access Templates consente di individuare le risorse di rete cui i computer possono o non possono accedere durante la quarantena basata sul client. I modelli di accesso di Agent Enforcer vengono applicati solo ai computer che utilizzano Quarantine Agent.

Le risorse di rete definite nei modelli di accesso di Agent Enforcer regolano l'accesso dei computer alla rete. Per esempio, se una verifica di conformità indica che un computer è risultato non conforme, verrà applicato il modello di accesso di Agent Enforcer associato allo stato del criterio Non-compliant che consentirà o negherà a tale computer l'accesso a determinate risorse di rete. Per ulteriori informazioni sulle risorse di rete, consultare la sezione [Creazione di risorse di rete](#) a pagina 51. Una volta creato un modello di accesso, è possibile assegnarlo ai criteri. Per ulteriori informazioni, consultare la sezione [Aggiornamento dei criteri](#) a pagina 16.

Procedura

1. Cliccare su **Enforce > Agent Enforcer Access Templates**. Quindi, cliccare su **Create Agent Enforcer Access Template** in basso a sinistra nella pagina.
2. Digitare un nome e una descrizione per il modello di accesso di Agent Enforcer.
3. Spuntare la casella accanto allo stato di conformità del modello appropriato per determinare il modo in cui il modello di accesso di Agent Enforcer vada assegnato o designato per la selezione nei criteri.

4. Per specificare le risorse di rete dei computer, seguire una delle seguenti procedure.
 - Cliccare su **Select** per aggiungere le risorse di rete esistenti al modello di accesso, selezionare le risorse di rete appropriate e cliccare su **OK**.
 - Cliccare su **Create** per creare nuove risorse di rete per il modello di accesso, specificare le informazioni nei campi appropriati e cliccare su **Save**. Ripetere eventualmente questo passaggio per creare ulteriori risorse di rete per il modello di accesso. Per ulteriori informazioni, consultare la sezione [Creazione di risorse di rete](#) a pagina 51.
5. Selezionare il comportamento di accesso per ciascuna risorsa di rete. Opzioni disponibili:
 - **Deny**: nega tutto il traffico di rete originato dal computer verso le risorse.
 - **Permit**: permette tutto il traffico di rete originato dal computer verso le risorse.
6. Eventualmente, utilizzare le frecce per determinare la priorità delle risorse di rete.

Se un computer ha più di una risorsa di rete, la prima di tali risorse determina l'accesso alla rete per la sessione del computer. Si consiglia di dare maggiore priorità alle risorse di rete più specifiche e di dare meno priorità a quelle meno specifiche. Le risorse di rete eseguibili vengono valutate prima delle risorse di rete porta/protocollo.
7. Cliccare su **Save**.

Nota: cliccare sul collegamento **View Template Details** per visualizzare le applicazioni e le risorse di rete, in ordine di priorità, associate al modello di accesso di Agent Enforcer. Una volta creato il modello di accesso di Agent Enforcer, è possibile visualizzare i criteri che utilizzano questo modello cliccando sulla relativa opzione del menu del tasto destro del mouse nella pagina **Agent Enforcer Access Templates** o, durante la modifica del modello di accesso, cliccando sul collegamento **View Usage Details**.

3.3 Creazione dei modelli di accesso di DHCP Enforcer

La pagina DHCP Enforcer Access Templates consente di specificare le impostazioni di accesso necessarie per l'attuazione DHCP. I modelli di accesso di DHCP Enforcer vengono utilizzati solo con l'attuazione di DHCP in Sophos NAC.

Se si configura l'attuazione DHCP per la prima volta, si consiglia l'utilizzo della procedura guidata di configurazione di DHCP. Per ulteriori informazioni, consultare la sezione [Esecuzione della procedura guidata di configurazione di DHCP](#) a pagina 49. Se si utilizza la configurazione avanzata di DHCP, è possibile creare o aggiornare i modelli di accesso di DHCP Enforcer esistenti.

Le risorse di rete definite nei modelli di accesso di DHCP Enforcer regolano l'accesso dei computer alla rete. Per esempio, se una verifica di conformità indica che un computer è risultato non conforme, verrà applicato il modello di accesso di DHCP Enforcer associato allo stato del criterio Non-compliant e corrispondente al server DHCP; verrà altrimenti applicato l'indirizzo IP del relay DHCP che consentirà o negherà l'accesso a determinate risorse di rete. Per ulteriori informazioni sulle risorse di rete, consultare la sezione [Creazione di risorse di rete](#) a pagina 51. Una volta creato un modello di accesso, è possibile assegnarlo a criteri, esenzioni o alle impostazioni di Enforcer. Per ulteriori informazioni, consultare le sezioni [Aggiornamento dei criteri](#) a pagina 16, [Creazione di esenzioni](#) a pagina 53, o [Specificazione delle impostazioni di Enforcer](#) a pagina 77.

Procedura

1. Cliccare su **Enforce > DHCP Enforcer Access Templates** . Quindi, cliccare su **Create DHCP Enforcer Access Template** in basso a sinistra nella pagina.
2. Digitare un nome e una descrizione per il modello di accesso di DHCP Enforcer.
3. Spuntare la casella accanto agli stati di conformità del modello appropriati per determinare il modo in cui il modello di accesso di DHCP Enforcer vada assegnato o designato per la selezione in criteri, esenzioni e nelle impostazioni di Enforcer.
4. Selezionare **Full Access** per consentire ai computer pieno accesso alla rete o **Restricted** per indicare specifiche risorse di rete a cui consentire l'accesso. Se si limita l'accesso, si consente l'accesso solo alle risorse di rete specificate, a NAC Server e al server di Dissolvable Agent; è invece negato l'accesso a tutto il resto della rete.
5. Se si seleziona **Restricted** al punto 4, è possibile scegliere di selezionare la casella di spunta **Prevent LAN Access** per evitare che i computer accedano alla rete di area locale (LAN). In aggiunta, eseguire una delle seguenti operazioni, per specificare le risorse di rete a cui si desidera consentire l'accesso:
 - Cliccare su **Select** per aggiungere le risorse di rete esistenti al modello di accesso, selezionare le risorse di rete appropriate e cliccare su **OK**. Solo le risorse di rete porta/protocollo con range di indirizzi IP specifici (non ANY) sono disponibili per la selezione.
 - Cliccare su **Create** per creare nuove risorse di rete per il modello di accesso, specificare le informazioni nei campi appropriati e cliccare su **Save**. Ripetere eventualmente questo passaggio per creare ulteriori risorse di rete per il modello di accesso. Per ulteriori informazioni, consultare la sezione [Creazione di risorse di rete](#) a pagina 51.

Importante: Se un server proxy non è predefinito per l'accesso a Internet come risorsa di rete, l'utente non avrà accesso a Internet, e il modello di accesso predefinito di DHCP - Internet Access DHCP Enforcer fornirà solo correzioni all'accesso. Per ulteriori informazioni, consultare la sezione [Esecuzione della procedura guidata di configurazione di DHCP](#) a pagina 49.

Nota: Se Sophos Enterprise Console è stata installata su un server diverso da quello di Sophos NAC, è necessario creare una risorsa di rete per il server di Sophos Enterprise Console ed aggiungerla al modello di accesso di DHCP, per consentire l'accesso ad essa.

Nota: Tutti i modelli di accesso di DHCP Enforcer consentono l'accesso a un numero prestabilito di route host e di route di rete, determinati da indirizzi IP e di sottorete designati nelle risorse di rete. Se si supera il numero massimo, è possibile risolvere questo problema eliminando risorse di rete dal modello di accesso o rimuovendo route dalle risorse di rete comprese nel modello di accesso.

6. È possibile indicare opzioni DHCP aggiuntive cliccando su **Advanced Options** in basso a sinistra nella pagina. Advanced options comprende:
- **User Class:** questa opzione consente sia di utilizzare la classe utente client di DHCP che di eluderla utilizzando una classe utente specifica. È possibile configurare il server DHCP in modo tale da assegnare gli indirizzi IP in base alla classe utente. Se specificato, la classe utente è applicata ai computer in base allo stato di conformità del computer a cui il modello è associato e precedente all'assegnazione dell'indirizzo IP.
- Importante:**
- Se utilizzata, la classe dell'utente è alfanumerica, distingue fra minuscole e maiuscole e deve coincidere con una delle classi utenti presente nel server DHCP.
 - Se si specifica una classe utente e Quarantine Agent non ha ancora recuperato il criterio secondo il Policy Refresh Interval, è possibile che l'agente non stia utilizzando la classe utente appropriata e, pertanto, non possa ottenere gli indirizzi IP corretti finché non sia avvenuto il recupero del criterio giusto.
 - **Lease Duration:** questa opzione consente sia di utilizzare le impostazioni di lease nel server DHCP che di assegnarne di specifiche.
 - **Server DNS:** questa opzione consente di designare server DNS primari o secondari. È necessaria solo se si utilizza un portale captive. È possibile direzionare gli utenti ospiti o sconosciuti ai server DNS in base allo stato di conformità dei propri computer.
 - **IP Scopes del server DHCP:** questa opzione consente di specificare gli scope IP per cui si utilizzerà il modello di accesso. Spuntare la casella **ANY** o digitare l'inizio e la fine degli indirizzi IP dello scope IP nei campi a disposizione, quindi cliccare su **Add**. Ripetere eventualmente questo passaggio per aggiungere altri ambiti.

7. Cliccare su **Save**.

Nota: una volta creato il modello di accesso di DHCP Enforcer, è possibile visualizzare i criteri, le esenzioni o gli stati di accesso di Enforcer che utilizzano questo modello, cliccando sulla relativa opzione del menu del tasto destro del mouse nella pagina **DHCP Enforcer Access Templates** o, durante la modifica del modello di accesso, cliccando sul collegamento **View Usage Details**.

3.4 Esecuzione della procedura guidata di configurazione di DHCP

La Procedura guidata di configurazione di DHCP aiuta ad identificare i server proxy, di correzione, di Dissolvable Agent e di DHCP Enforcer da utilizzare con le implementazioni di Sophos NAC e a configurare automaticamente i modelli di accesso predefiniti di DHCP in base alle definizioni del proprio server. Se si utilizza la procedura guidata per aggiornare le impostazioni, verrà sovrascritta la configurazione di DHCP corrente e i server predefiniti nei modelli di accesso di DHCP Enforcer verranno sostituiti con quelli definiti nella procedura guidata.

Per ulteriori informazioni su come configurare l'attuazione di DHCP, consultare la *Sophos NAC DHCP di Guida alla configurazione*.

Procedura

1. Cliccare su **Configure System > DHCP Configuration Wizard** . Cliccare su **Avanti** per continuare.
2. 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 4.

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.
3. 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.
4. 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.
5. Effettuare una delle seguenti operazioni:
 - Se Dissolvable Agent è installato, cliccare su **Yes** e successivamente su **Next**. Passare al punto seguente.
 - Se Dissolvable Agent **non** è installato, cliccare su **No** e successivamente su **Next**. Passare al punto 7.

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

6. Definire i server che ospitano 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 di Dissolvable Agent e cliccare su **OK**. Quindi cliccare su **Next**. Una volta creati, questi server possono essere gestiti dalla pagina **Configure System > Server Settings** .
7. Definire i server DHCP nei quali è installato DHCP Enforcer. 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** .
8. Cliccare su **Fine**.

Nota: per impostazione predefinita, i nuovi server di DHCP Enforcer sono impostati per rilevare l'accesso solo di computer sconosciuti. Al fine di attuare l'accesso alla rete per i computer sconosciuti, è necessario modificare la modalità per computer sconosciuto in tutti i server di DHCP Enforcer e selezionare **Enforce** dalla pagina **Configure System > Server Settings** . Per ulteriori informazioni, consultare la sezione [Creazione dei server di DHCP Enforcer](#) a pagina 78.

Nota: per impostazione predefinita, i criteri sono impostati in modo tale da rilevare solo l'accesso dei computer. Per attuare l'accesso alla rete per computer noti, gestiti e non, è necessario cambiare la modalità di tutti i criteri e scegliere **Enforce** dalla pagina **Manage > Policies** . Per ulteriori informazioni, consultare la sezione [Aggiornamento dei criteri](#) a pagina 16.

3.5 Creazione di risorse di rete

Le risorse di rete sono applicazioni o dispositivi necessari per la correzione dei computer o responsabili della negazione dell'accesso alla rete dei computer messi in quarantena. Per esempio, si può scegliere di permettere l'accesso alle applicazioni dei software antivirus o ai file server che ospitano tali applicazioni, oppure di bloccare le applicazioni della posta elettronica aziendale o i dispositivi di rete che utilizzano indirizzi IP pubblici. Le risorse di rete possono essere aggiunte sia ai modelli di accesso di Agent Enforcer che a quelli di DHCP Enforcer. I modelli di accesso possono quindi essere assegnati ai criteri per l'attuazione dell'accesso (permettendo o negando l'accesso) in base allo stato di accesso del computer.

Procedura

1. Cliccare su **Enforce > Network Resources** . Quindi, cliccare su **Create Network Resource** in basso a sinistra nella pagina.
2. Digitare un nome e una descrizione per la risorsa di rete.

3. Cliccare sull'elenco **Network Resource Type** e selezionare **Port/Protocol** o **Executable**.

Per le risorse di rete eseguibili utilizzate nei modelli di accesso di Agent Enforcer, l'agente valuta il traffico generato dal computer al fine di stabilire quali processi consentire e quali negare. Per le risorse di rete porta/protocollo utilizzate nei modelli di accesso di Agent Enforcer o DHCP Enforcer, l'agente o DHCP Enforcer valutano rispettivamente a quali destinazioni consentire o negare l'accesso.

Nota: per ogni applicazione eseguibile è necessario creare una risorsa di rete a parte.

Nota: solo le risorse di rete porta/protocollo sono disponibili per l'attuazione DHCP.

4. Eseguire una delle seguenti procedure.

- Se al punto 3 si è selezionato porta/protocollo, scegliere la categoria del server dall'elenco **Server Category**. Quindi cliccare sull'opzione **ANY** per creare una risorsa di rete applicabile a tutte le porte, cliccare sul pulsante di opzione accanto al campo messo a disposizione e digitare in quest'ultimo una porta specifica; selezionare il protocollo e cliccare su **Add**. Ripetere eventualmente questo passaggio per aggiungere altre porte e protocolli.
- Se al punto 3 è stato selezionato Executable, digitare nel campo **Name** il nome del processo dell'eseguibile dell'applicazione.

Importante:

- Il nome del processo dell'eseguibile **deve** essere lo stesso visualizzato in **Windows Task Manager**, scheda **Processi**.
 - I nomi degli eseguibili **devono** contenere l'estensione .exe, a meno che il nome di un processo non contenga nessuna estensione; **non possono** superare i 64 caratteri; **non possono** utilizzare i seguenti caratteri: \ / : * ? " < > e |; **non possono** contenere informazioni sul percorso dei file; **non** supportano i caratteri jolly; saranno supportati **solo** per i protocolli TCP e UDP.
 - Il software rileva solo gli eseguibili che girano al livello Winsock.
5. È inoltre possibile designare un server di destinazione, selezionare **IP Address** o **Host Name** e digitare, nei relativi campi, l'indirizzo IP, la sottorete opzionale e la descrizione, o il nome host e la descrizione; quindi cliccare su **Add**.

Ripetere eventualmente questo passaggio per aggiungere altri indirizzi IP, sottoreti e nomi host.

Importante: le risorse di rete aventi una maschera di sottorete che **non** è 255.255.255.255 e utilizzate nei modelli di accesso di DHCP Enforcer negheranno l'accesso ai computer che eseguono Windows 2000.

6. Cliccare su **Save**.

Nota: Una volta creata la risorsa di rete, è possibile visualizzare i modelli di accesso che utilizzano questa risorsa cliccando sull'opzione del menu del tasto destro del mouse nella pagina **Network Resources** oppure, durante la modifica della risorsa di rete, cliccando sul collegamento **View Usage Details**.

3.6 Creazione di esenzioni

La pagina relativa alle esenzioni consente di identificare, in base a vari criteri, i computer che non devono essere valutati per conformità quando si connettono alla rete. Le esenzioni includono i computer che non possono eseguire l'agente, quali i computer che utilizzano sistemi operativi non Windows, o quelli che non richiedono verifica della conformità, quali server, router o stampanti. Inoltre, quando si esegue in tutta l'impresa l'attuazione dei criteri per fasi, è possibile escludere i computer o le reti in cui non si desidera ancora applicare questa procedura.

Nota: le esenzioni vengono utilizzate solo con l'attuazione di DHCP.

3.7 Creazione di esenzioni per i criteri DHCP

La pagina Exemptions consente di identificare i computer che non verranno sottoposti alla verifica di conformità al momento di connettersi alla rete. 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. Una volta create le esenzioni, è possibile ordinarle per priorità nella pagina Exemptions.

Procedura

1. Cliccare su **Enforce > Exemptions** . Quindi, cliccare su **Create Exemption** nella pagina in basso a sinistra.
2. Digitare un nome e una descrizione per l'esenzione.
3. Se si desidera disabilitare l'esenzione, selezionare la casella di spunta **Disable Exemption**.

La disabilitazione di un'esenzione consente ai computer di essere valutati in base alla conformità. Se l'esenzione è disabilitata e il computer non ha Sophos Compliance Agent installato, il computer viene considerato sconosciuto.

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. In Access Templates, cliccare su **Select** per aggiungere il modello di accesso esistente di DHCP Enforcer all'esenzione, selezionare i modelli appropriati e cliccare su **OK**.
Se non si trova il modello di accesso di DHCP Enforcer che si sta cercando, è possibile crearlo. Per ulteriori informazioni, consultare la sezione [Creazione dei modelli di accesso di DHCP Enforcer](#) a pagina 47.

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.

3.8 Creazione di esenzioni in base allo scope IP

La pagina Exemptions consente di individuare, in base allo scope IP, i computer che non verranno sottoposti alla verifica di conformità al momento di connettersi alla rete. Le esenzioni per scope IP sono esenzioni create per segmenti di rete. Il modello di accesso di DHCP Enforcer associato determina sia lo scope IP che l'appropriata azione di accesso alla rete da intraprendere. Le esenzioni in base all'ambito IP sono utili per un'attuazione graduale dei criteri di sicurezza aziendali; è possibile così esentare computer o reti che non si desidera ancora rendere conformi. Una volta create le esenzioni, è possibile ordinarle per priorità nella pagina Exemptions.

Procedura

1. Cliccare su **Enforce > Exemptions**. Quindi, cliccare su **Create Exemption** nella pagina in basso a sinistra.
2. Digitare un nome e una descrizione per l'esenzione.
3. Se si desidera disabilitare l'esenzione, selezionare la casella di spunta **Disable Exemption**.

La disabilitazione di un'esenzione consente ai computer di essere valutati in base alla conformità. Se l'esenzione è disabilitata e il computer non ha Sophos Compliance Agent installato, il computer viene considerato sconosciuto.

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 ulteriori informazioni, consultare la sezione [Creazione dei modelli di accesso di DHCP Enforcer](#) a pagina 47.

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

Se a una particolare esenzione è applicato più di uno scope, viene utilizzato il primo di essi. Si consiglia di dare maggiore priorità agli intervalli 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. Si consiglia di dare maggiore priorità alle esenzioni più specifiche e di dare minore priorità a quelle meno specifiche.

3.9 Disabilitazione o abilitazione delle esenzioni

Al momento della loro creazione le esenzioni vengono automaticamente abilitate, a meno che non vengano volutamente disabilitate. La disabilitazione di un'esenzione consente ai computer

di essere valutati in base alla conformità. Se l'esenzione è disabilitata e il computer non ha Sophos Compliance Agent installato, il computer viene considerato sconosciuto.

Procedura

1. Cliccare su **Enforce > Exemptions** .
2. Cliccare sull'elenco **Status** accanto al nome dell'esenzione che si desidera abilitare o disabilitare e successivamente su **Enabled** o **Disabled**.

Nota: per utilizzare un'esenzione predefinita, quale stampante, impostare il suo stato su Enabled.

3. Cliccare su **Save**.

4 Panoramica dell'area Report

L'area Report contiene tutti i componenti necessari per la reportistica relativa a conformità e risoluzione dei problemi. Dal menu Report è possibile accedere alle seguenti aree:

Area e azione	Descrizione
Compliance reports	
Utilizzare i report sulla conformità per visualizzare la conformità dell'utente ai criteri.	<p>I report sulla conformità comprendono dati e report di riepilogo relativi alla conformità.</p> <ul style="list-style-type: none"> ■ I report sulla conformità mostrano i dati dei computer conformi ai criteri e i totali dei computer conformi ai criteri in un dato arco di tempo. Utilizzare i dati delle verifiche associati ai record dei report relativi ai dettagli della conformità per visualizzare i dati concernenti le verifiche della conformità condotte in un determinato computer.
Troubleshooting reports	
Utilizzare i report sulla risoluzione dei problemi per risolvere i problemi di accesso, conformità ai criteri, quarantena ed esenzioni.	<p>I report sulla risoluzione dei problemi sono Agent Session, Non-Compliance Detail, Agent Enforcer, DHCP Enforcer e DHCP Exemption.</p> <ul style="list-style-type: none"> ■ I report Agent Session mostrano tutte le sessioni dell'agente e le verifiche condotte nei computer in un dato arco di tempo. ■ I report Non-Compliance Detail mostrano i dati relativi ai computer che non sono conformi ai criteri. ■ I report Agent Enforcer mostrano l'accesso alla rete utilizzando la quarantena dell'agente in un dato arco di tempo. ■ I report DHCP Enforcer mostrano l'accesso alla rete utilizzando l'attuazione DHCP in un dato arco di tempo. ■ I report DHCP Exemption mostrano le esenzioni DHCP in un dato arco di tempo. ■ I dati della verifica sono inclusi nei report per la risoluzione dei problemi di Agent Session, Non-Compliance Detail, Agent Enforcer e DHCP Enforcer. Utilizzare i dati delle verifiche associati ai record dei report relativi ai dettagli della conformità per visualizzare i dati concernenti le verifiche della conformità condotte in un determinato computer.
Saved reports	
Utilizzare i report salvati per ricreare i report più facilmente.	I report salvati consentono di salvare e riutilizzare le impostazioni comuni dei report in modo tale da non doverle immettere più volte. Tutti i report possono essere salvati e riutilizzati.
Audits	
Visualizzare gli audit per ricercare gli aggiornamenti	Gli audit costituiscono un audit trail, vale a dire la cronologia degli eventi verificatisi all'interno del sistema. Gli eventi comprendono aggiornamenti, nuovi elementi o l'attività del sistema, quali aggiornamenti ai criteri correnti,

Area e azione	Descrizione
agli eventi di sistema.	creazione di nuovi modelli di accesso o account che si connettono o disconnettono da NAC Manager.

4.1 Stampa dei report

È possibile stampare un report creato oppure un record cui si sta accedendo.

Procedura

1. Cliccare su **Report > Compliance or Troubleshooting**.
2. Cliccare sull'elenco **Report Type** e selezionare il nome del report che si desidera stampare.
3. Se pertinente, cliccare sul **segno più** accanto a **Report Criteria** e digitare o selezionare le adeguate opzioni di ricerca. 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 Computer Name, vengono visualizzati tutti i nomi di computer che iniziano con la lettera M. Se invece si specifica M senza il carattere %, vengono visualizzati solo i nomi di computer uguali a M.

4. Cliccare su **Run**.
5. Cliccare su **Stampa**.

4.2 Esecuzione di report Compliance

Utilizzare i report di conformità per sapere quali computer sono conformi ai criteri in un dato arco di tempo. I report Compliance sono utilizzabili per valutare gli andamenti della conformità ai criteri. Sono disponibili due tipi di report Compliance:

- **Compliance Detail:** questo report fornisce il dettaglio dei computer conformi ai criteri in un dato arco di tempo, in base all'ultima sessione dell'agente. È possibile visualizzare i dati della verifica nel report Compliance Detail.
- **Compliance Summary:** questo report fornisce i totali dei computer conformi ai criteri in un dato arco di tempo.

Procedura

1. Cliccare su **Report > Compliance**.
2. Cliccare sull'elenco **Report Type** e selezionare **Compliance Detail** o **Compliance Summary**.

3. Se pertinente, cliccare sul **segno più** accanto a **Report Criteria** e digitare o selezionare le adeguate opzioni di ricerca. 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 Computer Name, vengono visualizzati tutti i nomi di computer che iniziano con la lettera M. Se invece si specifica M senza il carattere %, vengono visualizzati solo i nomi di computer uguali a M.

4. Cliccare su **Run**.

Per ulteriori informazioni sui campi dei risultati del report, consultare la tabella Campi e descrizioni.

Campi e descrizioni

Nota: il report Compliance Summary non contiene tutti i campi descritti sotto. I numeri in ciascun campo visualizzato nel report Compliance Summary rappresentano il numero di istanze di un particolare oggetto.

Campo	Descrizione
Compliance State	Stato di conformità di un computer, assegnato durante la verifica della conformità. Per ulteriori informazioni, consultare la sezione Determinazione dello stato di conformità del computer a pagina 42. 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.
Policy Name	Nome del criterio verificato dall'agente.
Policy Version	Versione del criterio verificato dall'agente. Se la versione del criterio è quella più recente viene visualizzato il valore Latest . Nota: ogni volta che il criterio viene aggiornato, il numero della versione aumenta di una unità.
Computer Name	Nome del computer nel quale l'agente è installato.
Agent ID	Identificativo dell'installazione dell'agente, o del computer, dal quale è stata avviata la sessione. Nota: l'Agent ID è un GUID (Globally Unique Identifier, identificatore unico globale) che identifica in modo univoco ogni installazione dell'agente.
Last Assessment Date/Time	Data e ora della verifica di conformità più recente nell'arco di tempo selezionato per il report. La verifica include le operazioni che verificano e attuano i criteri nei computer. La frequenza della verifica si basa sull'Assess and Enforce Interval impostato nel criterio. Un trattino triplo (---) indica che la sessione dell'agente è continuata oltre l'orario selezionato nelle opzioni di ricerca.

Campo	Descrizione
	Nota: la data e l'ora vengono ricavate dal fuso orario del browser web che accede a NAC Manager.
Associated Reports	Icona che dà accesso ai dati relativi alla verifica di conformità associata alla voce Compliance Detail. Per ulteriori informazioni, consultare la sezione Visualizzazione dei dati della verifica a pagina 70.

4.3 Esecuzione del report Agent Session

Utilizzare il report Agent Session per visualizzare tutte le sessioni e verifiche dell'agente eseguite nei computer in un dato intervallo di tempo. Il report Agent Session è utilizzabile per risolvere i problemi di accesso alla rete o di conformità al criterio. Questo report fornisce i dati relativi alla sessione dell'agente nel computer, alle verifiche della conformità eseguite nel computer e a eventuali cambiamenti dello stato di conformità. Nel report Agent Session è possibile visualizzare le relative voci di Agent Enforcer, DHCP Enforcer oppure i dati della verifica.

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

Procedura

1. Cliccare su **Report > Troubleshooting**.
2. Cliccare sull'elenco **Report Type** e selezionare **Agent Session**.
3. Se pertinente, cliccare sul **segno più** accanto a **Report Criteria** e digitare o selezionare le adeguate opzioni di ricerca. 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 Computer Name, vengono visualizzati tutti i nomi di computer che iniziano con la lettera M. Se invece si specifica M senza il carattere %, vengono visualizzati solo i nomi di computer uguali a M.

4. Cliccare su **Run**.

Per ulteriori informazioni sui campi dei risultati del report, consultare la tabella Campi e descrizioni.

Campi e descrizioni

Campo	Descrizione
Voce del report riepilogativo	
Computer Name	Nome del computer nel quale l'agente è installato.

Campo	Descrizione
Agent ID	Identificativo dell'installazione dell'agente, o del computer, dal quale è stata avviata la sessione. Nota: l'Agent ID è un GUID (Globally Unique Identifier, identificatore unico globale) che identifica in modo univoco ogni installazione dell'agente.
MAC Address	Indirizzi MAC del computer nel quale l'agente è installato. Nel report, ogni indirizzo MAC è assegnato alla stessa NIC dell'indirizzo IP accanto.
Indirizzo IP	Indirizzi IP del computer nel quale l'agente è installato. Nel report, ogni indirizzo IP è assegnato alla stessa NIC dell'indirizzo MAC accanto. Un trattino triplo (---) indica che la NIC non è in possesso di alcun indirizzo IP.
Sistema operativo	Il sistema operativo installato nel computer.
Session Start	Data e ora in cui l'agente comincia la sessione con Sophos NAC in un computer. Nota: la data e l'ora vengono ricavate dal fuso orario del browser web che accede a NAC Manager.
Session End	Data e ora in cui l'agente termina la sessione con Sophos NAC in un computer. Un trattino triplo (---) indica che la sessione dell'agente non è terminata. Nota: la data e l'ora vengono ricavate dal fuso orario del browser web che accede a NAC Manager.
Voce del report nel dettaglio	
Assessment Start	Data e ora della prima istanza dei risultati delle verifiche di conformità nell'intervallo di tempo selezionato per il report. La verifica include le operazioni che verificano e attuano i criteri nei computer. La frequenza della verifica si basa sull'Assess and Enforce Interval impostato nel criterio. Nota: la data e l'ora vengono ricavate dal fuso orario del browser web che accede a NAC Manager.
Assessment End	Data e ora dell'ultima istanza dei risultati delle verifiche di conformità nell'intervallo di tempo selezionato per il report. La verifica include le operazioni che verificano e attuano i criteri nei computer. Un trattino triplo (---) indica che la verifica della conformità non è terminata. Nota: la data e l'ora vengono ricavate dal fuso orario del browser web che accede a NAC Manager.
Count	Numero delle verifiche di conformità intercorse senza alcun cambiamento nei risultati della verifica. Questo numero è il conteggio delle volte in cui l'agente ha eseguito la verifica della conformità, in base all'Assess and Enforce Interval impostato nel criterio.

Campo	Descrizione
Compliance State	Stato di conformità di un computer, assegnato durante la verifica della conformità. Per ulteriori informazioni, consultare la sezione Determinazione dello stato di conformità del computer a pagina 42. 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.
Policy Name	Nome del criterio verificato dall'agente.
Policy Version	Versione del criterio verificato dall'agente. Se la versione del criterio è quella più recente viene visualizzato il valore Latest . Nota: ogni volta che il criterio viene aggiornato, il numero della versione aumenta di una unità.
Associated Reports	Icona che dà accesso alle voci di Agent Enforcer, DHCP Enforcer o ai dati riguardanti la verifica della conformità associata a questa voce di Agent Session. L'icona viene visualizzata solo se è disponibile una voce associata. Per ulteriori informazioni, consultare le sezioni Esecuzione del report Agent Enforcer a pagina 62, Esecuzione del report DHCP Enforcer a pagina 64, o Visualizzazione dei dati della verifica a pagina 70.

4.4 Esecuzione del report Non-Compliance Detail

Utilizzare il report Non-Compliance Detail per visualizzare i computer che sono non conformi o parzialmente conformi ai criteri in un dato arco di tempo, basato sull'ultima sessione dell'agente del computer. Il report Non-Compliance Detail è utilizzabile per individuare rapidamente i computer che non sono pienamente conformi ai criteri e la causa della mancata conformità. È possibile visualizzare i dati della verifica nel report Non-Compliance Detail.

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

Procedura

1. Cliccare su **Report > Troubleshooting**.
2. Cliccare sull'elenco **Report Type** e selezionare **Non-Compliance Detail**.
3. Se pertinente, cliccare sul **segno più** accanto a **Report Criteria** e digitare o selezionare le adeguate opzioni di ricerca. 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 Computer Name, vengono visualizzati tutti i nomi di computer che iniziano con la lettera M. Se invece si specifica M senza il carattere %, vengono visualizzati solo i nomi di computer uguali a M.

4. Cliccare su **Run**.

Per ulteriori informazioni sui campi dei risultati del report, consultare la tabella Campi e descrizioni.

Campi e descrizioni

Campo	Descrizione
Voce del report riepilogativo	
Computer Name	Nome del computer nel quale l'agente è installato.
Compliance State	Stato di conformità di un computer, assegnato durante la verifica della conformità. Per ulteriori informazioni, consultare la sezione Determinazione dello stato di conformità del computer a pagina 42. Gli stati di conformità disponibili sono Partially Compliant e Non-Compliant. Un trattino triplo (---) indica che l'agente non ha registrato alcuno stato di conformità.
Associated Reports	Icona che dà accesso ai dati relativi alla verifica di conformità associata alla voce Non-Compliance Detail. Per ulteriori informazioni, consultare la sezione Visualizzazione dei dati della verifica a pagina 70.
Voce del report nel dettaglio	
Profile Name	Nome del profilo che l'agente ha tentato di rilevare nel computer. Il tipo di profilo associato viene visualizzato fra parentesi.
Capability	Funzione del profilo per il quale il computer è stato riscontrato parzialmente conforme o non conforme.
Compliance State	Stato di conformità rilevato solo se nel computer è rispettata la condizione. Gli stati di conformità disponibili sono Partially Compliant e Non-Compliant. Un trattino triplo (---) indica che l'agente non ha registrato alcuno stato di conformità.

4.5 Esecuzione del report Agent Enforcer

Utilizzare il report Agent Enforcer per visualizzare l'accesso alla rete tramite l'attuazione della quarantena dell'agente in un dato arco di tempo. Il report Agent Enforcer è utilizzabile per risolvere i problemi legati alla quarantena in uno o più computer. Questo report fornisce dati relativi allo stato di conformità dei computer, al modello di accesso associato e al motivo per cui un particolare modello di accesso è stato applicato. È possibile visualizzare i dati della verifica nel report Agent Enforcer.

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

Procedura

1. Cliccare su **Report > Troubleshooting**.

2. Cliccare sull'elenco **Report Type** e selezionare **Agent Enforcer**.
3. Se pertinente, cliccare sul **segno più** accanto a **Report Criteria** e digitare o selezionare le adeguate opzioni di ricerca. 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 Computer Name, vengono visualizzati tutti i nomi di computer che iniziano con la lettera M. Se invece si specifica M senza il carattere %, vengono visualizzati solo i nomi di computer uguali a M.

4. Cliccare su **Run**.

Per ulteriori informazioni sui campi dei risultati del report, consultare la tabella Campi e descrizioni.

Campi e descrizioni

Campo	Descrizione
Date/Time	Data e ora in cui lo stato di attuazione di Agent Enforcer è cambiato. Nota: la data e l'ora vengono ricavate dal fuso orario del browser web che accede a NAC Manager.
Agent ID	Identificativo dell'installazione dell'agente, o del computer, da cui è stato riportato il cambiamento dello stato dell'attuazione. Nota: l'Agent ID è un GUID (Globally Unique Identifier, identificatore unico globale) che identifica in modo univoco ogni installazione dell'agente.
Computer Name	Nome del computer nel quale l'agente è installato.
Compliance State	Stato di conformità di un computer, assegnato durante la verifica della conformità. Per ulteriori informazioni, consultare la sezione Determinazione dello stato di conformità del computer a pagina 42. 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 dell'Agent Enforcer conformi associati allo stato di conformità del criterio.
Template Name (Version)	Nome e versione del modello di accesso che determina l'azione intrapresa da Agent Enforcer. Il modello di accesso utilizzato si basa sul motivo. Per ulteriori informazioni, consultare la sezione Creazione dei modelli di accesso di Agent Enforcer a pagina 46. I modelli di accesso disponibili includono i seguenti modelli predefiniti, oltre che i modelli personalizzati: <ul style="list-style-type: none"> ■ Default - Agent and Internet Access Only: modello di accesso di Agent Enforcer utilizzato per dare accesso a tutti i prodotti Sophos e a Internet nelle reti interne che utilizzano indirizzi IP privati, e per negare l'accesso a tutto il resto del traffico in uscita.

Campo	Descrizione
	<ul style="list-style-type: none"> ■ Default - Agent Permit All: modello di accesso di Agent Enforcer utilizzato per permettere tutto il traffico in uscita. ■ None: impostazione di accesso predefinita che consente tutto il traffico in uscita nel caso in cui i modelli Default - Agent and Internet Access Only e Default - Agent Permit All siano stati rimossi dal criterio e non sia stato selezionato nessun modello specifico per l'azienda. L'impostazione di accesso None assicura che l'agente possa accedere al NAC Server.
Reason	<p>Motivo per cui un particolare modello di accesso è stato assegnato da Agent Enforcer. Motivi disponibili:</p> <ul style="list-style-type: none"> ■ Assessment: la verifica eseguita dall'agente ha determinato lo stato di conformità. L'accesso alla rete è determinato dal modello di accesso di Agent Enforcer associato allo stato di conformità del criterio. Viene visualizzato un collegamento che dà accesso ai dati relativi alla verifica di conformità associati a questa voce di Agent Enforcer. ■ No Agent Tray: l'agente non è attualmente in esecuzione nel computer. Questo stato viene segnalato da Agent Enforcer nel caso in cui l'utente non sia connesso a Windows oppure l'applicazione dell'agente nell'area di notifica non sia più in esecuzione. L'accesso alla rete è determinato dal modello di accesso del criterio di Agent Enforcer associato allo stato No Agent Tray. ■ Policy Retrieval Error: non è stato possibile recuperare un criterio per il computer. Questo stato può esistere se l'agente non riesce a recuperare il criterio da NAC Server; oppure lo stato di conformità del computer non è aggiornato secondo il campo Agent Policy Update Threshold configurato nell'area Configure System > Enforcer Settings . ■ Remediate: il criterio è in modalità Remediate. L'accesso alla rete è determinato dal modello di accesso di Agent Enforcer associato alla modalità Remediate del criterio. ■ Report Only: il criterio è in modalità Report Only. L'accesso alla rete è determinato dal modello di accesso di Agent Enforcer associato alla modalità Report Only del criterio. ■ User Override: nel computer, l'utente ha ignorato la quarantena dell'agente. L'accesso alla rete è determinato dal modello di accesso associato allo stato dell'agente User Override.

4.6 Esecuzione del report DHCP Enforcer

Utilizzare il report DHCP Enforcer per visualizzare l'accesso alla rete tramite attuazione DHCP in un dato arco di tempo. Il report DHCP Enforcer è utilizzabile per risolvere i problemi di accesso alla rete. Questo report fornisce dati relativi allo stato di conformità dei computer, al modello di accesso associato e al motivo per cui un particolare modello di accesso è stato applicato. Dal report DHCP Enforcer è possibile rendere esenti i dispositivi e accedere ai dati di rilevamento.

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

Procedura

1. Cliccare su **Report > Troubleshooting**.
2. Cliccare sull'elenco **Report Type** e selezionare **DHCP Enforcer**.
3. Se pertinente, cliccare sul **segno più** accanto a **Report Criteria** e digitare o selezionare le adeguate opzioni di ricerca. 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.

4. Cliccare su **Run**.

Per ulteriori informazioni sui campi dei risultati del report, consultare la tabella Campi e descrizioni. Per informazioni relative all'esenzione dei dispositivi da questo report, consultare la sezione [Creazione di esenzioni dai report](#) a pagina 69.

Campi e descrizioni

Campo	Descrizione
Voce del report riepilogativo	
Date/Time	Data e ora del tentativo di accesso alla rete. Nota: 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. Per ulteriori informazioni, consultare la sezione Determinazione dello stato di conformità del computer a pagina 42. 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)	Nome e versione del modello di accesso che determina l'azione intrapresa dall'Agent Enforcer. Il modello di accesso utilizzato si basa sul motivo. Per

Campo	Descrizione
	<p>ulteriori informazioni, consultare la sezione Creazione dei modelli di accesso di DHCP Enforcer a pagina 47. I modelli di accesso disponibili includono i seguenti modelli predefiniti, oltre che i modelli personalizzati:</p> <ul style="list-style-type: none"> ■ DHCP - Full Access: consente pieno accesso alla rete. ■ DHCP - Internet Access: consente accesso a Internet, e nega l'accesso agli indirizzi IP privati e alla rete di area locale (LAN). <p>Importante: 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. Per ulteriori informazioni, consultare la sezione Esecuzione della procedura guidata di configurazione di DHCP a pagina 49.</p> <ul style="list-style-type: none"> ■ DHCP - Remediation Access: nega qualsiasi accesso alla rete, eccezion fatta per i server di correzione specificati, NAC Server, e il server di Dissolvable Agent.
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"> ■ Assessment: 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. ■ Default Template: 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 Configure System > Enforcer Settings . ■ Enforcer Override: l'attuazione non è stata verificata. Se la casella Override DHCP Enforcer nell'area Configure System > Enforcer Settings è spuntata, l'accesso alla rete è determinato dai modelli di accesso Maintenance Mode/Enforcer Override, designati nella medesima area. ■ Exempted: il computer è esentato in base ai criteri di esenzione definiti nell'area Enforce > Exemptions . 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"> ■ User Class: la classe dell'utente specificata come esenzione. ■ Vendor Class: la classe del fornitore specificata come esenzione. ■ MAC: l'indirizzo MAC specificato come esenzione. ■ IP Scope: l'ambito IP specificato come esenzione. ■ Maintenance Mode: il software è in modalità manutenzione. L'accesso alla rete è determinato dai modelli di accesso Maintenance Mode/Enforcer Override designati nell'area Configure System > Enforcer Settings .

Campo	Descrizione
	<ul style="list-style-type: none"> ■ 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 . L'accesso alla rete è determinato dai modelli di accesso di DHCP Enforcer del criterio e associati allo stato Policy Retrieval Error. ■ Remediate: 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. ■ Report Only: 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. ■ Reserved: l'indirizzo MAC del dispositivo che richiede accesso alla rete è riservato come dispositivo speciale nel server DHCP. ■ System Error: Enforcer ha riscontrato un errore che ha impedito il completamento dell'operazione. L'impostazione del registro SystemErrors del NAC Server nega l'accesso alla rete per impostazione predefinita. ■ Template Error: non è stato rilevato alcun modello associato e i modelli di accesso predefiniti designati nell'area Configure System > Enforcer Settings 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. ■ Unknown Endpoint: non esiste alcun dato relativo alla conformità. L'accesso alla rete è determinato dai modelli di accesso Unknown Endpoint designati nell'area Configure System > Enforcer Settings .
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.
Voce del report nel dettaglio	
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"> ■ None: gli indirizzi IP per il computer non sono né rilasciati né rinnovati. ■ 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. ■ Triple Dash (---): l'agente non ha registrato alcuna azione.

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.

4.7 Esecuzione del report DHCP Exemption

Utilizzare il report DHCP Exemption per visualizzare le esenzioni DHCP entro un determinato periodo di tempo. Il report DHCP Exemption è utilizzabile per risolvere i problemi di accesso alla rete specifici delle esenzioni.

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

Procedura

1. Cliccare su **Report > Troubleshooting**.
2. Cliccare sull'elenco **Report Type** e selezionare **DHCP Exemption**.
3. Se pertinente, cliccare sul **segno più** accanto a **Report Criteria** e digitare o selezionare le adeguate opzioni di ricerca. 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.

4. Cliccare su **Run**.

Per ulteriori informazioni sui campi dei risultati del report, consultare la tabella Campi e descrizioni.

Campi e descrizioni

Campo	Descrizione
Voce del report riepilogativo	

Campo	Descrizione
Date/Time	Data e ora del tentativo di accesso alla rete. Nota: la data e l'ora vengono ricavate dal fuso orario del browser web che accede a NAC Manager.
Template Name (Version)	Nome del modello di accesso che determina l'azione intrapresa da DHCP Enforcer. Per ulteriori informazioni, consultare la sezione Creazione dei modelli di accesso di DHCP Enforcer a pagina 47.
Exemption Condition Name	Nome dell'esenzione e dei dati del criterio di esenzione.
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.
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.
Voce del report nel dettaglio	
Source User Class	Classe dell'utente DHCP, se presente, che viene inviata al server DHCP dal client DHCP.
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.

4.8 Creazione di esenzioni dai report

È possibile creare esenzioni dai report di DHCP Enforcer per i dispositivi rilevati durante l'attuazione DHCP.

Le esenzioni vengono visualizzate nel report di DHCP Enforcer basato su "Exempted". Se i dispositivi vengono esentati dal report, non verranno visualizzati come esenti fino a quando non tenteranno di riconnettersi alla rete. Per ulteriori informazioni su campi e descrizioni dei report di DHCP Enforcer, consultare la sezione [Esecuzione del report DHCP Enforcer](#) a pagina 64.

Procedura

1. Cliccare su **Report > Troubleshooting**.
2. Cliccare sull'elenco **Report Type** e selezionare **DHCP Enforcer**.

3. Se pertinente, cliccare sul **segno più** accanto a **Report Criteria** e digitare o selezionare le adeguate opzioni di ricerca. 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.

4. Cliccare su **Run**.
5. Cliccare sulla casella di spunta di fianco ai dispositivi che si desidera esentare e poi cliccare su **Exempt**.
6. Confermare l'elenco dei dispositivi che si desidera esentare, selezionare il modello di accesso che si desidera applicare alle esenzioni e cliccare su **OK**.

Per gestire o applicare modelli di accesso aggiuntivi alle esenzioni create, andare all'area **Enforce > Exemptions**. Per ulteriori informazioni, consultare la sezione [Creazione di esenzioni per i criteri DHCP](#) a pagina 53.

4.9 Visualizzazione dei dati della verifica

Utilizzare i dati della verifica per visualizzare i dati realtivi alle verifiche di conformità eseguite nel computer.

È possibile visionare i dati della verifica da i seguenti report: Compliance Detail, Agent Session, Non-Compliance Detail, Agent Enforcer o DHCP Enforcer. I dati della verifica visualizzati sono associati alla voce del report dalla quale sono stati richiamati. I dati della verifica mostrano le condizioni del profilo testate nel computer, i relativi risultati, lo stato di conformità assegnato in base alla verifica e qualsiasi azione eseguita nel computer.

Procedura

1. Cliccare su **Report > Compliance o Troubleshooting**.
2. Cliccare sull'elenco **Report Type** e selezionare **Compliance Detail, Agent Session, Non-Compliance Detail, Agent Enforcer, o DHCP Enforcer**.
3. Se pertinente, cliccare sul **segno più** accanto a **Report Criteria** e digitare o selezionare le adeguate opzioni di ricerca. 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 Computer Name, vengono visualizzati tutti i nomi di computer che iniziano con la lettera M. Se invece si specifica M senza il carattere %, vengono visualizzati solo i nomi di computer uguali a M.

4. Cliccare su **Run**.
5. Solo nel report Agent Session, cliccare sul **segno più** accanto alla voce di un report riepilogativo per visualizzare la relativa voce del report dettagliato.

6. Cliccare sull'icona **Assessment Details** o sul collegamento **Assessment**, a seconda del report.

Per ulteriori informazioni sui campi dei risultati del report, consultare la tabella Campi e descrizioni.

Campi e descrizioni

Campo	Descrizione
Dati della verifica del tipo di profilo	
Profile Type	Tipo di profilo che l'agente ha tentato di rilevare nel computer.
Compliance State	Stato di conformità del tipo di profilo. Questo stato di conformità si compone dei profili valutati nel computer e del comportamento del criterio Required, Best o All. Per ulteriori informazioni, v. Selection Reason in basso. 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.
Dati della verifica del profilo	
Profile Name	Nome del profilo che l'agente ha tentato di rilevare nel computer.
Selected	Specifica se il profilo è stato utilizzato per determinare lo stato di conformità per il tipo di profilo. Se il valore è True, il profilo è stato utilizzato. Se il valore è False, il profilo non è stato utilizzato e per determinare lo stato di conformità è stato utilizzato un altro profilo. Per ulteriori informazioni sulla modalità di valutazione dei profili nel computer, v. Selection Reason in basso.
Selection Reason	<p>Specifica perché il profilo è stato utilizzato o meno per determinare lo stato di conformità per il tipo di profilo. Si basa sul comportamento del criterio, che determina la modalità di valutazione dei profili in base agli altri profili dello stesso tipo presenti nel computer. I valori disponibili sono:</p> <ul style="list-style-type: none"> ■ Required (Best): visualizzato se nel computer viene rilevato il profilo del sistema operativo richiesto. Il profilo del sistema operativo è necessario ed è valutato come migliore profilo. ■ Best: visualizzato se nel computer viene rilevato il profilo migliore. Nel computer viene verificato ciascun profilo di un particolare tipo nel criterio, viene stabilita la migliore corrispondenza e infine vengono intraprese solo le azioni garantite associate al 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 diagnosticati, vengono valutati in questo modo. ■ Best (No Match): visualizzato se una valutazione Best non rileva alcun profilo nel computer. Se nel computer non è installato nessuno dei profili da verificare, per determinare lo stato di conformità e le azioni per il tipo di profilo nel criterio, viene utilizzato lo stato di conformità della condizione Else del profilo a priorità più elevata. Nel caso in cui uno dei

Campo	Descrizione
	<p>sistemi operativi necessari non sia installato nel computer, per determinare lo stato di conformità e le azioni per il tipo di profilo del sistema operativo viene utilizzato lo stato di conformità della condizione Else nel profilo di sistema operativo a priorità più alta; per quel criterio non verranno valutati altri profili.</p> <ul style="list-style-type: none"> ■ All: visualizzato se nel computer vengono valutati tutti i profili. 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 dell'applicazione che si desidera escludere dal computer possono essere valutati in questo modo.
Detected	Indica se l'oggetto del profilo (sistema operativo o applicazione) è stato rilevato nel computer. Se il valore è True, l'oggetto del profilo è stato rilevato. Se il valore è False, non è stato rilevato.
Compliance State	Stato di conformità del profilo. Questo stato di conformità è composto dalle condizioni del profilo valutate nel computer. Tutte le condizioni vengono valutate per determinare lo stato di conformità del profilo. 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.
Dati della verifica della funzione del profilo	
Profile Condition	Visualizza una condizione configurata nel profilo confrontandola con il risultato del rilevamento nel computer. Il risultato può essere costituito da una versione, un numero o una data o qualsiasi altro oggetto che delinea la condizione nel computer. Un trattino triplo (---) indica che la condizione non possiede un delineatore.
Risultato	Risultato della valutazione della condizione. Se il risultato è True, la condizione definita nel profilo è soddisfatta nel computer. Se il risultato è False, la condizione non è soddisfatta nel computer.
Compliance State	Stato di conformità rilevato solo se nel computer è rispettata la condizione. 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.
Action Type	<p>Tipo di azione correttiva eseguita nel computer. Le azioni vengono visualizzate o eseguite nel computer solo se la condizione, cui l'azione è associata, vengono soddisfatte. Tipi di azione disponibili:</p> <ul style="list-style-type: none"> ■ Message: visualizza un messaggio nel computer. Questa azione è disponibile per tutte le funzioni. ■ Enable: nel computer, abilita la protezione in tempo reale per le applicazioni antivirus o antispyware, il firewall per le applicazioni firewall

Campo	Descrizione
	<p>oppure gli aggiornamenti automatici per le applicazioni Patch Manager. Questa azione è disponibile sia per la funzione Real-Time Protection che Enabled.</p> <ul style="list-style-type: none"> ■ Update: aggiorna il file della firma nel computer. Questa azione è disponibile per la funzione Signature Date o per la funzione Signature Grace Period dell'applicazione. ■ Scan: avvia un motore di scansione nel computer. Questa azione è disponibile per la funzione Scan Date o Scan Grace Period dell'applicazione. ■ Apply: applica il criterio di Sophos Enterprise Console per l'applicazione di Sophos Anti-Virus sul computer endpoint. Questa azione è disponibile per la funzione dell'applicazione di SEC Policy.
Action Value	Messaggio visualizzato all'utente. Nel computer viene visualizzato un messaggio solo se la relativa condizione viene soddisfatta. Nessun altro tipo di azione presenta un valore.

4.10 Salvataggio dei report

È possibile salvare i report personalizzando i criteri di ricerca e di ordinamento di un report esistente a seconda delle proprie necessità. Il criterio viene salvato durante il salvataggio del report.

Procedura

1. Cliccare su **Report > Compliance or Troubleshooting**.
2. Cliccare sull'elenco **Report Type** e selezionare il nome del report che si desidera salvare.
3. Se pertinente, cliccare sul **segno più** accanto a **Report Criteria** e digitare o selezionare le adeguate opzioni di ricerca. 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 Computer Name, vengono visualizzati tutti i nomi di computer che iniziano con la lettera M. Se invece si specifica M senza il carattere %, vengono visualizzati solo i nomi di computer uguali a M.

4. Cliccare su **Run**.
5. Cliccare su **Save**.
6. Nella finestra di dialogo, digitare il nome del report nel campo **Report Name**.
7. Cliccare su **Save**.

4.11 Esecuzione dei report salvati

I report salvati consentono di salvare e riutilizzare le impostazioni comuni dei report in modo tale da non doverle immettere più volte. È possibile inoltre aggiornare le impostazioni dei report per quelli salvati senza dover salvarne di nuovi.

Procedura

1. Cliccare su **Report > Saved**.
2. Cliccare sull'elenco **Saved Report** e selezionare il nome del report salvato che si desidera eseguire.
3. Se pertinente, cliccare sul **segno più** accanto a **Report Criteria** e digitare o selezionare le adeguate opzioni di ricerca. 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 Computer Name, vengono visualizzati tutti i nomi di computer che iniziano con la lettera M. Se invece si specifica M senza il carattere %, vengono visualizzati solo i nomi di computer uguali a M.

4. Cliccare su **Run**.

4.12 Cancellazione dei report salvati

La cancellazione dei report salvati li rimuove completamente dal software.

Procedura

1. Cliccare su **Report > Saved**.
2. Cliccare sull'elenco **Saved Report** e selezionare il nome del report salvato che si desidera cancellare.
3. Cliccare su **Delete**.
4. Nella finestra di dialogo, cliccare su **OK** per confermare la cancellazione.

4.13 Visualizzazione degli audit

L'area Audits fornisce un audit trail, o cronologia, degli eventi verificatisi nel sistema. Gli eventi comprendono aggiornamenti, nuovi elementi o l'attività del sistema, quali aggiornamenti ai criteri correnti, creazione di nuovi modelli di accesso o account che si connettono o disconnettono da NAC Manager.

Procedura

1. Cliccare su **Report > Audit**.
2. Digitare o selezionare le appropriate opzioni di ricerca nei campi forniti e cliccare su **Search**.

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 Item Name, vengono visualizzati tutti i nomi di oggetto che iniziano con la lettera M.

3. Effettuare una delle seguenti operazioni:
 - Per ordinare l'elenco, cliccare sull'intestazione di colonna appropriata.
 - Per visualizzare i dati dell'audit relativi a un evento, cliccare sul collegamento **Details**.

5 Panoramica dell'area Configure System

L'area Configure System include tutti i componenti necessari per la configurazione dei componenti di sistema di NAC Manager. Dal menu Configure System è possibile accedere alle seguenti aree:

Area e azione	Descrizione
Accounts	
Creazione di account di sistema.	Account consente diversi livelli di accesso a NAC Manager. L'amministratore di sistema può creare i nomi e i ruoli di protezione degli account di sistema. Il nome dell'account e la password vengono utilizzati per accedere a NAC Manager. I ruoli di protezione stabiliscono il livello dei privilegi di ogni account.
Disabilitazione o abilitazione degli account.	Gli account possono essere disabilitati o abilitati dall'amministratore di sistema. La disabilitazione di un account impedisce che l'utente di tale account acceda a NAC Manager per visualizzare informazioni di sistema o svolgere qualsiasi funzione di amministratore. L'abilitazione di un account consente all'utente di tale account di accedere a NAC Manager e svolgere le funzioni di amministrazione assegnate dal ruolo di protezione dell'account.
Enforcer settings	
Specificazione delle impostazioni di Enforcer.	Enforcer settings specifica i dati relativi all'attuazione per i tipi di attuazione di Agent Enforcer e DHCP Enforcer. Agent Enforcer viene utilizzato per l'applicazione della quarantena basata sul client. DHCP Enforcer viene utilizzato con le implementazioni DHCP di Sophos NAC.
Server settings	
Creazione dei server di DHCP Enforcer.	Utilizzare questa area per definire i server di DHCP Enforcer in modo tale che vengano utilizzati con le implementazioni di DHCP in Sophos NAC. Si tratta dei server DHCP nei quali è installato DHCP Enforcer.
Creazione dei server di Dissolvable Agent.	Utilizzare questa area per definire i server ospitanti Dissolvable Agent in modo tale che DHCP Enforcer ne possa concedere l'accesso.
Aggiornamento delle impostazioni del server proxy di NAC.	Durante l'installazione di NAC, NAC può essere configurato in modo da utilizzare un server proxy per l'accesso a internet. Per ottenere le informazioni più aggiornate relative al rilevamento delle applicazioni di sicurezza, è necessario avere accesso a Internet. Utilizzare questa area per aggiornare le impostazioni di proxy e, se lo si desidera, gli indirizzi IP del NAC Server.
Download account details	
Aggiornamento dei dettagli dell'account di download.	Il nome utente e la password dell'account di download sono utilizzati da NAC per scaricare le informazioni più aggiornate relative al rilevamento delle applicazioni di sicurezza.

5.1 Creazione degli account

L'area Accounts consente agli amministratori di sistema di creare nome e ruoli di sicurezza per gli account del sistema. Il nome dell'account e la password vengono utilizzati per accedere a NAC Manager. I ruoli di protezione stabiliscono il livello dei privilegi di ogni account.

Procedura

1. Cliccare su **Configure System > Accounts** . Quindi, cliccare su **Create Account** in basso a sinistra nella pagina.
2. Digitare il nome dell'account.
3. Facoltativamente, spuntare la casella **Disable Account** per creare un account disabilitato.
4. Digitare e confermare la password relativa all'account.

Nota: se si aggiorna la password di un account esistente, bisogna digitare anche la password del proprio account. Questo campo assicura che solo gli amministratori di sistema con account validi possano aggiornare le password degli account.

5. Selezionare uno dei seguenti ruoli di sicurezza:
 - **System Administrator:** possiede diritti di accesso completi per tutte le aree di NAC Manager. Gli amministratori di sistema possono creare, aggiornare o cancellare gli account.
 - **Administrator:** possiede diritti di accesso completi per le aree Manage, Report ed Enforce di NAC Manager. Possiede diritti di sola lettura per l'area Configure System di NAC Manager. Il ruolo di sicurezza Administrator non può visualizzare né gestire gli account.
 - **Help Desk:** possiede diritti di accesso completi per le aree Report di NAC Manager. Possiede diritti di sola lettura per le aree Manage, Enforce e Configure System di NAC Manager. Il ruolo di sicurezza Help Desk non può visualizzare né gestire gli account.
 - **Guest:** possiede diritti di sola lettura per tutte le aree di NAC Manager. Il ruolo di sicurezza Guest non può visualizzare né gestire gli account.

Nota: tutti i ruoli di sicurezza possono accedere alle funzioni dell'utilità di navigazione, comprese le password dei propri account, la Guida in linea e le informazioni su NAC Manager.

6. Cliccare su **Save**.

5.2 Abilitazione e disabilitazione degli account

Al momento della loro creazione gli account vengono automaticamente abilitati, a meno che li si disabiliti esplicitamente. La disabilitazione di un account impedisce che l'utente di tale account acceda a NAC Manager per visualizzare informazioni di sistema o svolgere qualsiasi funzione di amministratore.

Procedura

1. Cliccare su **Configure System > Accounts** .
2. Cliccare sull'icona **Enabled Account** o **Disabled Account** accanto al nome dell'account che si desidera abilitare o disabilitare. L'icona visualizza lo stato corrente.

5.3 Specificazione delle impostazioni di Enforcer

La pagina Enforcer Settings consente di configurare le impostazioni che specificano le modalità di attuazione per DHCP Enforcer o Agent Enforcer. DHCP Enforcer viene utilizzato con le implementazioni DHCP di Sophos NAC. Agent Enforcer viene utilizzato per l'applicazione della quarantena basata sul client.

Procedura

1. Cliccare su **Configure System > Enforcer Settings**.
2. Se si sta utilizzando Agent Enforcer, specificare la seguente impostazione per la soglia dei criteri. Se si sta utilizzando anche DHCP Enforcer, passare al punto seguente, altrimenti al 7:
 - **Agent Policy Update Threshold:** specifica il tempo (in minuti, ore o giorni) a disposizione di Quarantine Agent per recuperare il criterio prima che il computer venga messo in quarantena. Se viene superato il livello di soglia, il computer viene messo in quarantena e si rende necessario un nuovo recupero del criterio. Nel frattempo l'accesso alla rete è determinato dal modello di accesso di Agent Enforcer associato allo stato di accesso Policy Retrieval Error del criterio. Questo livello di soglia viene utilizzata per l'attuazione dell'agente. Il valore predefinito è 8 ore. Il valore predefinito è 1.
Importante: il valore impostato per il livello di soglia di aggiornamento del criterio deve essere sempre **superiore** all'intervallo di aggiornamento specificato per ciascun criterio; altrimenti, ad ogni raggiungimento della soglia, l'accesso alla rete viene determinato dallo stato Policy Retrieval Error del criterio e il computer viene messo in quarantena (se si utilizza il Quarantine Agent).
3. Specificare le seguenti impostazioni per la soglia dei criteri di DHCP Enforcer:
 - **DHCP Policy Update Threshold:** specifica il tempo (in minuti, ore o giorni) che intercorre fra il recupero del criterio da parte dell'agente e la sua scadenza. Se scade, viene richiesto un nuovo recupero del criterio. Nel frattempo l'accesso alla rete è determinato dal modello di accesso di DHCP Enforcer associato allo stato di accesso Policy Retrieval Error del criterio. Questo livello di soglia viene utilizzata per l'attuazione DHCP. Se impostato sul valore 0, questo livello di soglia risulta disabilitato. Il valore predefinito è 5 ore.
Nota: si consiglia di impostarlo su un valore che **superi** di almeno 10 minuti l'intervallo di aggiornamento del criterio specificato per ciascun criterio.
 - **Dissolvable Agent Compliance Threshold:** specifica il tempo (in minuti, ore o giorni) in cui il dato relativo alla conformità del computer non gestito viene considerato valido da DHCP Enforcer. Se il valore di soglia viene superato, il computer non gestito viene considerato sconosciuto finché nel computer non venga svolta una verifica della conformità. Nel frattempo l'accesso alla rete viene determinato dai modelli di accesso Unknown Endpoint specificati al punto 5. Se impostato sul valore 0, questo valore di soglia risulta disabilitato. Il valore predefinito è 12 ore.

4. Selezionare le impostazioni del server DHCP Enforcer appropriate:
 - **Report Exemptions:** casella di spunta che determina l'eventuale segnalazione di esenzioni da parte di DHCP Enforcer. Se selezionata, i computer endpoint definiti come esenzioni vengono esentati e segnalati, e successivamente visualizzati nel report di DHCP Exemption. Se non selezionata, i computer definiti come esenzioni vengono semplicemente esentati. Per ulteriori informazioni, consultare la sezione [Esecuzione del report DHCP Exemption](#) a pagina 68.
 - **Exempt DHCP Reservations:** casella di spunta che determina se i computer riservati, configurati nel server DHCP, siano esenti. Se selezionata, i computer riservati sono esentati dall'attuazione. Tuttavia, se un computer ha un agente installato, il modello di accesso associato allo stato di accesso del computer verrà assegnato a prescindere dalla sua designazione di computer riservato.
 - **Override DHCP Enforcer:** casella di spunta che determina se DHCP Enforcer deve eseguire l'attuazione secondo i criteri di sicurezza predefiniti. Se spuntata, l'attuazione è disabilitata e l'accesso alla rete è determinato dai modelli di accesso Maintenance Mode/Enforcer Override specificati al punto 5; tuttavia, i modelli di accesso vengono utilizzati solo se il computer non è un'esenzione definita.
5. Per aggiungere o modificare i modelli di accesso per un determinato stato di accesso, cliccare su **Select** sotto DHCP Enforcer Access Templates, spuntare le caselle accanto ai modelli e ai relativi stati di accesso e poi cliccare su **OK**. È possibile anche uscire da o cancellare il modello di accesso predefinito. Sono disponibili i seguenti stati di accesso:
 - **Unknown Endpoint:** determina l'accesso alla rete in mancanza di dati sulla conformità. I computer sconosciuti non sono gestiti da Sophos Enterprise Console, non sono esenti e possono non avere eseguito Dissolvable Agent o avere superato il limite di conformità di Dissolvable Agent descritto al punto 2. È possibile selezionare modelli di accesso per computer sconosciuti quando il server DHCP si trova nella modalità per computer sconosciuti Report Only o Enforce. Per ulteriori informazioni, consultare la sezione [Creazione dei server di DHCP Enforcer](#) a pagina 78.
 - **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 DHCP Enforcer.
 - **Default:** determina l'accesso alla rete nel caso in cui non venga rilevato alcun modello di accesso associato.
6. 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.
7. Cliccare su **Save**.

5.4 Creazione dei server di DHCP Enforcer

I server di DHCP Enforcer vengono utilizzati per l'attuazione delle implementazioni di DHCP in Sophos NAC. Si tratta dei server DHCP nei quali è installato DHCP Enforcer. Per ulteriori informazioni su come configurare l'attuazione di DHCP, consultare la [Guida alla configurazione di Sophos NAC DHCP](#).

Procedura

1. Cliccare su **Configure System > Server Settings** . Cliccare su **Create Server** in basso a sinistra nella pagina.
2. Digitare un nome e una descrizione per il server.
3. Cliccare sull'elenco **Server Type** e selezionare **DHCP Enforcer Server**.
4. Digitare il nome host o l'indirizzo IP del server e cliccare su **Add**. Se si inserisce il nome host, NAC Manager cerca di collegarlo all'indirizzo IP corretto. Se ciò non è possibile, è necessario inserire l'indirizzo IP corretto.
5. Digitare e confermare la chiave condivisa del server.

Importante: la chiave condivisa deve corrispondere a quanto inserito durante l'installazione di DHCP Enforcer nel server.

6. Selezionare la modalità per computer sconosciuto per stabilire se il server di DHCP Enforcer debba generare o attuare report sull'accesso di computer sconosciuti.

L'opzione **Report Only** consente la distribuzione dei server di DHCP Enforcer senza avere ripercussioni sull'accesso alla rete. Una volta che sono state create le esenzioni DHCP e che gli utenti ospiti utilizzano Dissolvable Agent, è possibile cambiare la modalità per computer sconosciuto con la modalità **Enforce** per permettere l'attuazione DHCP.

I computer sconosciuti non sono gestiti da Sophos Enterprise Console, non sono esenti, e possono non avere eseguito Dissolvable Agent o avere superato il limite di conformità di Dissolvable Agent.

Nota: In base alla la modalità per computer sconosciuto, i modelli di accesso Unknown Endpoint stabiliti nell'area **Configure System > Enforcer Settings** determinano l'accesso alla rete. Per ulteriori informazioni, consultare la sezione [Specificazione delle impostazioni di Enforcer](#) a pagina 77.

7. Cliccare su **Save**.

5.5 Creazione dei server di Dissolvable Agent

I server di Dissolvable Agent vengono utilizzati come host di Dissolvable Agent. Una volta definiti, DHCP Enforcer può consentirne l'accesso.

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

Procedura

1. Cliccare su **Configure System > Server Settings** . Cliccare su **Create Server** in basso a sinistra nella pagina.
2. Digitare un nome e una descrizione per il server.
3. Cliccare sull'elenco **Server Type** e selezionare **Dissolvable Agent Server**.
4. Digitare il nome host o l'indirizzo IP del server e cliccare su **Add**. Se si inserisce il nome host, NAC Manager cerca di collegarlo all'indirizzo IP corretto. Se ciò non è possibile, è necessario inserire l'indirizzo IP corretto.
5. Cliccare su **Save**.

5.6 Aggiornamento delle impostazioni del server NAC proxy

Durante l'installazione di NAC, NAC può essere configurato in modo da utilizzare un server proxy per l'accesso a Internet. Per ottenere le informazioni più aggiornate relative al rilevamento delle applicazioni di sicurezza, è necessario avere accesso a Internet. Utilizzare questa area per aggiornare le impostazioni di proxy e, se lo si desidera, gli indirizzi IP del NAC Server.

Procedura

1. Cliccare su **Configure System > Server Settings**.
2. Cliccare sul nome del NAC Server per aggiornare le relative impostazioni.
3. A scelta, digitare il nome host o l'indirizzo IP del server e cliccare su **Add**. Se si inserisce il nome host, NAC Manager cerca di collegarlo all'indirizzo IP corretto. Se ciò non è possibile, è necessario inserire l'indirizzo IP corretto.

Importante: dal momento che gli indirizzi IP definiscono la connessione tra l'agente e NAC Server, assicurarsi che siano corretti. Se non lo sono, gli agenti non saranno in grado di comunicare con il NAC Server.

4. Cliccare sull'elenco **Proxy Settings** per selezionare l'opzione adeguata del server proxy:
 - **No Proxy:** il NAC Server utilizza un server proxy per l'accesso a Internet.
 - **Use Proxy:** il NAC Server utilizza un server proxy per l'accesso a Internet. Le impostazioni del server proxy vengono inizialmente definite durante l'installazione di NAC; possono comunque essere aggiornate a seconda della necessità.
 - **Use SEC Proxy Settings:** per accedere a Internet, NAC Server utilizza le impostazioni del server proxy definite in Sophos Enterprise Console. Questa opzione è disponibile solo se Sophos Enterprise Console è installata nello stesso server di Sophos NAC. Se questa opzione è selezionata, le impostazioni del server proxy devono essere aggiornate in Sophos Enterprise Console.

5. Aggiornare le impostazioni del server proxy.

Nota: l'indirizzo e il numero di porta del server proxy sono obbligatori. Il nome utente, la password e la conferma della password vengono richiesti solo se si utilizza un proxy autenticato.

6. Cliccare su **Save**.

5.7 Aggiornamento dei dati dell'account di download

Il nome utente e la password dell'account di download sono utilizzati da NAC per scaricare le informazioni più aggiornate relative al rilevamento delle applicazioni di sicurezza. Il nome utente e la password inseriti durante l'installazione di NAC devono corrispondere a quelli forniti da Sophos. Se durante l'installazione di NAC sono stati inseriti in modo non corretto, è possibile correggerli nella pagina Download Account Details.

Procedura

1. Cliccare su **Configure System > Download Account Details**.
2. Aggiornare il nome utente e/o la password.

Se si aggiorna una password esistente, bisogna confermare la nuova password.

3. Cliccare su **Save**.

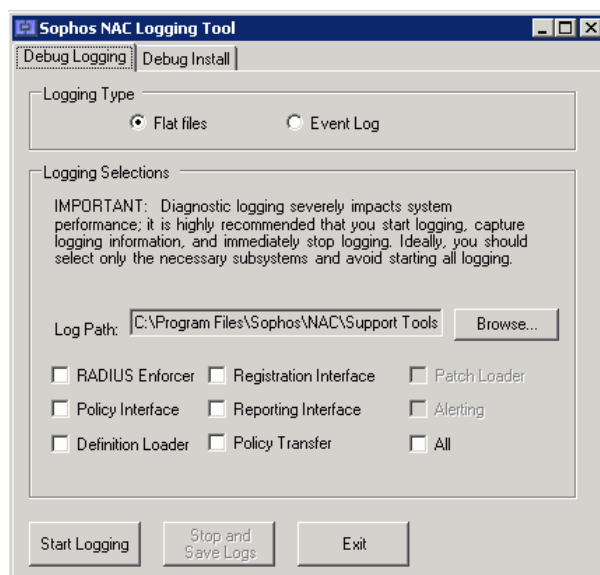
6 Tool di log

Il tool di log consente di abilitare la registrazione nel log per installazione e sottosistemi, in modo tale da fornire la risoluzione dei problemi. La scheda Debug Logging consente di identificare il metodo di log, la posizione del file e di avviare e interrompere manualmente la registrazione nel log per i sottosistemi selezionati. La scheda Debug Install consente di identificare il file di installazione da sottoporre a diagnosi e la posizione dei file di log. Il log è impostato al livello massimo; i dati di log dipendono dal tipo di registrazione svolta.

Importante: Si consiglia di utilizzare questo tool solo per la risoluzione dei problemi, sotto la guida di un rappresentante Sophos, e di non lasciare attiva la registrazione nel log dal momento che incide notevolmente sulle prestazioni del sistema.

6.1 Log del sottosistema di Sophos NAC Server

1. Posizionare il tool di log in Sophos NAC Server. Il percorso predefinito di questo tool è C:\Programmi\Sophos\NAC\Support Tools.
2. Cliccare due volte su **LoggingUtil.exe**.



3. Nella scheda **Debug Logging**, scegliere il tipo di log e le selezioni appropriate, cliccare poi su **Start Logging**.

Per ulteriori informazioni relative a ciascun campo, consultare la sezione [Campi e descrizioni della scheda Debug Logging](#) a pagina 83.

Nota: una volta cliccato sul pulsante **Start Logging**, non è possibile selezionare o deselegionare sottosistemi aggiuntivi. È necessario bloccare il log, modificarne le opzioni e ricominciare la procedura di log.

4. In NAC Server svolgere le operazioni per le quali si desidera reperire dati di log.

5. Una volta svolte le operazioni adeguate, cliccare su **Stop and Save Logs** per salvare i dati del log negli adeguati file di log.

I file vengono salvati nel percorso prescelto indicato nella finestra **Log Path**. Il percorso predefinito è: C:\Programmi\Sophos\NAC\Support Tools\Logs. Per ulteriori informazioni sui tipi di file di log e su cosa contengano, consultare la sezione *File di log* a pagina 85.

Nota: **Stop and Save Logs** non è selezionabile quando il log è disabilitato.

6.2 Campi e descrizioni della scheda Debug Logging

Il log diagnostico incide notevolmente sulle prestazioni del sistema. Una volta cominciata la registrazione nel log, si consiglia fortemente di interromperla non appena salvate le informazioni necessarie. Idealmente, sarebbe consigliabile scegliere solo i sottosistemi necessari evitando così di avviare tutti i log.

Nota: il log è fissato al livello massimo e comprende errori del log, avvisi e messaggi informativi, full trace e di chiamata stack.

Campi	Descrizioni
Tipo di log	
Flat File	Imposta il log in modo tale da generare dei flat file. Per ogni sottosistema selezionato, viene creato un flat file.
Event Log	Imposta il log in modo tale da aggiungere all'Event Log, nel NAC Server, le informazioni relative al sottosistema.
Selezioni di log	
Log Path	Determina il percorso in cui vengono collocati i file di log generati.
RADIUS Enforcer	Imposta il log per il NAC Server. Questa opzione viene utilizzata esclusivamente per l'attuazione di DHCP. Il NAC Server è il componente del software che verifica i risultati di conformità dell'agente per conto di DHCP Enforcer.
Policy Interface	Imposta il log per il servizio Policy Interface. Policy Interface è il componente lato server che recupera il criterio per l'agente e verifica la validità della richiesta di quest'ultimo.
Definition Loader	Imposta il log per il definition loader. Il definition loader è il tool lato server responsabile del rilevamento di: applicazioni di sicurezza, versioni delle firme, versioni del motore di scansione, data dell'ultima scansione, protezione in tempo reale, abilitazione del rilevamento e azioni autocorrettive.

Campi	Descrizioni
Registration Interface	Imposta il log per il servizio Registration Interface. Registration Interface è il componente lato server che fornisce all'agente i servizi di registrazione. Conduce l'autenticazione dell'utente ogni qual volta un utente si registri per la prima volta o si reregistri.
Reporting Interface	Imposta il log per il servizio Reporting Interface. Reporting Interface è il componente lato server che raccoglie i dati dei report provenienti dall'agente. Reporting Interface verifica, inoltre, la validità della richiesta dell'agente.
Policy Transfer	Imposta il log per il servizio Policy Transfer. Policy Transfer è il componente lato server che trasferisce i dati dall'archivio del criterio a quello dei report, in modo tale che le informazioni aggiornate relative a un criterio vengano replicate nei report.
All	Imposta il log per tutti i sottosistemi di NAC.

6.3 Log dell'installazione di Sophos NAC Server

Questo tool deve essere utilizzato solo per la risoluzione dei problemi di installazione. Per prima cosa è necessario provare ad installare Sophos NAC. Se si ricevono messaggi di errore durante l'installazione, è possibile utilizzare questo tool per reperire dati della registrazione relativi all'installazione.

1. Posizionare il tool di log in Sophos NAC Server. Il percorso predefinito di questo tool è C:\Programmi\Sophos\NAC\Support Tools.
2. Cliccare due volte su **LoggingUtil.exe**.
3. Cliccare sulla scheda **Debug Install**.
4. Scegliere il percorso adeguato per il file di installazione che si desidera correggere e quello in cui si desidera collocare i file di log; infine cliccare su **Start Install**.

Per ulteriori informazioni relative a ciascun campo, consultare la sezione [Campi e descrizioni della scheda di installazione del debug](#) a pagina 84.

Nota: Una volta portata a termine l'installazione, i file vengono salvati nella posizione prescelta nel campo **Log Path**. Il percorso predefinito è: C:\Programmi\Sophos\NAC\Support Tools\Logs. Per ulteriori informazioni sui tipi di file di log e su cosa contengano, consultare la sezione [File di log](#) a pagina 85.

6.4 Campi e descrizioni della scheda di installazione del debug

La registrazione è fissata a un livello massimo stabilito dal programma di installazione di Microsoft® Windows®.

Campi	Descrizioni
Install File Path	Determina il percorso per l'installazione del file.
Log Path	Determina il percorso in cui vengono collocati i file di log generati durante l'installazione.

6.5 File di log

Il percorso predefinito dei file di log è: C:\Programmi\Sophos\NAC\Support Tools\Logs nel Sophos NAC Server. Questo percorso può essere modificato prima di generare i file di log. Ogni qualvolta si avvii un log, tutti i file esistenti nel percorso specificato e aventi lo stesso nome verranno sovrascritti.

Campi	Descrizioni
AppEvent.xml	È il file che contiene gli eventi delle applicazioni esportati dall'Event Log all'interno del NAC Server. Quando l'opzione Event Log è selezionata come tipo di log, i dati dei log dei sottosistemi vengono inclusi in questo file.
SystemEvent.xml	File contenente gli eventi di sistema esportati dall'Event Log nel NAC Server. Le informazioni relative al Servizio autenticazione Internet (IAS) sono contenute in questo file di log.
Systeminfo.nfo	File contenente i dati dell'hardware e del sistema operativo relativi al NAC Server.
UserInfo.txt	File contenente i dati relativi all'account (quali il nome e le autorizzazioni) degli utenti registrati al NAC Server e quelli dell'account con cui vengono eseguiti i sottosistemi installati.
<Sottosistema>.xml	File contenente i dati di log del sottosistema di Sophos NAC. Quando l'opzione Flat File viene scelta come tipo di log, ciascun sottosistema del Sophos NAC viene salvato nel rispettivo flat file: <ul style="list-style-type: none"> ■ Policy Interface: PolicyInterfaceLog.xml ■ Definition Loader: CurrentDefsLoaderLog.xml ■ Registration Interface: RegistrationInterfaceLog.xml ■ Reporting Interface: ReportingInterfaceLog.xml ■ Policy Transfer: PolicyTransferLog.xml
SophosNACLogs.zip	File comprendente tutti i file di log della scheda Debug Logging.
InstallLogs.zip	File comprendente tutti i file di log della scheda Debug Install.

7 Tool della modalità di manutenzione

Utilizzare il tool della modalità di manutenzione per effettuare la , manutenzione del database e/o nel caso di problemi alla rete o relativi al database. È un tool da riga di comando utilizzato per attivare e disattivare la modalità di manutenzione. Il tool blocca determinati servizi di Sophos NAC in modo tale da permettere di effettuare la manutenzione richiesta. Una volta pronti per tornare in produzione, bloccare il tool della modalità di manutenzione. Il tool riavvia automaticamente i servizi bloccati.

Quando Sophos NAC è in modalità di manutenzione, Sophos Compliance Agent riconosce tale modalità e opera senza errori, interruzioni o indicazioni all'utente relative alla modalità di manutenzione. L'agente salva localmente tutti i dati relativi alla verifica e ai report fino a quando il software non ritorna in modalità produttiva. L'agente viene inoltre verificato in base al criterio cache e, nel caso in cui sia in uso la quarantena dell'agente, il computer può comunque essere messo in quarantena in base alle regole del criterio cache. Inoltre, se si sta utilizzando l'attuazione DHCP, i modelli di accesso di DHCP Enforcer e le eccezioni vengono memorizzati nella cache e a tutte le richieste DHCP viene data risposta utilizzando tali modelli di accesso ed eccezioni.

Nota: non è necessario utilizzare questo tool durante l'upgrade di Sophos NAC. L'installazione mette il NAC Server in modalità di manutenzione e lo toglie da tale modalità una volta portata a termine l'installazione.

7.1 Esecuzione del tool della modalità di manutenzione

1. Dal prompt dei comandi di Sophos NAC Server, andare alla directory Programmi\Sophos\NAC\Support Tools.
2. Digitare **MaintMode.exe /start**. Questo comando mette Sophos NAC nella modalità di manutenzione.
3. Digitare **MaintMode.exe /stop**. Questo comando riporta Sophos NAC nella modalità di produzione.

7.2 Comandi del tool della modalità di manutenzione

I comandi non distinguono tra maiuscole e minuscole. I parametri dei comandi utilizzano il simbolo della la barra / seguita dal nome del parametro. Tutti i valori del parametro DOS comprendenti uno spazio richiedono le virgolette.

Comandi	Descrizioni
MaintMode.exe /start	Avvia il tool della modalità di manutenzione.
MaintMode.exe /stop	Blocca il tool della modalità di manutenzione.
MaintMode.exe /E:silent	Indica che nella finestra di dialogo della riga di comando non è presente alcun messaggio. I messaggi di errore vengono sempre scritti nell'Event Log.

Comandi	Descrizioni
MaintMode.exe /E:error	Indica che solo gli errori vengono scritti nella console. I messaggi di errore vengono sempre scritti nell'Event Log.
MaintMode.exe /E:warn	Indica che gli errori e gli avvisi vengono scritti nella console. I messaggi di errore vengono sempre scritti nell'Event Log.
MaintMode.exe /E:info	Indica che errori, avvisi e messaggi informativi vengono scritti nella console. I messaggi di errore vengono sempre scritti nell'Event Log.
MaintMode.exe /?	Visualizza la finestra della guida in linea del tool della modalità di manutenzione.

8 Glossario

Questo è il glossario relativo a Sophos NAC.

Account	L'account è formato da nome di accesso e ruolo di protezione per l'utente. Il nome dell'account e la password vengono utilizzati per accedere a NAC Manager. I ruoli di protezione stabiliscono il livello dei privilegi di ogni account.
Agent Enforcer	Tipo di attuazione che protegge la rete tramite la verifica basata sul client e l'attuazione della quarantena sui computer che eseguono il Quarantine Agent.
Application Type	I tipi di applicazione categorizzano le applicazioni e stabiliscono i comportamenti dei criteri predefiniti per tutte le applicazioni associate a un determinato tipo.
Applicazione	Le applicazioni sono le applicazioni del software supportate da Sophos NAC. Le applicazioni definiscono le funzioni, le condizioni associate, gli stati di conformità e le azioni possibili. Sono legate a un determinato tipo di applicazione, che stabilisce come debbano essere valutate quando il loro profilo viene aggiunto a un criterio.
Audits	Gli audit costituiscono un audit trail, vale a dire la cronologia degli eventi verificatisi all'interno del sistema. Gli eventi comprendono aggiornamenti, nuovi elementi o l'attività del sistema, quali aggiornamenti ai criteri correnti, creazione di nuovi modelli di accesso o account che si connettono o disconnettono da NAC Manager.
Azione correttiva	Azione che viene condotta sui computer durante la verifica della conformità in modo tale da rendere i computer conformi al criterio. Le azioni correttive non sono disponibili per tutti i criteri o tutte le funzioni di un'applicazione.
Capability	Per funzioni si intendono le funzioni di un'applicazione che possono essere testate durante una verifica di conformità. Le funzioni comprendono regole utilizzate per la verifica, composte a loro volta da condizioni, stati di conformità, messaggi e azioni correttive.
Compliance State	Lo stato di conformità viene stabilito tramite la valutazione dei risultati di rilevamento del computer secondo le condizioni definite nel profilo. Lo stato di conformità viene collegato ai modelli di accesso appropriati contenuti nel criterio per poter determinare il tipo di accesso alla rete effettivamente consentito al computer. Gli stati di conformità a disposizione sono: compliant, partially compliant o non-compliant.
Comportamento del criterio	Comportamento del criterio che stabilisce come valutare i profili in base agli altri dello stesso tipo presenti nel computer. Opzioni disponibili: Required, Best e All. Per ulteriori informazioni, leggere

	le definizioni di Required Policy Behavior, Best Policy Behavior e All Policy Behavior.
Comportamento del criterio All	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 dell'applicazione che si desidera escludere dal computer possono essere valutati in questo modo.
Comportamento del criterio Best	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 diagnosticati, 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.
Comportamento del criterio Required	È indispensabile un profilo di sistema operativo che viene valutato come profilo best. 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.
Computer	Un computer che cerca di connettersi alla rete. Un computer può eseguire l'agente, essere esentato e non avere alcun agente, oppure può essere sconosciuto.
Computer gestito	Per computer gestito si intende un computer che gestito con Sophos Enterprise Console su cui è installato Sophos Compliance Agent. Un computer gestito utilizza Quarantine Agent per la valutazione della conformità e per ottenere accesso alla rete.
Computer non gestito	Per computer non gestito si intende un computer non gestito da Sophos Enterprise Console ed esterno all'azienda. Un computer non gestito utilizza Dissolvable Agent per la valutazione della conformità e per ottenere accesso alla rete.
Computer sconosciuto	Stato di accesso definito nell'area Configure System > Enforcer Settings che determina l'accesso alla rete quando non esiste nessun dato relativo alla conformità. I computer sconosciuti non sono gestiti da Sophos Enterprise Console, non sono esenti, e possono non avere eseguito Dissolvable Agent o avere superato il limite di

	conformità di Dissolvable Agent. È possibile selezionare modelli di accesso per computer sconosciuti quando il server DHCP si trova nella modalità per computer sconosciuti Report Only o Enforce.
Condizione	Le condizioni vengono utilizzate durante la verifica per stabilire lo stato di conformità associato e le azioni da intraprendere nei computer.
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.
Criterio Managed	Il criterio predefinito Managed viene utilizzato nei computer che sono gestiti da Sophos Enterprise Console e su cui è installato un agente. 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.
Criterio predefinito	Il criterio predefinito viene utilizzato se in un computer è installato l'agente, ma non gli è stato attribuito nessun 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.
Criterio Unmanaged	Il criterio predefinito Unmanaged viene utilizzato dai computer esterni all'azienda. Questo criterio non svolge attività correttive nel computer. Il Dissolvable Agent utilizza il criterio Unmanaged.
DHCP Configuration Wizard	La Procedura guidata per la configurazione di DHCP aiuta ad identificare i server proxy, di correzione, di Dissolvable Agent e di DHCP Enforcer da utilizzare con le implementazioni di Sophos NAC.
DHCP Enforcer	DHCP Enforcer è il tipo di attuazione che protegge la rete per le implementazioni DHCP di Sophos NAC.
Dissolvable Agent	Dissolvable Agent verifica i computer in modo tale da stabilire se sono conformi al criterio di NAC prima di consentirne l'accesso alla rete. Dissolvable Agent deve venire eseguito da un browser. Dissolvable Agent è concepito per gli utenti che non hanno o non possono avere un agente installato nel computer, ma che devono poter accedere a specifiche risorse di rete in quanto collaboratori esterni o ospiti. Dissolvable Agent viene utilizzato con l'attuazione DHCP.
Esenzione	Le esenzioni identificano i computer in cui non è necessario valutare lo stato di conformità al momento della connessione alla rete. Le esenzioni includono i computer che non possono eseguire l'agente, quali i computer che utilizzano sistemi operativi non

	Windows, o quelli che non richiedono verifica della conformità, quali server, router o stampanti. Inoltre, quando si esegue in tutta l'impresa l'attuazione dei criteri per fasi, è possibile escludere i computer o le reti in cui non si desidera ancora applicare i criteri.
Impostazioni dell'agente	Le impostazioni dell'agente ne definiscono le funzioni quando è in esecuzione nel computer. È possibile impostarle durante la creazione dei modelli di configurazione dell'agente.
Impostazioni di Enforcer	Le impostazioni di Enforcer determinano le specificazioni di implementazione per i diversi tipi di implementazione di DHCP Enforce e Agent Enforcer.
Messaggio	Durante la verifica della conformità viene visualizzato un messaggio informativo o di errore. I Messaggi vengono visualizzati nel computer esclusivamente se la condizione a cui sono associati è stata rispettata. Tutte le funzioni possono determinare la visualizzazione di messaggi.
Modalità del criterio Enforce	La modalità Enforce del criterio indica che i computer sono valutati in base al criterio assegnato e 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.
Modalità del criterio Remediate	La modalità Remediate del criterio indica che i computer sono valutati in base al criterio assegnato e all'interno di NAC Manager viene generato un report informativo. I messaggi vengono visualizzati e vengono intraprese azioni correttive; non viene tuttavia svolta alcuna azione di attuazione.
Modalità del criterio Report Only	La modalità Report Only del criterio 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 nessun messaggio e non viene intrapresa alcuna azione correttiva e di attuazione.
Modalità di manutenzione/Enforcer Override	Stato di accesso definito nell'area Configure System > Enforcer Settings che determina l'accesso alla rete quando il sistema si trova in modalità di manutenzione oppure quando DHCP Enforcer è stato disabilitato.
Modello di accesso	I modelli di accesso stabiliscono l'accesso alla rete quando associati agli stati di accesso in criteri, esenzioni e impostazioni di Enforcer (a seconda del tipo di attuazione).
Modello di configurazione dell'agente	I modelli di configurazione dell'agente definiscono le impostazioni opzionali che controllano il funzionamento di Quarantine Agent nei computer.
No Agent Tray	Stato di accesso definito nel criterio e che determina l'accesso alla rete quando l'agente non è in esecuzione nel computer. Questo

	stato viene segnalato da Agent Enforcer nel caso in cui l'utente non sia connesso a Windows oppure l'applicazione dell'agente nell'area di notifica non sia più in esecuzione.
Policy Retrieval Error (Agent)	Stato di accesso, definito nel criterio, che determina l'accesso alla rete quando non è stato possibile recuperare un criterio per il computer. Questo stato può esistere se l'agente non riesce a recuperare il criterio da NAC Server; oppure lo stato di conformità del computer non è aggiornato secondo il campo Agent Policy Update Threshold configurato nell'area Configure System > Enforcer Settings .
Policy Retrieval Error (DHCP)	Stato di accesso, definito nel criterio, che determina l'accesso alla rete quando lo stato di conformità del computer è obsoleto secondo il campo DHCP Policy Update Threshold configurato nell'area Configure System > Enforcer Settings .
Predefinito	Stato di accesso definito nell'area Configure System > Enforcer Settings che determina l'accesso alla rete quando non esiste nessun dato relativo alla conformità.
Profile Type	I tipi di profilo categorizzano il profilo. I profili vengono inseriti all'interno dei criteri e valutati gli uni rispetto agli altri in base al tipo di profilo e all'associato comportamento del criterio.
Profilo	I profili consentono di definire quali elementi dei computer devono essere valutati (per es. sistemi operativi e applicazioni). I profili definiscono condizioni, stati di conformità, messaggi e azioni correttive. Una volta creati possono essere organizzati e ordinati per priorità all'interno dei criteri.
Quarantine Agent	Quarantine Agent verifica la conformità dei computer al criterio di NAC. Le verifiche vengono svolte prima di e periodicamente dopo aver concesso l'accesso alla rete. L'agente richiede un'interazione dell'utente minima o nulla. Quarantine Agent possiede una funzione di quarantena che consente l'attuazione e limita l'accesso dei computer a specifiche aree della rete qualora non siano conformi al criterio di NAC.
Regola di rilevamento	Una regola di rilevamento determina i valori del registro, i processi oppure i file che verranno valutati all'interno del computer in modo tale da stabilire se un'applicazione è installata, in esecuzione o è in possesso di una determinata versione o valore.
Risorse di rete	Le risorse di rete sono applicazioni o dispositivi necessari per la correzione dei computer o responsabili della negazione dell'accesso alla rete. Le risorse di rete possono essere aggiunte sia ai modelli di accesso di Agent Enforcer che a quelli di DHCP Enforcer.
Ruolo di sicurezza	I ruoli di protezione stabiliscono il livello dei diritti di ogni account di NAC Manager e vengono assegnati quando l'account viene creato.

Sessione dell'agente	La sessione dell'agente indica il periodo di tempo in cui l'agente è attivo nel computer e accede a Sophos NAC.
Stato di accesso	Gli stati di accesso comprendono tutti gli stati a cui può essere applicato un modello di accesso che permetta l'accesso alla rete. I modelli di accesso di Agent Enforcer possono essere applicati agli stati di accesso all'interno dei criteri. I modelli di accesso di DHCP Enforcer possono essere applicati agli stati di accesso in criteri, esenzioni e impostazioni di Enforcer.
User Override	Stato di accesso definito nel criterio che determina l'accesso alla rete quando l'utente ha ignorato la quarantena dell'agente nel computer. Se l'utente ignora lo stato di quarantena, quest'ultimo viene disabilitato.

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.it/support/>.
- Scaricando la documentazione del prodotto su <http://www.sophos.it/support/docs/>.
- Inviando un'e-mail a 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 © 2011 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.

OPSWAT, Inc.

This software contains technology licensed from and copyrighted © by OPSWAT, Inc. OPSWAT is a trademark of OPSWAT, Inc.

Indice

A

- abilitazione
 - account 76
 - esenzioni 55
- account
 - abilitazione e disabilitazione 76
 - creazione 76
 - download account details 80
 - rimozione 9
 - visualizzazione o ricerca 8
- accounts 75
- Agent configuration templates 12
 - blocco e sblocco 10
 - creazione 20
 - rimozione 9
 - Salvataggio come nuovo 8
 - visualizzazione delle impostazioni dell'agente per 20
 - visualizzazione o ricerca 8
- Agent Enforcer 18, 46, 77
- Agent Enforcer, report 62
- Agent Session, report 59
- aggiornamento
 - download account details 80
 - Impostazioni del server NAC proxy 80
 - policies 16
- aggiunta
 - di oggetti ai profili 29–30
 - di profili ai criteri 17
- applications 8
- applicazioni 12
- assegnazione dei modelli di accesso 18, 53–54, 78
- audits 56, 74
- azioni correttive 22, 32, 72

B

- Blocco di oggetti 9–10

C

- cancellazione di oggetti 9, 74
- classe del produttore 53
- classe dell'utente 47, 53
- Compliance reports 57

- comportamento del criterio 17, 71
- computer gestiti 15, 28
- computer non gestiti 15, 28
- condizioni 22, 29–30, 32–33, 72
- configurazione
 - Attuazione DHCP 49
 - dell'agente 16, 20
- consigli
 - applicazioni 12
 - criteri 12
 - profiles 12, 27
- creazione
 - account 76
 - Agent configuration templates 20
 - esenzioni 53–54
 - esenzioni da report 69
 - exemptions 53
 - modelli di accesso 46–47
 - network resources 51
 - profiles 27–28, 30
 - Server di DHCP Enforcer 79
 - Server web di Dissolvable Agent 79
- criteri 12
- criteri predefiniti 15

D

- dati della verifica 70
- definizioni dei termini 88
- determinazione dello stato di conformità 42
- DHCP Configuration Wizard 43, 49
- DHCP Enforcer 18, 47, 53–54, 77
- disabilitazione
 - account 76
 - esenzioni 55
- download account details 75, 80

E

- Enforcer settings 75, 77
- esecuzione dei report 57, 59, 61–62, 64, 68, 70, 74
- esenzioni
 - abilitazione e disabilitazione 55
 - blocco e sblocco 10
 - creazione 53–54
 - creazione dai report 69
 - reportistica 68, 78
 - rimozione 9
 - Salvataggio come nuovo 8

esenzioni (*continua*)

visualizzazione o ricerca 8

eventi di sistema 74

exemptions 43

creazione 53

F

funzioni 22, 31, 33, 72

funzioni del tasto destro del mouse 10

G

Glossario 88

H

home page 4

I

icone

account 6

esenzioni 7

funzioni comuni 5

profili delle applicazioni 7

profili e criteri 6

report 7

stati di conformità del modello 6

Impostazioni del server NAC proxy 80

Impostazioni dell'agente

nei criteri 16

nei modelli di configurazione dell'agente 20

impostazioni lease di DHCP 47

Indirizzo MAC 53, 69

IP scope 47, 54

M

menu, elementi 3, 12, 43, 56, 75

messaggi 22, 29–32, 72

migliori pratiche

Criterio 13

modello di accesso 44

profilo 22

modalità del criterio 13, 16, 18

Modalità Enforce del criterio 19

Modalità remediate del criterio 19

Modalità Report Only del criterio 18

modelli di accesso 43

blocco e sblocco 10

creazione 46–47

migliori pratiche 44

rimozione 9

Salvataggio come nuovo 8

test per un'attuazione accurata 44

verifica nel criterio 13

visualizzazione o ricerca 8

modelli di accesso predefiniti 44

N

NAC Manager 3

blocco e sblocco di oggetti 10

cancellazione di oggetti 9

funzioni del tasto destro del mouse 10

icone 5

salvataggio di oggetti come nuovi 8

visualizzazione o ricerca di oggetti degli elenchi 8

network resources 43, 46–47

blocco e sblocco (solo personalizzato) 10

cancellazione (solo personalizzata) 9

creazione 51

Salvataggio come nuovo 8

visualizzazione o ricerca 8

Non-Compliance Detail, report 61

O

oggetti degli elenchi 8

P

panoramica, sistema 3, 12, 43, 56, 75

policies

aggiornamento 16

blocco e sblocco 10

migliori pratiche 13

modalità e stati di accesso 18

utilizzo dei criteri predefiniti 15

visualizzazione o ricerca 8

profiles 12, 71

blocco e sblocco 10

creazione 27–28, 30

funzioni e condizioni di un'applicazione per 33

linee guida 27

migliori pratiche relative alle funzioni 22

profiles (*continua*)

- rimozione 9
- Salvataggio come nuovo 8
- visualizzazione o ricerca 8

profili

- migliori pratiche 22
- utilizzo dei profili predefiniti di Windows 28
- utilizzo di Sophos Patch Agent predefinito 28

profili delle applicazioni 30

profili di Windows Update 28

profili nei sistemi operativi 28

profili predefiniti 22, 28

profilo di Sophos Patch Agent 28

proxy autenticato 80

proxy server, impostazioni 80

Q

quarantine override 13

R

report 56

- Agent Enforcer, report 62
- Agent Session, report 59
- cancellazione di quelli salvati 74
- Compliance reports 57
- dati della verifica 70
- Non-Compliance Detail, report 61
- report DHCP Enforcer 64, 69
- report DHCP Exemption 68
- salvataggio 73–74
- stampa 57

report dettagliati 57

report DHCP Enforcer 64, 69

report DHCP Exemption 68

report riepilogativi 57

ricerca di oggetti degli elenchi 8

risorse di rete eseguibili 51

risorse di rete porta/protocollo 51

ruoli di sicurezza 76

S

Salvataggio come nuovo 7–8

saved reports 56

- esecuzione 74
- rimozione 74
- salvataggio 73

sblocco di oggetti 10

server

- DHCP Enforcer 79
- Dissolvable Agent 79
- Impostazioni di NAC proxy 80

Server di DHCP Enforcer 79

server DNS 47

server settings 75

Server web di Dissolvable Agent 79

Sophos Anti-Virus, funzioni 33

Sophos Enterprise Console 15, 33

Sophos Patch 28

specificazione delle impostazioni di Enforcer 77

stampa dei report 57

stati di accesso 18, 78

stati di conformità 18, 22, 29–30, 32, 42, 44, 46–47, 57, 59, 61–62, 64, 70, 72

stato di conformità 42

strumenti

- Tool della modalità di manutenzione 86
- Tool di log 82

supporto tecnico 94

T

tipi di applicazione 12

tipi di attuazione 18, 46–47, 53, 77

tipi di profilo 17, 29–30, 71

Tool della modalità di manutenzione 86

- comandi 86

- esecuzione del tool 86

Tool di log 82

- file di log 85

- Log del NAC Server 82

- Log dell'installazione di NAC 84

U

utilizzo

- dei profili predefiniti di Windows Update 28
- profilo predefinito di Sophos Patch Agent 28

Utilizzo

- criteri predefiniti 15

utilizzo di Network Access Control 3

V

Verifiche patch 28

visualizzazione

- audits 74
- dati della verifica 70

visualizzazione (*continua*)

funzioni e condizioni di un'applicazione 33

Impostazioni dell'agente 20

modalità e stati di accesso di un criterio 18

visualizzazione (*continua*)

oggetti degli elenchi 8

visualizzazione della home page 4