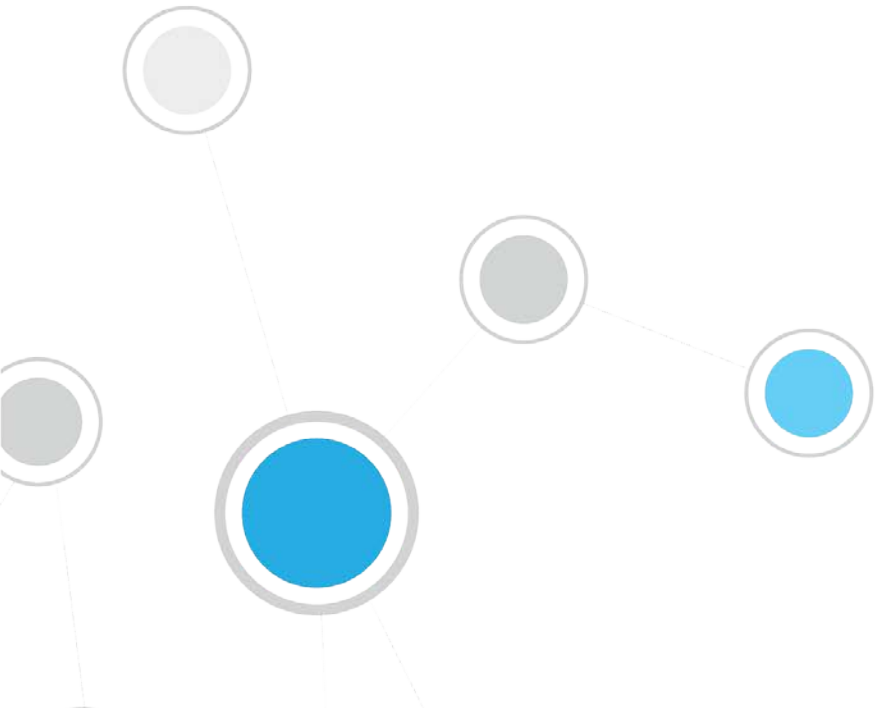
ForeScout CounterACT®

Singolo appliance CounterACT

Guida di installazione rapida

Versione 8.0



Sommario

Benvenuti in CounterACT Versione 8.0

La piattaforma CounterACT offre visibilità sulle infrastrutture e sui dispositivi, gestione delle policy, orchestrazione e ottimizzazione dei flussi di lavoro per migliorare la sicurezza della rete. CounterACT offre alle imprese informazioni contestuali in tempo reale riguardo i dispositivi e gli utenti sulla rete. Le policy in CounterACT vengono determinate attraverso l'uso di queste informazioni contestuali che aiutano a garantire la conformità, il monitoraggio e l'aggiornamento, il corretto accesso alla rete e l'ottimizzazione delle operazioni di manutenzione.

In questa guida viene descritta l'installazione di un singolo appliance CounterACT autonomo.

Per maggiori dettagli oppure per informazioni sulla distribuzione di appliance multipli per la protezione della rete aziendale, consultare la *Guida di installazione CounterACT* e *Guida all'amministrazione di CounterACT.* Per informazioni su come accedere a queste guide, vedere Documentazione CounterACT aggiuntiva.

Inoltre, è possibile accedere al sito Web all'indirizzo: http://www.forescout.com/support per la documentazione, gli articoli di knowledgebase e gli aggiornamenti per l'appliance più recenti.

Contenuto del pacchetto CounterACT

Il pacchetto CounterACT comprende:

- L'appliance CounterACT
- Pannello anteriore
- Kit di binari a scorrimento (staffe di montaggio)
- Cavi di alimentazione
- Cavo di collegamento alla console con connettore DB9 (solo connessioni seriali)
- Informazioni sulla sicurezza, sull'ambiente e sulle normative relative ai prodotti aziendali
- Guida introduttiva (solo dispositivi 51xx)

Informazioni generali

Effettuare quanto segue per impostare CounterACT:

1. Creare un piano di distribuzione

Prima di eseguire l'installazione, decidere dove distribuire l'appliance e acquisire familiarità con le relative interfacce di collegamento.

Dove distribuire l'appliance

Selezionare la giusta posizione di rete dove verrà distribuito l'appliance è fondamentale per il corretto impiego e per ottenere prestazioni ottimali di CounterACT. La giusta posizione dipenderà dai propri obiettivi di implementazione e dalla policy di accesso alla rete. L'appliance dovrà essere in grado di monitorare il traffico relativo alla policy desiderata. Ad esempio, se la policy desiderata dipende dal monitoraggio di autorizzazioni dagli endpoint ai server di autenticazione aziendali, l'appliance deve essere installato in maniera da poter vedere il traffico degli endpoint scorrere nei server di autenticazione.

Per informazioni più dettagliate sull'installazione e sulla distribuzione, fare riferimento alla *Guida di installazione CounterACT*. Per informazioni su come accedere a questa guida, vedere Documentazione CounterACT aggiuntiva.

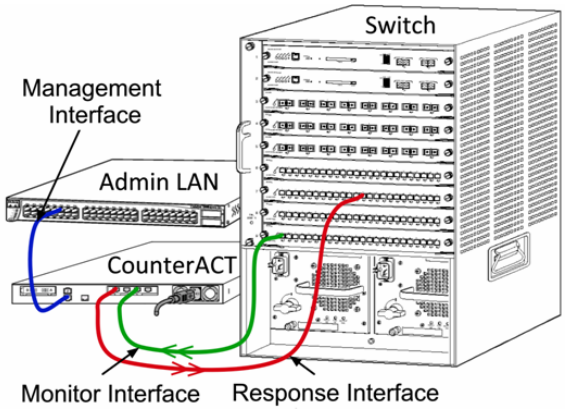
Interfacce di collegamento dell'appliance

Normalmente l'appliance è configurato con tre collegamenti allo switch di rete.

Interfaccia di gestione

L'interfaccia di gestione consente di gestire CounterACT ed eseguire query e approfondimenti sugli endpoint. L'interfaccia deve essere collegata alla porta dello switch con accesso a tutti gli endpoint di rete.

Ciascun appliance richiede una singola connessione per la gestione della rete. Questa connessione richiede un indirizzo IP sul LAN locale e accesso alla porta 13000/TCP dalle macchine che eseguiranno l'applicazione di gestione della console CounterACT. La porta di gestione deve avere accesso ai servizi di rete aggiuntivi.



Requisiti di accesso alla rete

Porta	Servizio	A o da CounterACT	Funzione
22/TCP	SSH	Da	Consente l'ispezione in remoto degli endpoint OS X e Linux. Consente a CounterACT di comunicare con gli switch di rete e con i router.
		A	Consente di accedere all'interfaccia con riga di comando di CounterACT.
2222/TCP	SSH	A	(Elevata disponibilità) Consente l'accesso ai dispositivi CounterACT fisici che fanno parte della coppia a elevata disponibilità. Utilizzare 22/TCP per accedere all'indirizzo IP condiviso (virtuale) della coppia.
25/TCP	SMTP	Da	Consente a CounterACT di accedere al servizio di Mail Relay aziendale.
53/UDP	DNS	Da	Consente a CounterACT di risolvere indirizzi IP interni.
80/TCP	HTTP	A	Consente il reindirizzamento HTTP.
123/UDP	NTP	Da	Consente a CounterACT di accedere a un server di riferimento con ora locale o a ntp.forescout.net. CounterACT accede a ntp.foreScout.net per impostazione predefinita.
135/TCP	MS-WMI	Da	Consente l'ispezione in remoto degli endpoint Windows.
139/TCP	SMB, MS-RPC	Da	Consente l'ispezione in remoto degli endpoint Windows (per endpoint che eseguono Windows 7 o precedente).
445/TCP			Consente l'ispezione in remoto degli endpoint Windows.
161/UDP	SNMP	Da	Consente a CounterACT di comunicare con gli switch di rete e con i router. Per informazioni sulla configurazione di SNMP, fare riferimento alla *Guida all'amministrazione di CounterACT*.
162/UDP	SNMP	A	Consente a CounterACT di ricevere trap SNMP dallo switch di rete e dai router. Per informazioni sulla configurazione di SNMP, fare riferimento alla *Guida all'amministrazione di CounterACT*.
389/TCP (636)	LDAP	Da	Consente a CounterACT di comunicare con Active Directory. Consente la comunicazione con portali Web CounterACT.

Porta	Servizio	A o da CounterACT	Funzione
443/TCP	HTTPS	A	Consente il reindirizzamento HTTP tramite TLS.
2200/TCP	SecureConnector per Linux	A	Consente a SecureConnector di creare una connessione protetta (SSH crittografato) all'appliance da macchine Linux. *SecureConnector* è un agente basato su script che abilita la gestione degli endpoint Linux mentre sono collegati alla rete.
10003/TCP	SecureConnector per Windows	A	Consente a SecureConnector di creare una connessione protetta (TLS crittografato) all'appliance da macchine Windows. *SecureConnector* è un agente che abilita la gestione degli endpoint Windows mentre sono collegati alla rete. Per ulteriori informazioni su SecureConnector, fare riferimento alla *Guida all'amministrazione di CounterACT*. Quando SecureConnector si collega a un appliance o a Enterprise Manager viene reindirizzato all'appliance a cui il proprio host è assegnato. Assicurarsi che questa porta sia aperta a tutti gli appliance e a Enterprise Manager per consentire mobilità trasparente all'interno dell'organizzazione.
10005/TCP	SecureConnector per OS X	A	Consente a SecureConnector di creare una connessione protetta (crittografata con TLS) all'appliance da macchine OS X. *SecureConnector* è un agente che abilita la gestione degli endpoint OS X mentre sono collegati alla rete. Per ulteriori informazioni su SecureConnector, fare riferimento alla *Guida all'amministrazione di CounterACT*. Quando SecureConnector si collega a un appliance o a Enterprise Manager viene reindirizzato all'appliance a cui il proprio host è assegnato. Assicurarsi che questa porta sia aperta a tutti gli appliance e a Enterprise Manager per consentire mobilità trasparente all'interno dell'organizzazione.

Porta	Servizio	A o da CounterACT	Funzione
13000/TCP	CounterACT	Da/A	Per ambienti con un solo appliance - dalla console all'appliance. Per ambienti con più di un appliance CounterACT - dalla console all'appliance CounterACT e da un appliance CounterACT a un altro. La comunicazione tra dispositivi CounterACT comprende la comunicazione con Enterprise Manager e con Recovery Enterprise Manager, tramite TLS.

Interfaccia di monitoraggio

L'interfaccia di monitoraggio consente all'appliance di monitorare e tracciare il traffico di rete. È possibile utilizzare un'interfaccia disponibile come interfaccia di monitoraggio.

Il mirroring del traffico è indirizzato su una porta sullo switch e monitorato dall'appliance. L'utilizzo di codifica VLAN 802.1Q dipende dal numero di VLAN di cui è stato eseguito il mirroring.

- ***VLAN singola***: quando il traffico monitorato è generato da una singola VLAN, il traffico di cui è stato eseguito il mirroring non necessita di codifica VLAN.
- ***VLAN multiple***: se il traffico monitorato proviene da più di una VLAN, il traffico di cui è stato eseguito il mirroring deve necessariamente essere codificato con VLAN 802.1Q.

Quando due switch sono collegati come una coppia ridondante, l'appliance deve monitorare il traffico da entrambi gli switch.

Non è richiesto alcun indirizzo IP sull'interfaccia del monitor.

Interfaccia di risposta

L'appliance risponde al traffico utilizzando l'interfaccia di risposta. Il traffico di risposta viene utilizzato come protezione da attività dannose e per eseguire azioni determinate da policy. Tra queste, ad esempio, vi possono essere il reindirizzamento di browser Web o il blocco delle sessioni. La configurazione della relativa porta dello switch dipende dal traffico che viene monitorato.

È possibile utilizzare un'interfaccia disponibile come interfaccia di risposta.

- ***VLAN singola***: quando il traffico monitorato è generato da una singola VLAN, la porta di risposta deve appartenere alla stessa VLAN. In questo caso, l'appliance richiede un singolo indirizzo IP su quella VLAN.
- ***VLAN multiple***: se il traffico monitorato proviene da più di una VLAN, la porta di risposta deve anche essere configurata con codifica VLAN 802.1Q per le stesse VLAN. L'appliance richiede un indirizzo IP per ogni VLAN monitorata.

2. Configurare lo switch

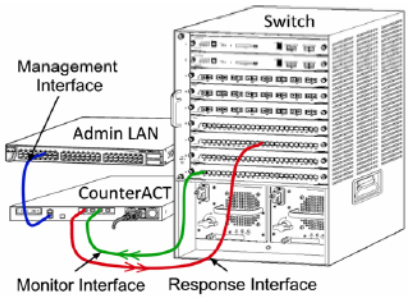
A. Opzioni di collegamento dello switch

L'appliance è stato realizzato per integrarsi con un'ampia varietà di ambienti di rete. Per poter integrare correttamente l'appliance con la propria rete, verificare che lo switch sia impostato per monitorare il traffico richiesto.

Sono disponibili diverse opzioni per connettere l'appliance al proprio switch.

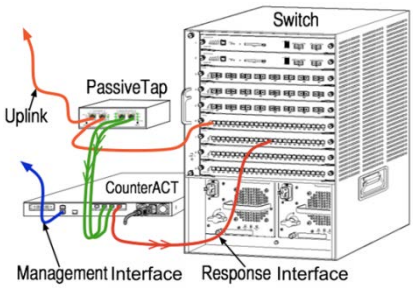
1 Distribuzione standard (interfacce di gestione, monitoraggio e risposta separate)

La distribuzione consigliata utilizza tre porte separate. Queste porte sono descritte in Interfacce di collegamento dell'appliance.



2 Commutatore in linea passivo

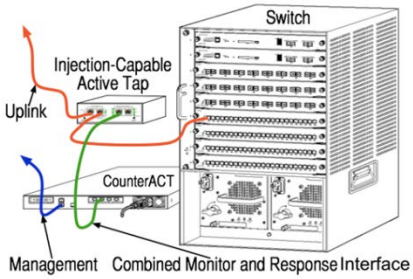
Invece di collegarsi alla porta di monitoraggio dello switch, l'appliance è in grado di utilizzare un commutatore in linea passivo.



Un commutatore in linea passivo richiede due porte di monitoraggio (una per il traffico upstream e una per il traffico downstream), nel caso in cui non sia disponibile un commutatore di *ricombinazione* che combini i due flussi duplex in una singola porta. Se il traffico sulla porta commutata è codificato con VLAN 802.1Q, allora anche la porta di risposta deve essere codificata con VLAN 802.1Q.

3 Commutatore in linea passivo (con funzione di iniezione)

L'appliance è in grado di utilizzare un commutatore in linea attivo. Se il commutatore è dotato di funzione di iniezione, l'appliance combina le porte di monitoraggio e di risposta in modo che non sia necessario configurare una porta di risposta separata sullo switch. Questa opzione è disponibile a prescindere dalla configurazione dello switch upstream o downstream.



4 Risposta livello IP (per installazioni con switch di Livello 3)

L'appliance è in grado di utilizzare la propria interfaccia di gestione per rispondere al traffico. Sebbene questa opzione possa essere utilizzata con qualsiasi traffico monitorato, si consiglia di utilizzarla soltanto in situazioni in cui l'appliance monitori porte che non fanno parte di alcuna VLAN e, quindi, che non possono rispondere al traffico monitorato utilizzando qualsiasi altra porta dello switch. Questo accade generalmente durante il monitoraggio di un collegamento tra due router. Questa opzione non è in grado di rispondere alle richieste dell'Address Resolution Protocol (ARP), che limita la capacità dell'appliance di rilevare analisi volte agli indirizzi IP inclusi nella subnet monitorata. Questa limitazione non viene applicata nel caso in cui il traffico tra i due router sia monitorato.

B. Note sulle Impostazioni dello switch

Codifiche VLAN (802.1Q)

- ***Monitoraggio di una VLAN singola***: se il traffico monitorato proviene da una singola VLAN, il traffico non necessita di codifiche VLAN 802.1Q.
- ***Monitoraggio VLAN multiple***: se il traffico monitorato proviene da due o più VLAN, allora *sia* la porta monitorata *sia* quella di risposta devono avere la codifica VLAN 802.1Q abilitata. Monitorare le VLAN multiple è consigliato in quanto fornisce la migliore copertura globale riducendo al minimo il numero delle porte di mirroring.
- Se lo switch non è in grado di utilizzare una codifica VLAN 802.1Q sulla porta di mirroring, eseguire una delle seguenti operazioni:
  - eseguire il mirroring di una singola VLAN;
  - eseguire il mirroring di una singola porta uplink non codificata;
  - utilizzare l'opzione di risposta del livello IP.
- Se lo switch è in grado di eseguire solo il mirroring di una porta, allora eseguire il mirroring di una singola porta uplink. È possibile che questa sia codificata. In genere, se lo switch rimuove le codifiche VLAN 802.1Q, è necessario utilizzare l'opzione di risposta del livello IP.

Linee guida aggiuntive

- Nei seguenti casi bisogna eseguire il mirroring soltanto di un'interfaccia (che consente la ricezione/trasmissione):
  - se lo switch non è in grado di eseguire sia il mirroring del traffico trasmesso che del traffico ricevuto;
  - se lo switch non è in grado di eseguire il mirroring di tutto il traffico dello switch;
  - se lo switch non è in grado di eseguire il mirroring di tutto il traffico su una VLAN.
- Verificare di non sovraccaricare la porta di mirroring.

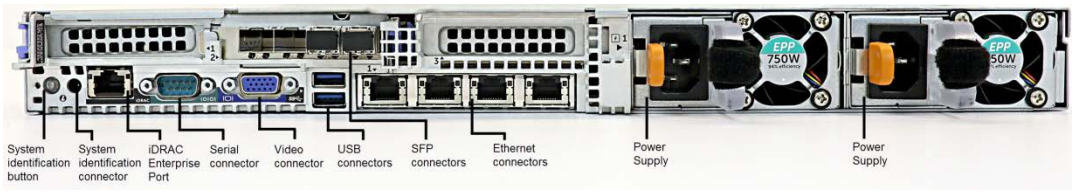
- Alcuni switch (ad esempio Cisco 6509) potrebbero richiedere che l'attuale configurazione della porta venga completamente eliminata prima di poter accedere a una nuova configurazione. La mancata eliminazione delle informazioni di una porta obsoleta spesso causa la rimozione delle codifiche 802.1Q da parte dello switch.

3. Collegamento dei cavi di rete e accensione

A. Rimozione dell'appliance dall'imballaggio e collegamento dei cavi

1. Rimuovere l'appliance e il cavo di alimentazione dal contenitore dall'imballaggio.
2. Rimuovere il kit di scorrimento ricevuto assieme all'appliance.
3. Assemblare il kit di scorrimento sull'appliance e montare l'appliance sul rack.
4. Collegare i cavi di rete tra le interfacce di rete presenti sul pannello posteriore dell'appliance e le porte dello switch.

Immagine esempio del pannello posteriore - Appliance CounterACT



È possibile sostituire gli SFP ForeScout forniti in dotazione con gli SFP Finisar precedentemente testati e approvati da ForeScout. Per ulteriori dettagli, fare riferimento alla *Guida di installazione CounterACT*.

B. Registro delle Assegnazioni delle interfacce

Al termine dell'installazione dell'appliance presso il data center e della console CounterACT, verrà richiesto di registrare le assegnazioni delle interfacce. Queste assegnazioni, chiamate *Definizioni di canale*, vengono inserite nel corso della procedura di configurazione guidata iniziale che si apre durante il primo accesso alla console.

Registrare le assegnazioni delle interfacce fisiche qui sotto e utilizzarle al termine dell'impostazione del canale sulla console.

Interfaccia Eth	Assegnazione interfaccia (ad esempio Gestione, Monitoraggio, Risposta)
Eth0	
Eth1	
Eth2	
Eth3	

Eth4	
Eth5	
Eth6	
Eth7	

C. Accensione dell'appliance

1. Collegare il cavo di alimentazione al connettore di alimentazione sul pannello posteriore dell'appliance.
2. Collegare l'altra estremità del cavo di alimentazione a una presa di alimentazione CA.
3. Collegare la tastiera e il monitor all'appliance o configurare l'appliance per il collegamento in serie. Per ulteriori informazioni, fare riferimento alla *Guida di installazione CounterACT*.
4. Accendere l'appliance dal pannello frontale.

4. Configurazione dell'appliance

Preparare le seguenti informazioni prima di configurare l'appliance.

Nome host appliance	
Password Amministratore CounterACT	Conservare la password in un luogo sicuro
Interfaccia di gestione	
Indirizzo IP appliance	
Network mask	
Indirizzo IP gateway predefinito	
Nome dominio DNS	
Indirizzi server DNS	

Dopo l'accensione, verrà richiesto di iniziare la configurazione con il seguente messaggio:

```
CounterACT Appliance boot is complete. (Avvio dell'appliance
CounterACT completato.)
Press <Enter> to continue. (Premere <Invio> per continuare.)
```

1. Premere **Enter** (Invio). In caso di appliance CounterACT 51xx, viene visualizzato il seguente menu:

```
CounterACT 8.0.0-<build> options: (Opzioni CounterACT <build>
8.0.0:)


1) Configure CounterACT (Configura CounterACT)
2) Restore saved CounterACT configuration (Ripristina una
configurazione CounterACT salvata)
3) Identify and renumber network interfaces (Identifica e
rinumera le interfacce di rete)
4) Configure keyboard layout (Configura il layout della
tastiera)
5) Turn machine off (Spegni il computer)
6) Reboot the machine (Riavvia il computer)

Choice (1-6) :1 (Scelta (1-6) :1)
```

   In caso di appliance CounterACT CT-xxxx, la versione visualizzata nella parte superiore del menu sarà CounterACT 7.0.0 oppure CounterACT 8.0.0.

- Nel caso venga mostrata la versione CounterACT 7.0.0, è possibile eseguire l'aggiornamento o eseguire una nuova installazione della versione 8.0.0. Per i dettagli, fare riferimento alla *Guida di installazione CounterACT*. Dopo l'aggiornamento o l'installazione della versione 8.0.0, verrà mostrato il menu elencato prima.
- Nel caso venga mostrata la versione CounterACT 8.0.0, il menu offre un'opzione per installare CounterACT 7.0.0 o per configurare CounterACT 8.0.0, come mostrato qui sotto. Se si seleziona CounterACT 7.0.0, non sarà più possibile reinstallare CounterACT 8.0.0 attraverso il menu di Configurazione. Per i dettagli sulla configurazione di CounterACT 7.0.0, consultare la *Guida di installazione CounterACT versione 7.0.0*.

```
CounterACT 8.0.0-<build> options: (Opzioni CounterACT <build>
8.0.0:)


1) Install CounterACT 7.0.0-<build> (Installa CounterACT 7.0.0-
<build> 2) Configure CounterACT (Configura CounterACT)
3) Restore saved CounterACT configuration (Ripristina una
configurazione CounterACT salvata)
4) Identify and renumber network interfaces (Identifica e
rinumera le interfacce di rete)
5) Configure keyboard layout (Configura il layout della
tastiera)
6) Turn machine off (Spegni il computer)
7) Reboot the machine (Riavvia il computer) Choice (1-7) :
(Scelta (1-7) :)
```

> *Se la configurazione viene interrotta o se è stata selezionata la versione di CounterACT sbagliata, sarà necessario ricreare l'immagine dell'appliance con la relativa versione del file ISO. Per ulteriori informazioni su come ricreare l'immagine dell'appliance, fare riferimento alla Guida di installazione CounterACT.*

2. Selezionare **Configure CounterACT** (Configura CounterACT). Al messaggio di richiesta:

   `Continue: (Yes/no)? (Continua: Sì/no?)`

   Premere **Enter** (Invio) per avviare la procedura di impostazione.

3. Viene aperto il messaggio di richiesta Modalità a elevata disponibilità. Premere **Enter** (Invio) per selezionare l'installazione standard.

4. Viene visualizzato il messaggio di richiesta CounterACT Initial Setup (Impostazione iniziale CounterACT). Premere **Enter** (Invio) per continuare.

5. Viene aperto il messaggio di richiesta Select CounterACT Installation Type (Selezione del tipo di installazione di CounterACT). Digitare **1** e premere **Enter** (Invio) per installare un appliance CounterACT standard.

   La procedura di installazione viene inizializzata. Questa operazione può richiedere alcuni minuti.

6. Viene aperto il messaggio di richiesta Select Licensing Mode (Selezione della modalità di gestione licenze). Selezionare la modalità di gestione licenze utilizzata dalla propria distribuzione. La modalità di gestione licenze viene determinata durante l'acquisto. ***Do not type a value until you have verified what licensing mode your deployment uses*** (Non digitare alcun valore prima di aver verificato quale modalità di gestione licenze utilizza la propria distribuzione). Contattare il proprio rappresentante ForeScout per verificare la propria modalità di gestione licenze o se si ha inserito la modalità sbagliata.

7. Al messaggio di richiesta Enter Machine Description (Inserisci descrizione computer), inserire un breve testo che identifichi questo appliance, quindi premere **Enter** (Invio).

   Viene visualizzato il messaggio:

```
>>>>>> Set Administrator Password <<<<<< (Imposta password
amministratore)
This password will be used to log in as 'root' to the machine
Operating System and as 'admin' to the CounterACT Console.
The password must be between 6 and 15 characters long and should
contain at least one non-alphabetic character. (Questa password
verrà utilizzata per accedere come 'root' al sistema operativo
del computer e come 'admin' alla console CounterACT. La password
deve contenere tra i 6 e i 15 caratteri e almeno un carattere
non alfabetico.)
Administrator password : (Password amministratore)
```

8. Al messaggio di richiesta Set Administrator Password (Imposta password amministratore), digitare la stringa con la propria password (la stringa non è ripetuta sullo schermo) e premere **Enter** (Invio). Verrà richiesto di confermare la password. La password deve contenere tra i 6 e i 15 caratteri e almeno un carattere non alfabetico.

Accedere all'appliance come root*, quindi accedere alla console come* admin*.*

9. Al messaggio di richiesta Set Host Name (Imposta nome Host), digitare un nome host e premere **Enter** (Invio). Il nome host può essere utilizzato all'accesso alla console e viene visualizzato sulla console per aiutare a identificare l'appliance CounterACT che si sta visualizzando. Il nome host non deve contenere più di 13 caratteri.

10. Viene visualizzata la schermata Configure Network Settings (Configura impostazioni di rete) che richiede una serie di parametri di configurazione. Digitare un valore ad ogni messaggio di richiesta e premere **Enter** (Invio) per visualizzare il messaggio di richiesta successivo.

    – I componenti CounterACT comunicano attraverso interfacce di gestione. Il numero delle interfacce di gestione elencato dipende dal modello dell'appliance.

    – Il **Management IP address** (Indirizzo IP gestione) è l'indirizzo dell'interfaccia attraverso la quale i componenti CounterACT comunicano. Aggiungere un VLAN ID per questa interfaccia solo se l'interfaccia utilizzata dai componenti CounterACT per comunicare è collegata alla porta codificata.

- Se è presente più di un **DNS server address** (Indirizzo server DNS), separare ciascun indirizzo con uno spazio. La maggior parte dei server DNS interni risolvono indirizzi esterni e interni ma potrebbe essere necessario includere un server DNS di risoluzione esterna. Poiché quasi tutte le query DNS eseguite dall'appliance saranno per gli indirizzi interni, il server DNS esterno dovrebbe essere elencato per ultimo.

11. Viene visualizzata la schermata di Setup Summary (Riepilogo procedura di impostazione). Verrà richiesto di eseguire test di connettività generale, riconfigurare le impostazioni o completare la procedura di impostazione. Digitare **D** per completare la procedura di impostazione.

Licenza

Al termine della configurazione, assicurarsi che il proprio appliance CounterACT disponga di una licenza valida. Lo stato della licenza predefinito relativo al proprio appliance CounterACT dipende dalla modalità di licenza utilizzata dalla propria distribuzione.

- Se la propria distribuzione CounterACT opera in ***Per-Appliance Licensing Mode*** (Modalità di licenza per appliance), è possibile iniziare a lavorare utilizzando la licenza di prova, valida per 30 giorni. Durante questo periodo, si riceverà una licenza permanente da ForeScout che deve essere posizionata in una cartella accessibile sul proprio disco rigido o sulla rete. Installare la licenza da questa posizione prima della scadenza della licenza di prova di 30 giorni (se necessario, è possibile richiedere un'estensione della licenza di prova).

  Verranno mostrati diversi messaggi di avviso in prossimità della data di scadenza della licenza di prova. Per ulteriori informazioni sugli avvisi della licenza di prova, fare riferimento alla *Guida all'amministrazione di CounterACT*.

  Se si lavora con un sistema virtuale CounterACT:

  - La licenza di prova non è installata automaticamente in questa fase. È necessario installare la licenza di prova ricevuta tramite email dal proprio rappresentate ForeScout.
  - Almeno un appliance CounterACT deve essere in grado di accedere a Internet. Questa connessione è utilizzata per convalidare le licenze CounterACT sul Server licenze ForeScout. Le licenze che non possono essere autenticate per un mese saranno revocate. CounterACT invierà un'email di avviso ogni giorno a indicare la presenza di un errore di comunicazione con il server.

    Per ulteriori informazioni, fare riferimento alla *Guida di installazione CounterACT*.

- Se la propria distribuzione CounterACT opera in ***Centralized Licensing Mode*** (Modalità di licenza centralizzata), l'*Entitlement administrator* (Amministratore beneficiario) riceverà un'email quando una licenza abilitata verrà creata e sarà disponibile nel ForeScout Customer Portal (Portale clienti ForeScout). Una volta disponibile, il *CounterACT administrator* (Amministratore CounterACT) della distribuzione è in grado di attivare la licenza nella console CounterACT. Fino all'attivazione della licenza, i contenuti CounterACT non funzioneranno in maniera corretta. Ad esempio, le policy non saranno valutate e le azioni non verranno eseguite. *Durante l'installazione di sistema nessuna licenza di prova verrà installata automaticamente.*

Per ulteriori informazioni sulla gestione delle licenze, fare riferimento alla *Guida all'amministrazione di CounterACT*.

5. Gestione remota

Procedura di impostazione iDRAC

Integrated Dell Remote Access Controller (iDRAC) è un server di sistema integrato che offre agli appliance CounterACT accesso remoto indipendente dalla posizione o dal sistema operativo tramite LAN o Internet. Utilizzare il modulo per realizzare un accesso a KVM, accendere/spegnere/ripristinare ed eseguire le attività di risoluzione problemi e di manutenzione.

Eseguire le seguenti operazioni per lavorare con il modulo iDRAC:

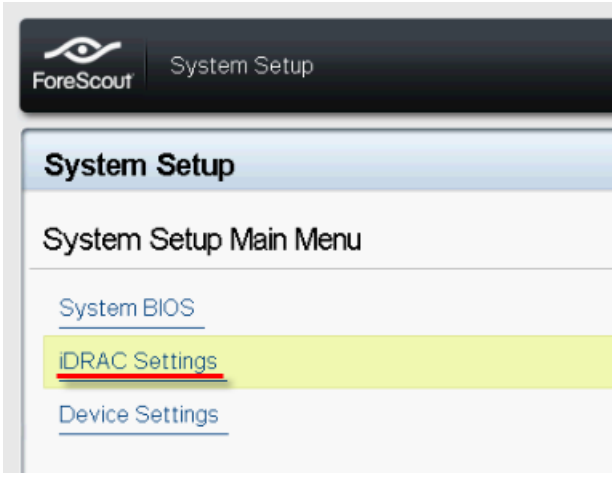
- Abilitare e configurare il modulo iDRAC
- Collegare il modulo alla rete
- Accesso a iDRAC

Abilitare e configurare il modulo iDRAC

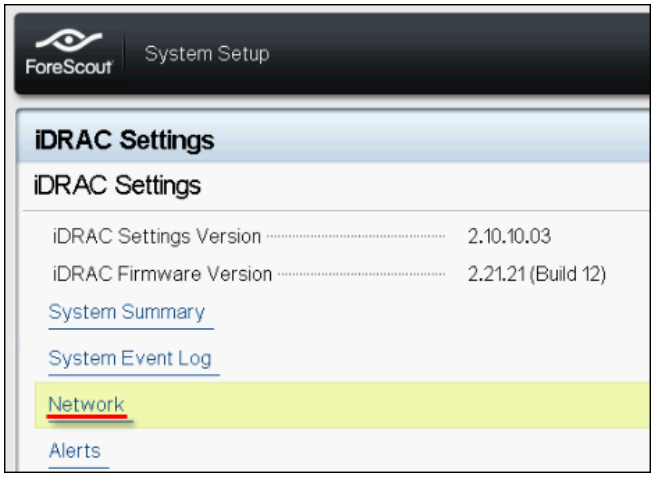
Modificare le impostazioni iDRAC per abilitare l'accesso remoto sull'appliance CounterACT. Questa sezione descrive le impostazioni di integrazione di base necessarie per lavorare con CounterACT.

Per configurare iDRAC:

1. Accendere l'appliance da gestire.
2. Selezionare F2 durante il processo di avvio.
3. Nella pagina del System Setup Main Menu (Menu principale impostazione del sistema), selezionare **iDRAC Settings** (Impostazioni iDRAC).

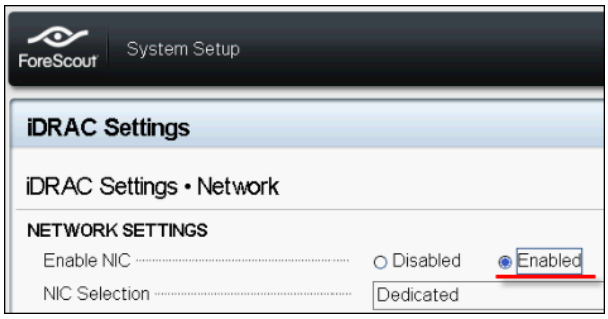


4. Nella pagina iDRAC Settings (Impostazioni iDRAC), selezionare **Network** (Rete).



5. Configurare le seguenti Impostazioni di rete:

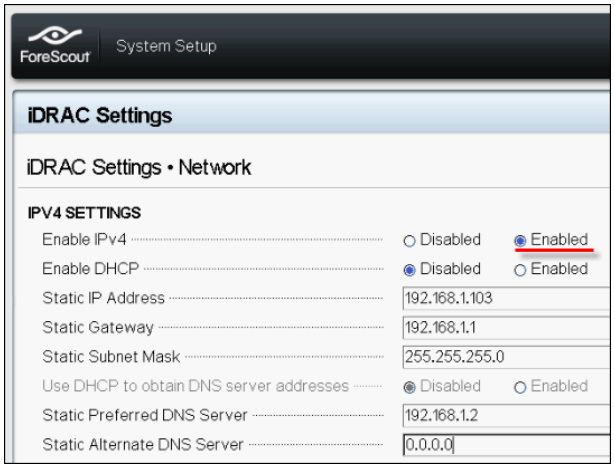
   – ***Network Settings*** (Impostazioni di rete). Verificare che il campo **Enable NIC** (Abilita NIC) sia impostato su **Enabled** (Abilitato).



   – ***Common Settings*** (Impostazioni comuni). Nel campo DNS DRAC Name (Nome DRAC DNS) è possibile aggiornare un DNS dinamico (facoltativo).

   – ***IPV4 Settings*** (impostazioni IPV4). Verificare che il campo **Enable IPV4** (Abilita IPV4) sia impostato su **Enabled** (Abilitato).

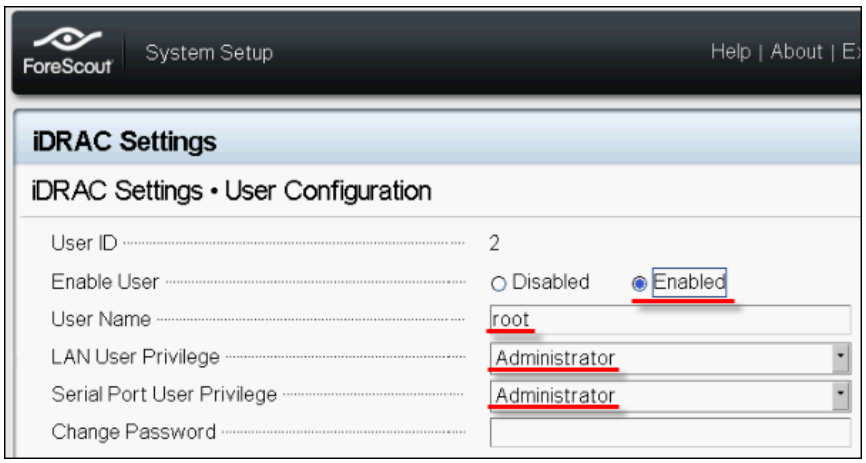
     Impostare il campo **Enable DHCP** (Abilita DHCP) su **Enabled** (Abilitato) per utilizzare l'indirizzo IP dinamico o su **Disabled** (Disabilitato) per utilizzare un indirizzo IP statico. Se abilitato, il DHCP assegnerà automaticamente indirizzo IP, gateway e subnet mask all'iDRAC. Se disabilitato, inserire i valori per i campi **Static IP Address** (Indirizzo IP statico), **Static Gateway** (Gateway statico) e **Static Subnet Mask** (Subnet Mask statico).



6. Selezionare **Back** (Indietro).
7. Selezionare **User Configuration** (Configurazione utente).
8. Configurare i seguenti campi di Configurazione utente per l'utente root:
   - ***Enable User*** (Abilita utente). Verificare che questo campo sia impostato su Enabled (Abilitato).

     Il nome utente configurato qui non corrisponde al nome utente CounterACT.

   - ***LAN and Serial Port User Privileges*** (Privilegi utente LAN e porta seriale). Impostare i livelli di privilegi su Administrator (Amministratore).
   - ***Change Password*** (Modifica password). Impostare una password per l'acceso utente.

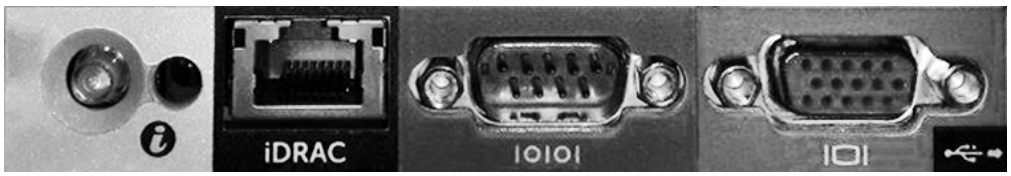


9. Selezionare **Back** (Indietro) e poi selezionare **Finish** (Fine). Confermare le impostazioni modificate.

   Le impostazioni modificate vengono salvate e il sistema viene riavviato.

Collegare il modulo alla rete

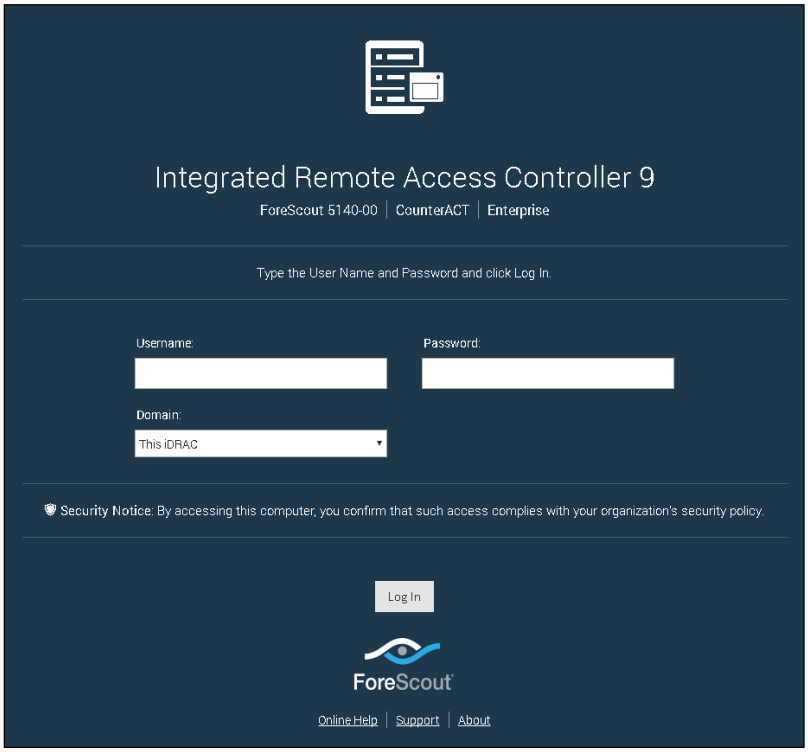
L'iDRAC si connette a una rete Ethernet. È consuetudine collegarlo a una rete di gestione. L'immagine seguente mostra la posizione della porta iDRAC nella parte posteriore del pannello dell'appliance CT-1000:



Accesso a iDRAC

Accedere a iDRAC:

1. Spostarsi fino all'indirizzo IP o al nome dominio configurato in **iDRAC Settings** (Impostazioni iDRAC) > **Network** (Rete).



2. Inserire Username e Password configurati nella pagina User Configuration (Configurazione utente) della procedura di impostazione del sistema iDRAC.
3. Selezionare **Submit** (Invia).

Per ulteriori informazioni su iDRAC, fare riferimento al *Manuale dell'utente iDRAC*. È possibile accedere a questo manuale in una delle seguenti posizioni, a seconda della modalità di licenza utilizzata dalla propria distribuzione:

- Per-Appliance Licensing Mode (Modalità di licenza per appliance) - https://updates.forescout.com/downloads/support/iDRAC_user_guide.pdf

- Centralized Licensing Mode (Modalità di licenza centralizzata) – Customer Portal, pagina Documentazioni.

Per scoprire la modalità di licenza utilizzata dalla propria distribuzione, consultare Documentazione CounterACT aggiuntiva (*Identifying Your Licensing Mode in the Console* Identificazione della Modalità di licenza sulla console).

È fondamentale aggiornare la password di root predefinita se non è già stato fatto in precedenza.

6. Verifica della connettività

Verificare la connessione dell'interfaccia di gestione

Per testare la connessione dell'interfaccia di gestione, accedere all'appliance ed eseguire il seguente comando:

fstool linktest

Vengono visualizzate le seguenti informazioni:

```
Management Interface status (Stato interfaccia di gestione)
Pinging default gateway information (Ping dell’indirizzo del gateway predefinito)
Ping statistics (Statistiche ping)
Performing Name Resolution Test (Esecuzione del test di risoluzione nomi)
Test summary (Riepilogo test)
```

Eseguire un test del ping

Eseguire il seguente comando dall'appliance a un desktop di rete per verificare la connettività:

Ping <network_desktop_IP_address>

7. Installazione della console CounterACT

Installare la console CounterACT

La console è l'applicazione per la gestione di CounterACT utilizzata per visualizzare informazioni dettagliate sugli endpoint e per controllarli. Queste informazioni vengono raccolte dai dispositivi CounterACT. Per ulteriori informazioni, fare riferimento alla *Guida all'amministrazione CounterACT*.

È necessario fornire un computer per ospitare il software relativo all'applicazione della console CounterACT. I requisiti hardware minimi sono:

- Computer non dedicato, con sistemi operativi:
  - Windows 7/8/8.1/10
  - Windows Server 2008/2008 R2/2012/2012 R2/2016
  - Linux RHEL/CentOS 7
- 2 GB di RAM
- 1 GB di spazio su disco

Il seguente metodo è disponibile per eseguire l'installazione della console:

Utilizzare il software di installazione incorporato nell'appliance.

1. Aprire una finestra del browser dal computer della console.
2. Nella riga indirizzo del browser digitare:

   `http://<Appliance_ip>/install`

   Dove Appliance_ip è l'indirizzo IP di questo appliance. Il browser visualizza la finestra di installazione della console.
3. Seguire le istruzioni su schermo.

Accesso

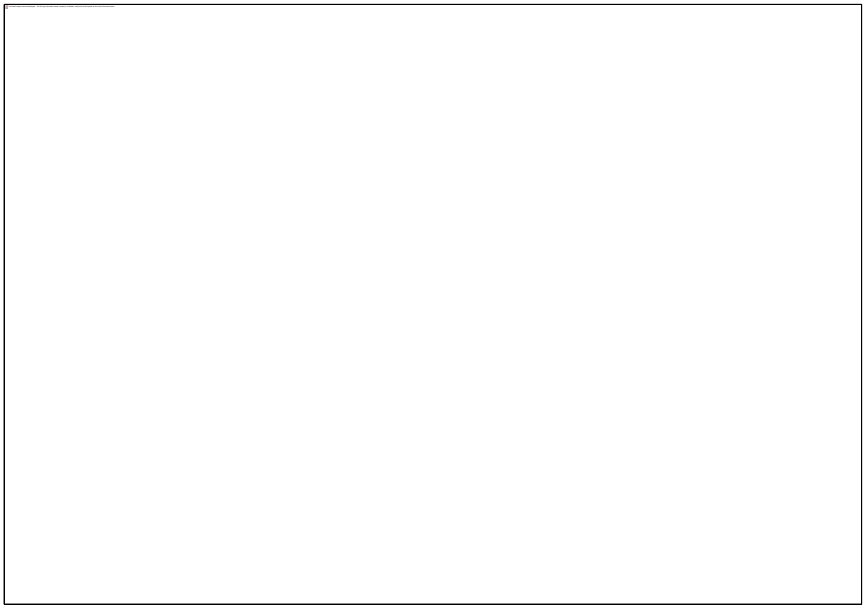
Al termine dell'installazione è possibile effettuare l'accesso alla console CounterACT.

1. Selezionare l'icona CounterACT dalla posizione dove è stato creato il collegamento.

2. Inserire l'indirizzo IP o il nome host dell'appliance nel campo **IP/Name** (IP/Nome).
3. Nel campo **User Name** (Nome utente), inserire admin.
4. Nel campo **Password** (Password), inserire la password creata durante l'installazione dell'appliance.
5. Selezionare **Login** (Accesso) per avviare la console.

Eseguire la procedura di Configurazione iniziale

Al primo accesso, viene aperta la procedura di configurazione guidata iniziale. La procedura guidata mostra le fasi di configurazione essenziali per configurare CounterACT e permetterne l'esecuzione in maniera rapida ed efficiente.



Prima di avviare la configurazione iniziale

Preparare le seguenti informazioni prima di avviare la procedura guidata:

Informazioni richieste dalla procedura guidata	**Valore**
Indirizzo server NTP utilizzato dalla propria organizzazione (facoltativo)	
Indirizzo IP mail relay interno per consentire l'invio di email di avviso se il traffico SMTP non è consentito dall'appliance (facoltativo)	
Indirizzo email amministratore CounterACT	
Interfacce di monitoraggio e di risposta	
Per segmenti/VLAN senza DHCP, il segmento/VLAN di rete al quale l'interfaccia di risposta è direttamente collegata e un indirizzo IP permanente che CounterACT possa utilizzare in ognuna di tali VLAN	
Intervallo indirizzi IP che verranno monitorati dall'appliance (tutti gli indirizzi interni, inclusi gli indirizzi non utilizzati)	
Informazioni account utente LDAP e indirizzo IP server LDAP	
Credenziali del dominio, inclusi nome e password dell'account amministrativo del dominio	
Server di autenticazione, in modo che CounterACT possa analizzare quali host di rete sono stati correttamente autenticati	
Parametri SNMP, Fornitore e Indirizzo IP dello switch	

Per ulteriori informazioni sulla procedura guidata, fare riferimento alla *Guida all'amministrazione di CounterACT* o alla Guida in linea.

Documentazione CounterACT aggiuntiva

Per informazioni su altre caratteristiche e moduli CounterACT, fare riferimento alle seguenti risorse:

- Download documentazioni
- Portale documentazione
- Strumenti della Guida CounterACT

Download documentazioni

È possibile accedere ai download delle documentazioni da uno dei due portali ForeScout, a seconda della modalità di licenza utilizzata dalla propria distribuzione.

- ***Per-Appliance Licensing Mode (Modalità di licenza per appliance)*** - Portale degli aggiornamenti per i prodotti
- ***Centralized Licensing Mode (Modalità di licenza centralizzata)*** - Portale clienti

I download dei software sono disponibili anche da questi portali.

Per scoprire la modalità di licenza utilizzata dalla propria distribuzione, consultare Identificare la modalità di licenza nella console.

Portale degli aggiornamenti per i prodotti

Il Portale degli aggiornamenti per i prodotti fornisce collegamenti alle versioni di rilascio di CounterACT, moduli di Base e Contenuti e Moduli estesi, oltre alla documentazione correlata. Il portale fornisce anche diverse documentazioni aggiuntive.

Per accedere al Portale degli aggiornamenti per i prodotti:

1. Andare su https://updates.forescout.com/support/index.php?url=counteract.
2. Selezionare la versione di CounterACT desiderata.

Portale clienti

La pagina dei download sul Portale clienti ForeScout fornisce collegamenti alle versioni di rilascio di CounterACT acquistate, moduli di Base e Contenuti e Moduli estesi, oltre alla documentazione correlata. Il software e la relativa documentazione appariranno nella pagina dei download solo se si è in possesso di una licenza abilitata per il software. La pagina Documentazione sul portale fornisce svariata documentazione aggiuntiva.

Per accedere alla documentazione nel Portale clienti ForeScout:

1. Andare su https://forescout.force.com/support/.

2. Selezionare **Downloads** o **Documentation** (Documentazione).

Portale documentazione

Il Portale documentazione ForeScout è una libreria di ricerca basata sul Web che contiene informazioni sugli strumenti CounterACT, caratteristiche, funzionalità e integrazioni.

> *Se la propria distribuzione utilizza la Modalità di licenza centralizzata, è possibile che non siano disponibili le credenziali per accedere a questo portale.*

Per accedere al Portale documentazione:

1. Andare su www.forescout.com/docportal.
2. Utilizzare le proprie credenziali di assistenza clienti per accedere.
3. Selezionare la versione di CounterACT desiderata.

Strumenti della Guida CounterACT

Accedere alle informazioni direttamente dalla console CounterACT.

Pulsanti della Guida della Console

Utilizzare i pulsanti della *Guida* sensibile al contesto per accedere rapidamente alle informazioni sulle attività e gli argomenti col quale si sta lavorando.

Guida all'amministrazione CounterACT

Selezionare **CounterACT Help** (Guida CounterACT) dal menu **Help** (Guida).

File plug-in della Guida

1. Dopo l'installazione del plug-in, selezionare **Options** (Opzioni) dal menu **Tools** (Strumenti) e successivamente selezionare **Modules** (Moduli).
2. Selezionare il plug-in e successivamente selezionare **Help** (Guida).

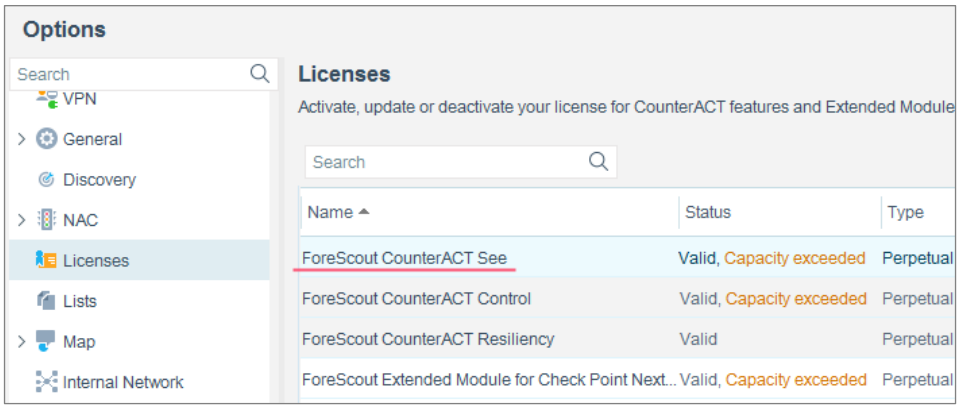
Portale documentazione

Selezionare **Documentation Portal** (Portale documentazione) dal menu **Help** (Guida).

Identificare la modalità di licenza nella console

Se Enterprise Manager ha una licenza *ForeScout CounterACT* vedere nell'elenco della console, la distribuzione sta operando in Modalità di licenza centralizzata. In caso contrario, la distribuzione sta operando in Modalità di licenza per appliance.

Selezionare **Options > Licenses** (Opzioni > Licenze) per vedere se è elencata una licenza *ForeScout CounterACT See* nella tabella.



Contattare il proprio rappresentante ForeScout per eventuali domande riguardo l'identificazione della propria modalità di licenza.

Informativa legale

Questi prodotti si basano su software sviluppati da ForeScout. I prodotti descritti in questo documento potrebbero essere protetti da uno o più brevetti negli Stati Uniti d'America: #6,363,489, #8,254,286, #8,590,004, #8,639,800 e #9,027,079, oltre ad altri brevetti negli Stati Uniti d'America e in altri paesi.

Inviare domande e commenti relativi a questo documento a: support@forescout.com

2018-03-27 15:04