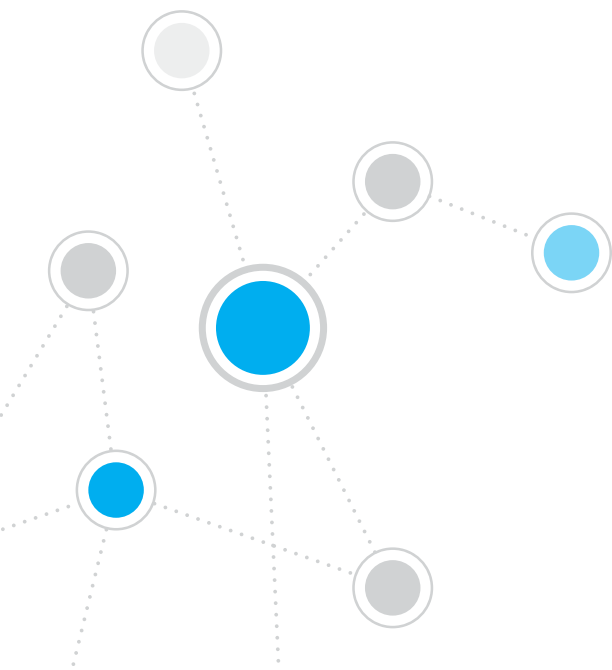




ForeScout CounterACT[®] 7

Appliance CounterACT singola

Guida rapida di installazione



Sommario

Introduzione a ForeScout CounterACT® versione 7	3
Contenuto della confezione di CounterACT	3
Panoramica	4
1. Creare un piano di distribuzione	5
Dove distribuire l'Appliance	5
Connessioni delle interfacce dell'Appliance	5
2. Configurazione dello switch	8
A. Opzioni di connessione dello switch	8
B. Note per la configurazione dello switch	9
3. Connessione dei cavi di rete e accensione	10
A. Disimballo dell'Appliance e collegamento dei cavi	10
B. Annotazione delle assegnazioni delle interfacce	11
C. Accensione dell'Appliance	11
4. Configurazione dell'Appliance	12
Licenza	14
Requisiti per la connessione di rete	14
5. Gestione remota	15
Configurazione del modulo iDRAC	15
Collegamento del modulo alla rete	18
Accesso a iDRAC	18
6. Verifica della connettività	19
Verifica della connessione dell'interfaccia di gestione	19
Verifica della connettività dello switch/Appliance	19
Esecuzione della verifica ping	20
7. Configurazione della Console CounterACT	21
Installazione della Console CounterACT	21
Accesso	22
Esecuzione della configurazione iniziale	22
Informazioni di contatto	24

Introduzione a ForeScout CounterACT® versione 7

ForeScout CounterACT è un'appliance per la sicurezza fisica o virtuale che identifica e valuta dinamicamente i dispositivi e le applicazioni di rete nell'istante in cui si collegano alla rete. Poiché CounterACT non richiede agenti, funziona con i dispositivi dell'utente: gestiti e non gestiti, noti e non noti, su PC e dispositivi mobili, incorporati e virtuali. CounterACT determina rapidamente l'utente, il proprietario, il sistema operativo, la configurazione del dispositivo, il software, i servizi, lo stato della patch e la presenza di agenti di sicurezza. Successivamente fornisce soluzioni, controlli e il monitoraggio continuo di questi dispositivi man mano che entrano ed escono dalla rete. Tutto questo integrandosi senza alcun tipo di problema con l'infrastruttura IT esistente.



Questa guida descrive l'installazione di una singola Appliance CounterACT autonoma.

Per informazioni più approfondite o per istruzioni su come distribuire più Appliance per la protezione della rete dell'intera azienda, consultare la *Guida all'installazione di CounterACT* e il *Manuale utente della Console*. Tali documenti sono disponibili sul CD di CounterACT nella directory /docs.

È inoltre possibile consultare il sito Web dell'assistenza all'indirizzo <https://www.forescout.com/support> per la documentazione più aggiornata, gli articoli della knowledge base e gli aggiornamenti relativi all'Appliance in uso.

Contenuto della confezione di CounterACT

- Appliance CounterACT
- Guida rapida di installazione
- CD di CounterACT con software Console, Manuale utente della Console e Guida all'installazione di CounterACT
- Documento di garanzia
- Supporti di montaggio
- Cavo di alimentazione
- Cavo di collegamento Console DB9 (solo per le connessioni seriali)

Panoramica

Per configurare l'Appliance CounterACT, eseguire la seguente procedura:

1. Creare un piano di distribuzione
2. Configurare lo switch
3. Collegare i cavi di rete e l'alimentazione
4. Configurare l'Appliance
5. Gestione remota
6. Verificare la connettività
7. Configurare la Console CounterACT

1. Creare un piano di distribuzione

Prima di eseguire l'installazione, è necessario decidere dove distribuire l'Appliance e informarsi sulle connessioni delle interfacce dell'Appliance.

Dove distribuire l'Appliance

Per assicurare un'efficace distribuzione e un funzionamento ottimale di CounterACT, è fondamentale scegliere la corretta posizione per l'Appliance nella rete. La posizione corretta dipende dagli obiettivi di implementazione desiderati e dalle policy di accesso alla rete. L'Appliance deve essere in grado di monitorare il traffico pertinente alla policy desiderata. Ad esempio, se la policy di riferimento si basa sul monitoraggio degli eventi di autorizzazione dagli endpoint ai server di autenticazione aziendali, l'Appliance dovrà essere installata in modo da poter vedere il flusso di traffico dagli endpoint a uno o più server di autenticazione.

Per ulteriori informazioni sull'installazione e la distribuzione, consultare la Guida all'installazione di CounterACT, disponibile sul CD di CounterACT accluso alla presente documentazione.

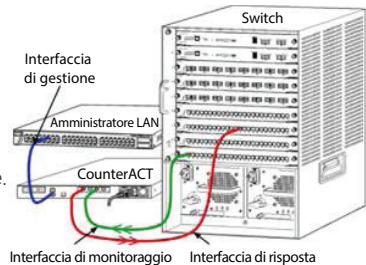
Connessioni delle interfacce dell'Appliance

In genere, l'Appliance è configurata con tre connessioni allo switch di rete.

Interfaccia di gestione

Questa interfaccia consente di gestire CounterACT e di eseguire query e ispezioni approfondite degli endpoint. L'interfaccia deve essere connessa a una porta dello switch dotata di accesso a tutti gli endpoint della rete.

Ogni Appliance richiede una connessione di gestione singola alla rete. Tale connessione necessita di un indirizzo IP sulla LAN locale e dell'accesso alla porta 13000/TCP dai computer che eseguono l'applicazione di gestione della Console CounterACT. L'interfaccia di gestione deve avere accesso ai seguenti elementi sulla rete:



Porta	Servizio	A o da CounterACT	Funzione
22/TCP	SSH	A	Consente l'accesso all'interfaccia della riga di comando di CounterACT
2222/TCP			(Disponibilità elevata) Consente l'accesso ai dispositivi CounterACT fisici che fanno parte del cluster a disponibilità elevata. Utilizzare la porta 22/TCP per accedere agli indirizzi IP condivisi (virtuali) del cluster.

Porta	Servizio	A o da CounterACT	Funzione
25/TCP	SMTP	Da	Utilizzato per inviare e-mail da CounterACT
53/UDP	DNS	Da	Consente a CounterACT di risolvere gli 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 orario NTP. Per impostazione predefinita, CounterACT utilizza ntp.foreScout.net.
135/TCP	MS-WMI	Da	Consente l'ispezione remota degli endpoint Windows.
139/TCP	SMB, MS-RPP	Da	Consente l'ispezione remota degli endpoint Windows (per gli endpoint su cui è in esecuzione Windows 7 e versioni precedenti).
445/TCP			Consente l'ispezione remota degli endpoint Windows.
161/UDP	SNMP	Da	Consente a CounterACT di comunicare con i dispositivi dell'infrastruttura di rete, quali switch e router. Per informazioni sulla configurazione di SNMP, consultare il <i>Manuale utente della Console CounterACT</i> .
162/UDP	SNMP	A	Consente a CounterACT di ricevere le trap SNMP dai dispositivi dell'infrastruttura di rete, quali switch e router. Per informazioni sulla configurazione di SNMP, consultare il <i>Manuale utente della Console CounterACT</i> .
443/TCP	HTTPS	A	Consente il reindirizzamento HTTP utilizzando TLS.
2200/TCP	Secure Connector	A	Consente a SecureConnector di creare una connessione protetta (con crittografia SSH) all'Appliance dai computer Macintosh/Linux. <i>SecureConnector</i> è un agente basato su script che consente la gestione degli endpoint Macintosh e Linux mentre sono connessi alla rete.
10003/TCP	Secure Connector for Windows	A	Consente a SecureConnector di creare una connessione protetta (con crittografia TLS) all'Appliance dai computer Windows. <i>SecureConnector</i> è un agente che consente la gestione degli endpoint Windows mentre sono connessi alla rete. Per ulteriori informazioni su SecureConnector, consultare il <i>Manuale utente della Console CounterACT</i> .

			Quando SecureConnector si collega a un'Appliance o a Enterprise Manager, viene reindirizzato all'Appliance a cui è assegnato il relativo host. Assicurarsi che questa porta sia aperta a tutte le Appliance e a Enterprise Manager per consentire una mobilità trasparente all'interno dell'organizzazione.
13000/TCP	CounterACT	A	Consente la connessione dalla Console all'Appliance. Per i sistemi con più Appliance CounterACT, consente la connessione dalla Console a Enterprise Manager e da Enterprise Manager a ciascuna Appliance.

Interfaccia di monitoraggio

Questa connessione consente all'Appliance di monitorare e registrare il traffico di rete.

Su una porta dello switch viene effettuato il mirroring del traffico, che viene quindi monitorato dall'Appliance. L'assegnazione del VLAN tag 802.1Q al traffico dipende dal numero di VLAN soggette a mirroring.

- **VLAN singola (senza tag):** Quando il traffico monitorato viene generato da una VLAN singola, il traffico soggetto a mirroring non necessita di essere dotato del VLAN tag.
- **Più VLAN (dotate di tag):** Quando il traffico monitorato proviene da più VLAN, il traffico soggetto a mirroring *deve* essere dotato del VLAN tag 802.1Q.

Quando i due switch sono connessi come coppia ridondante, l'Appliance deve monitorare il traffico da entrambi gli switch.

L'interfaccia di monitoraggio non richiede un indirizzo IP.

Interfaccia di risposta

L'Appliance risponde al traffico utilizzando questa interfaccia. Il traffico di risposta viene utilizzato per la protezione da attività dannose e per l'esecuzione delle azioni delle policy NAC. Tali azioni possono includere, ad esempio, il reindirizzamento dei browser Web o l'esecuzione del blocco firewall. La configurazione della porta dello switch correlata dipende dal traffico monitorato.

- **VLAN singola (senza tag):** Quando il traffico monitorato viene generato da una VLAN singola, l'interfaccia di risposta deve essere configurata in modo da fare parte della stessa VLAN. In tal caso, l'Appliance richiede un indirizzo IP singolo su quella VLAN.
- **Più VLAN (dotate di tag):** Se il traffico monitorato proviene da più VLAN, anche l'interfaccia di risposta deve essere configurata con il tag 802.1Q per le stesse VLAN. L'Appliance richiede un indirizzo IP per ogni VLAN protetta.

2. Configurazione dello switch

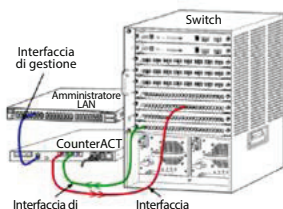
A. Opzioni di connessione dello switch

L'Appliance è stata progettata per integrarsi senza problemi in svariati ambienti di rete. Per integrare correttamente l'Appliance nella rete, verificare che lo switch sia configurato in modo da monitorare il traffico richiesto.

Sono disponibili diverse opzioni per connettere l'Appliance allo switch.

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

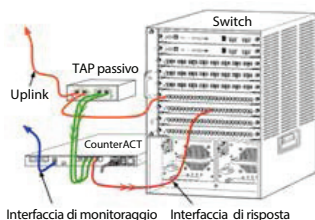
La distribuzione consigliata utilizza tre porte separate. Tali porte sono descritte in *Connessioni delle interfacce dell'Appliance*.



2. TAP passivo in linea

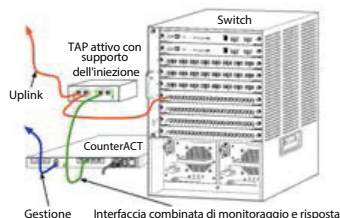
Anziché connettersi a una porta di monitoraggio dello switch, l'Appliance può utilizzare un TAP in linea passivo.

Un TAP passivo richiede due porte di monitoraggio, tranne nel caso dei TAP di ricombinazione, che combinano due flussi duplex in un'unica porta. Il traffico sulla porta con TAP e sull'interfaccia di risposta deve essere configurato allo stesso modo. Ad esempio, se il traffico sulla porta con TAP è dotato di VLAN tag (802.1Q), anche l'interfaccia di risposta deve essere una porta dotata di VLAN tag.



3. TAP in linea attivo (con supporto dell'iniezione)

Quando l'Appliance utilizza un TAP in linea con supporto dell'iniezione, le interfacce di monitoraggio e di risposta possono essere combinate. Non è necessario configurare una porta di risposta separata sullo switch. Questa opzione può essere utilizzata per qualsiasi tipo di configurazione switch a monte o a valle.



4. Risposta livello IP (per le installazioni switch di livello 3)

L'Appliance può utilizzare la propria interfaccia di gestione per rispondere al traffico. Benché questa opzione possa essere utilizzata con qualsiasi traffico monitorato, è consigliata quando l'Appliance monitora porte che non fanno parte di alcuna VLAN e quindi non è in grado di rispondere al traffico monitorato utilizzando qualsiasi altra porta dello switch. Ciò avviene, di norma, durante il monitoraggio di un collegamento tra due router.

Questa opzione non è in grado di rispondere alle richieste Address Resolution Protocol (ARP), il che limita la capacità dell'Appliance di rilevare le scansioni destinate agli indirizzi IP inclusi nella sottorete monitorata. Questa limitazione non si applica quando viene monitorato il traffico tra due router.

B. Note per la configurazione dello switch

VLAN tag (802.1Q)

- **Monitoraggio di una VLAN singola (traffico senza tag)** Se il traffico monitorato proviene da una VLAN singola, non necessita dei tag 802.1Q.
- **Monitoraggio di più VLAN (traffico con tag)** Se il traffico monitorato proviene da due o più VLAN, *in entrambe* le interfacce (di monitoraggio e di risposta) deve essere abilitato il tag 802.1Q. Il monitoraggio di più VLAN è l'opzione consigliata, dal momento che fornisce la miglior copertura complessiva riducendo il numero di porte di mirroring.
- Se lo switch non è in grado di utilizzare un VLAN tag 802.1Q sulle porte di mirroring, eseguire una delle seguenti operazioni:
 - Eseguire il mirroring su un'unica VLAN
 - Eseguire il mirroring di una singola porta uplink, senza tag
 - Utilizzare l'opzione di risposta livello IP
- Se lo switch è in grado di eseguire il mirroring di una sola porta, eseguire il mirroring di una singola porta uplink, che può anche essere dotata di tag. In generale, se lo switch rimuove i VLAN tag 802.1Q, è necessario utilizzare l'opzione di risposta livello IP.

Altre informazioni

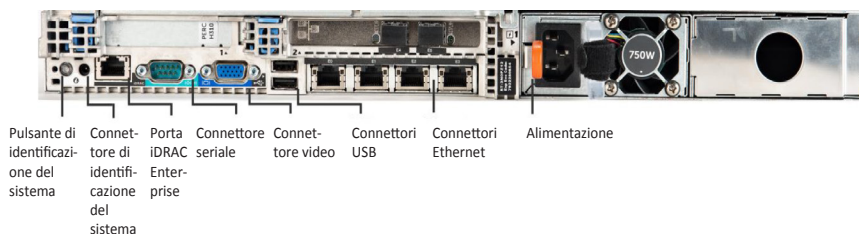
- Se lo switch non è in grado di eseguire il mirroring del traffico in trasmissione e ricezione, monitorare l'intero switch, le VLAN complete (in modo da disporre di trasmissione/ricezione) o una sola interfaccia (che consente la trasmissione/ricezione). Verificare che la porta di mirroring non sia sovraccarica.
- Alcuni switch, ad esempio Cisco 6509, potrebbero richiedere l'eliminazione completa delle porte preesistenti prima di poter immettere le nuove configurazioni. Il risultato più comune quando non si eliminano le informazioni sulle porte precedenti è l'eliminazione dei tag 802.1Q da parte dello switch.

3. Connessione dei cavi di rete e accensione

A. Disimballo dell'Appliance e collegamento dei cavi

1. Estrarre l'Appliance e il cavo di alimentazione dal contenitore utilizzato per la spedizione.
2. Estrarre il kit cremagliera fornito con l'Appliance.
3. Assemblare il kit cremagliera sull'Appliance e montare quest'ultima sul rack.
4. Collegare i cavi di rete tra le interfacce di rete sul pannello posteriore dell'Appliance e le porte dello switch.

Esempio di pannello posteriore: dispositivo CounterACT



B. Annotazione delle assegnazioni delle interfacce

Dopo aver completato l'installazione dell'Appliance nel centro dati e aver installato la Console CounterACT, verrà richiesto di annotare le assegnazioni dell'interfaccia. Queste assegnazioni, denominate *Definizioni dei canali*, vengono immesse nella Procedura guidata di configurazione iniziale che si apre quando si accede per la prima volta alla Console.

Annotare qui sotto le assegnazioni delle interfacce fisiche e utilizzarle per il completamento della configurazione dei canali sulla Console.

Interfaccia Ethernet	Assegnazione interfaccia (ad es. gestione, monitoraggio, risposta)
Eth0	
Eth1	
Eth2	
Eth3	
Eth4	
Eth5	
Eth6	
Eth7	
Eth8	

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 c.a. a terra.
3. Collegare la tastiera e il monitor all'Appliance oppure impostare l'Appliance per la connessione seriale. Consultare la *Guida all'installazione di CounterACT* disponibile sul CD di CounterACT.
4. Accendere l'Appliance dal pannello anteriore.

Importante: spegnere il computer prima di scollegare.

4. Configurazione dell'Appliance

Prima di configurare l'Appliance, preparare le seguenti informazioni.

<input type="checkbox"/> Nome host Appliance	
<input type="checkbox"/> Password amministrativa CounterACT	Conservare la password in un luogo sicuro
<input type="checkbox"/> Interfaccia di gestione	
<input type="checkbox"/> Indirizzo IP Appliance	
<input type="checkbox"/> Network mask	
<input type="checkbox"/> Indirizzo IP gateway predefinito	
<input type="checkbox"/> Nome dominio DNS	
<input type="checkbox"/> Indirizzi server DNS	

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

```
CounterACT Appliance boot is complete. (L'avvio
dell'Appliance CounterACT è completo).
Press <Enter> to continue. (Premere <Invio> per
continuare).
```

1. Premere **Invio** per visualizzare il seguente menu:

```
1) Configure CounterACT (Configura CounterACT)
2) Restore saved CounterACT configuration
   (Ripristina configurazione CounterACT salvata)
3) Identify and renumber network interfaces
   (Identifica e rinumeri interfacce di rete)
4) Configure keyboard layout (Configura layout
   tastiera)
5) Turn machine off (Spegni Appliance)
6) Reboot the machine (Riavvia Appliance)
Choice (1-6) :1 [Scelta (1-6):1]
```

2. Selezionare **1**: Configure CounterACT (Configura CounterACT). Al prompt:

```
Continue: (yes/no)? [Continuare: (sì/no)?]
```

Premere **Invio** per avviare la configurazione.

3. Si apre il menu **High Availability Mode** (Modalità disponibilità elevata). Premere **Invio** per selezionare l'installazione standard.
4. Viene visualizzato il prompt **CounterACT Initial Setup** (Configurazione iniziale CounterACT). Premere **Invio** per continuare.
5. Si apre il menu **Select CounterACT Installation Type** (Seleziona tipo di installazione CounterACT). Immettere **1** e premere **Invio** per installare un'Appliance CounterACT standard. La configurazione viene inizializzata. L'operazione può richiedere alcuni minuti.

6. Al prompt **Enter Machine Description** (Immettere descrizione Appliance), immettere un breve testo per identificare il dispositivo e premere **Invio**.


Viene visualizzata la seguente schermata:

```
>>>>> Set Administrator Password <<<<<<
      (Impostazione password amministratore)

This password is used to log in as 'root' to
the machine Operating System and as 'admin' to
the CounterACT Console (Questa password viene
utilizzata per l'accesso come utente root
al sistema operativo del dispositivo e come
amministratore alla Console CounterACT) .
The password should be between 6 and 15
characters long and should contain at least
one non-alphabetic character (La password deve
essere lunga da 6 a 15 caratteri e contenere
almeno un carattere non alfabetico) .

Administrator password (Password amministratore):
```

7. Al prompt **Set Administrator Password** (Imposta password amministratore), immettere la password (la stringa non viene visualizzata sullo schermo) e premere **Invio**. Viene richiesto di confermare la password. La password deve essere lunga da sei a 15 caratteri e contenere almeno un carattere non alfabetico.

 *Eseguire l'accesso all'Appliance come utente root e accedere alla Console come amministratore.*

8. Al prompt **Set Host Name** (Imposta nome host), immettere un nome host e premere **Invio**. Il nome host può essere utilizzato durante l'accesso alla Console e viene visualizzato nella Console per aiutare l'utente a individuare l'Appliance CounterACT che sta visualizzando.
9. La schermata **Configure Network Settings** (Configura impostazioni di rete) richiede una serie di parametri di configurazione. Immettere un valore per ogni prompt e premere **Invio** per continuare.
- I componenti CounterACT comunicano tramite interfacce di gestione. Il numero delle interfacce di gestione elencate dipende dal modello dell'Appliance in uso.
 - L'**indirizzo IP di gestione** è l'indirizzo dell'interfaccia attraverso il quale comunicano i componenti CounterACT. Aggiungere un ID VLAN per questa interfaccia solo se l'interfaccia utilizzata per la comunicazione tra i componenti CounterACT è collegata a una porta dotata di tag.

- Se sono presenti più **indirizzi server DNS**, separare ogni indirizzo con uno spazio. La maggior parte dei server DNS interni risolvono gli indirizzi esterni e interni ma potrebbero richiedere l'inclusione di un server DNS per la risoluzione esterna. Poiché quasi tutte le query DNS eseguite dall'Appliance saranno riferite a indirizzi interni, il server DNS esterno deve essere elencato per ultimo.

10. Viene visualizzata la schermata **Setup Summary** (Riepilogo della configurazione). Viene richiesto di eseguire le verifiche di connettività generale, riconfigurare le impostazioni o completare la configurazione. Immettere **D** per completare la configurazione.

Licenza

Dopo l'installazione, è necessario installare la licenza demo iniziale fornita dal proprio rappresentante CounterACT. La licenza viene installata durante la configurazione iniziale della Console. Questa licenza demo iniziale è valida per un determinato numero di giorni. È necessario installare una licenza permanente prima della scadenza di questo periodo. Per informazioni sulla data di scadenza, si riceverà una comunicazione via e-mail. Inoltre, le informazioni sulla data di scadenza e sullo stato della licenza vengono visualizzate nella Console, riquadro Appliances/Devices (Appliance/ Dispositivi).

Una volta ricevuta una licenza permanente, essa viene convalidata ogni giorno dal server licenze ForeScout. Gli avvisi e le violazioni relativi alla licenza vengono visualizzati nel riquadro Device Details (Dettagli dispositivo).

Le licenze che non è possibile convalidare per un mese verranno revocate. Per ulteriori informazioni sulle licenze, consultare la Guida all'installazione di CounterACT.

Requisiti per la connessione di rete

Almeno un dispositivo CounterACT (Appliance o Enterprise Manager) deve disporre dell'accesso a Internet. Questa connessione viene utilizzata per convalidare le licenze CounterACT sul server licenze ForeScout.

Le licenze che non è possibile autenticare per un mese verranno revocate. CounterACT invierà un avviso e-mail comunicando che è presente un errore di comunicazione con il server.

5. Gestione remota

Configurazione del modulo iDRAC

L'Integrated Dell Remote Access Controller (iDRAC) è una soluzione di sistema server integrata che offre l'accesso remoto indipendente dalla posizione/indipendente dal sistema operativo sulla LAN o su Internet alle Appliance/Enterprise Manager CounterACT. Utilizzare questo modulo per eseguire l'accesso KVM, accendere/spegnere/ripristinare ed eseguire attività di risoluzione dei problemi e manutenzione.

Per utilizzare il modulo iDRAC, eseguire le seguenti operazioni:

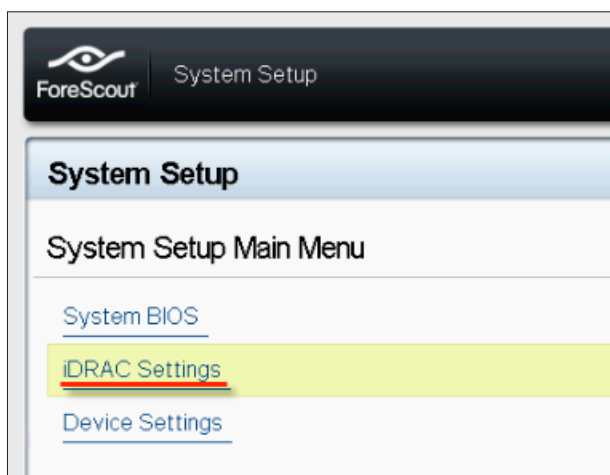
- *Abilitare e configurare il modulo iDRAC*
- *Collegare il modulo alla rete*
- *Accedere a iDRAC*

Abilitazione e configurazione del modulo iDRAC

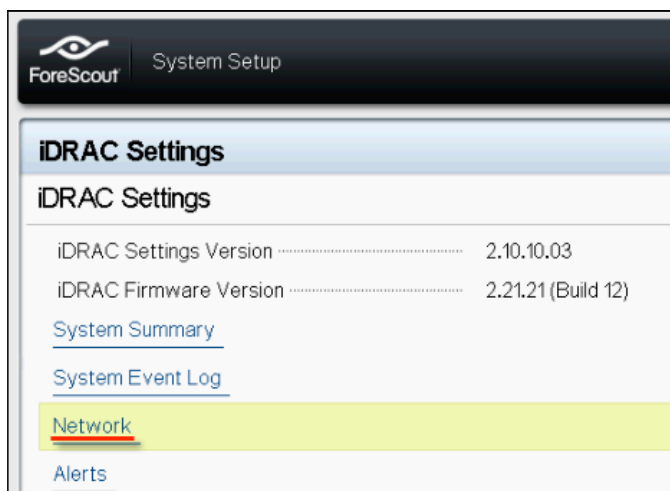
Modificare le impostazioni iDRAC per abilitare l'accesso remoto sul dispositivo CounterACT. Questa sezione descrive le impostazioni di integrazione di base richieste per l'utilizzo di CounterACT.

Per configurare iDRAC:

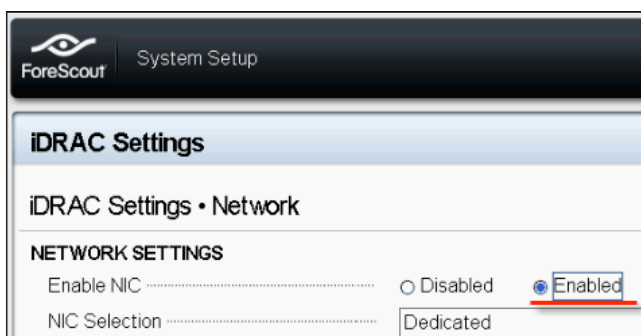
1. Accendere il sistema gestito.
2. Selezionare F2 durante il Power-on Self-test (POST).
3. Nella pagina System Setup Main Menu (Menu principale Configurazione sistema), selezionare **iDRAC Settings**.



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



5. Configurare le seguenti impostazioni di rete:
- **Network Settings (Impostazioni di rete).** Verificare che il campo **Enable NIC** sia impostato su **Enabled**.



- **Common Settings (Impostazioni comuni).** Nel campo DNS DRAC Name (Nome DRAC DNS), è possibile aggiornare un DNS dinamico (opzionale).

- **IPv4 Settings (Impostazioni IPv4).** Verificare che il campo **Enable IPv4** sia impostato su **Enabled**. Impostare il campo **Enable DHCP** su **Enabled** per utilizzare l'indirizzamento IP dinamico o su **Disabled** (Disabilitato) per utilizzare l'indirizzamento IP statico. Se abilitato, DHCP assegnerà automaticamente l'indirizzo IP, il gateway e la subnet mask a iDRAC. Se disabilitato, immettere i valori per i campi **Static IP Address**, **Static Gateway** e **Static Subnet Mask** (Subnet mask statica).

ForeScout System Setup

iDRAC Settings

iDRAC Settings • Network

IPv4 SETTINGS

Enable IPv4	<input type="radio"/> Disabled	<input checked="" type="radio"/> Enabled
Enable DHCP	<input checked="" type="radio"/> Disabled	<input type="radio"/> Enabled
Static IP Address	192.168.1.103	
Static Gateway	192.168.1.1	
Static Subnet Mask	255.255.255.0	
Use DHCP to obtain DNS server addresses	<input checked="" type="radio"/> Disabled	<input type="radio"/> Enabled
Static Preferred DNS Server	192.168.1.2	
Static Alternate DNS Server	0.0.0.0	

6. Selezionare **Back**.
7. Selezionare **User Configuration**.
8. Configurare i seguenti campi relativi alla configurazione utente:
 - **Enable User (Abilita utente).** Verificare che questo campo sia impostato su Enabled (Abilitato).
 - **User Name (Nome utente).** Immettere un nome utente.
 - **LAN and Serial Port User Privileges (Privilegi utente LAN e porta seriale).** Impostare i privilegi sul livello amministratore.
 - **Change Password (Modifica password).** Impostare una password per l'accesso dell'utente.

ForeScout System Setup Help | About | E

iDRAC Settings

iDRAC Settings • User Configuration

User ID	2
Enable User	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
User Name	root
LAN User Privilege	Administrator
Serial Port User Privilege	Administrator
Change Password	

9. Selezionare **Back** (Indietro) e quindi **Finish**. Confermare le impostazioni modificate. Le impostazioni di rete vengono salvate e il sistema riavviato.

Collegamento del modulo alla rete

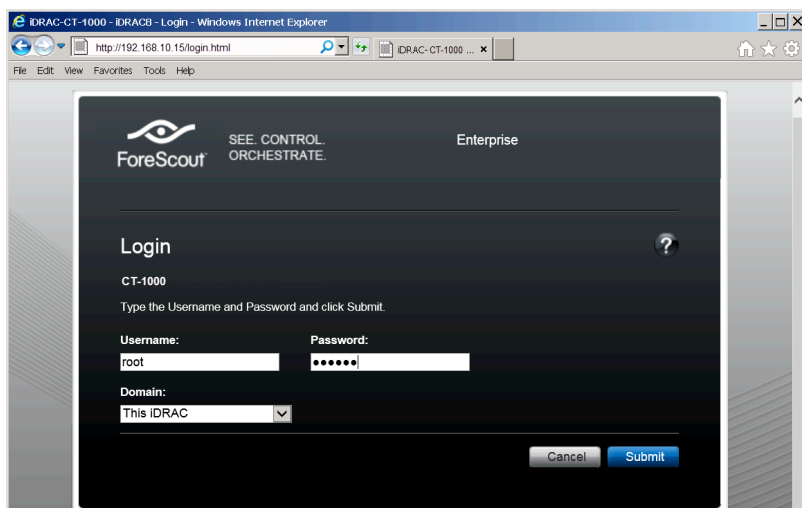
Il modulo iDRAC si connette a una rete Ethernet. Normalmente viene collegato a una rete di gestione. La figura seguente mostra la posizione della porta iDRAC sul pannello posteriore dell'Appliance CT-1000:



Accesso a iDRAC

Per accedere al modulo iDRAC:

1. Accedere all'indirizzo IP o al dominio configurato in **iDRAC Settings > Network**.



2. Immettere il nome utente e la password impostati nella pagina User Configuration (Configurazione utente) della configurazione del sistema iDRAC.
3. Selezionare **Submit**.

Per ulteriori informazioni su iDRAC, consultare la [Guida dell'utente di iDRAC](#).

È fondamentale aggiornare le credenziali predefinite.

6. Verifica della connettività

Verifica della connessione dell'interfaccia di gestione

Per verificare 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 delle
informazioni gateway predefinite)
Ping statistics (Statistiche ping)
Performing Name Resolution Test (Esecuzione
verifica risoluzione nome)
Test summary (Riepilogo verifiche)
```

Verifica della connettività dello switch/Appliance

Verificare che lo switch sia correttamente collegato all'Appliance prima di uscire dal centro dati. A questo scopo, eseguire il comando `fstool ifcount` sull'Appliance per ogni interfaccia rilevata.

```
fstool ifcount eth0 eth1 eth2
```

(Separare ogni interfaccia con uno spazio.)

Questo strumento visualizza in continuo il traffico di rete sulle interfacce specificate. Funziona in due modalità: per interfaccia o per VLAN. La modalità può essere cambiata dal display. Vengono mostrati i bit totali per secondo e la percentuale di ciascuna delle seguenti categorie di traffico:

- L'interfaccia di monitoraggio deve vedere in primo luogo il traffico soggetto a mirroring — oltre il 90%.
- L'interfaccia di risposta deve vedere in primo luogo il traffico trasmesso.
- Le interfacce di monitoraggio e di risposta devono vedere le VLAN attese.

Opzioni di comando:

```
v - display in VLAN mode (visualizza in modalità
VLAN)
I - display in interface mode (visualizza in
modalità interfaccia)
P - show previous (mostra precedente)
N - show next (mostra successivo)
q - quit displaying (esci da visualizzazione)
```

Modalità VLAN:

```
update=[4] [eth3: 14 vlans] (aggiorna=[4] [eth3: 14 vlan])
Interface/Vlan      Total Broadcast Mirrored *To my MAC *From my MAC
(Interfaccia/Vlan Totale Trasmesso Mirroring *A mio MAC *Da mio MAC)
eth3.untagged (senza tag) 4Mbps    0.2%    99.8%    0.0%    0.0%
eth3.1              9Mbps    0.0%    100.0%   0.0%    0.0%
eth3.2              3Mbps    0.1%    99.9%    0.0%    0.0%
eth3.4              542bps   100.0%   0.0%     0.0%    0.0%
eth3.20             1Kbps    100.0%   0.0%     0.0%    0.0%
Show [v]lans [i]nterfaces <-[p]rev [n]ext-> [q]uit
(Mostra vlan interfacce <-prec succ-> esci)
```

Modalità interfaccia:

```
update=[31] [eth0: 32 vlans] [eth1: 1 vlans]
(aggiorna=[31] [eth0: 32 vlan] [eth1: 1 vlan])
Interface          Total Broadcast Mirrored *To my MAC *From my MAC
(Interfaccia Totale Trasmesso Mirroring *A mio MAC *Da mio MAC)
eth0               3Kbps    42.3%    0.0%    14.1%    43.7%
eth1               475bps   0.0%    100.0%   0.0%     0.0%
```

*To my MAC (*A mio MAC)— Il MAC di destinazione è il MAC dell'Appliance..

*From my MAC (*Da mio MAC)— Traffico inviato da questa Appliance (il MAC di origine è il MAC dell'Appliance. La destinazione può essere broadcast o unicast).

Se non si visualizza alcun traffico, verificare che l'interfaccia sia funzionante. Utilizzare il seguente comando sull'Appliance:

```
ifconfig [interface name] up
```

Esecuzione della verifica ping

Eseguire una verifica ping dall'Appliance a un desktop della rete per verificare la connettività.

Per eseguire la verifica:

1. Accedere all'Appliance.
2. Eseguire il seguente comando: **Ping [IP desktop rete]**
Per impostazione predefinita, l'Appliance stessa non risponde al ping.

7. Configurazione della Console CounterACT

Installazione della Console CounterACT

La Console CounterACT è un'applicazione di gestione centrale utilizzata per visualizzare, tenere traccia e analizzare l'attività rilevata dall'Appliance. Dalla Console è possibile definire le policy relative al controllo degli accessi, alla protezione dalle minacce, al firewall e così via. Per ulteriori informazioni consultare il *Manuale utente della Console CounterACT*.

È necessario fornire un computer su cui ospitare l'applicazione Console CounterACT. Di seguito sono elencati i requisiti minimi per l'hardware:

- Computer non dedicato, con sistema operativo:
 - Windows XP, Windows Vista o Windows 7
 - Windows Server 2003 o Server 2008
 - Linux
- Pentium 3, 1 GHz
- 2 GB di memoria
- 1 GB di spazio su disco

Per eseguire l'installazione della Console sono disponibili due metodi:

Utilizzo del software di installazione integrato nell'Appliance.

1. Aprire una finestra del browser dal computer della Console.
2. Immettere la stringa seguente nella barra degli indirizzi del browser:
<http://<Appliance ip>/install>
dove <Appliance ip> è l'indirizzo IP di questa Appliance. Il browser visualizza la finestra di installazione della Console.
3. Seguire le istruzioni visualizzate sullo schermo.

Installazione dal CD-ROM di CounterACT

1. Inserire il CD ROM di CounterACT nell'unità DVD.
2. Aprire il file **ManagementSetup.htm** dal CD ROM con un browser.
3. Seguire le istruzioni visualizzate sullo schermo.

Accesso

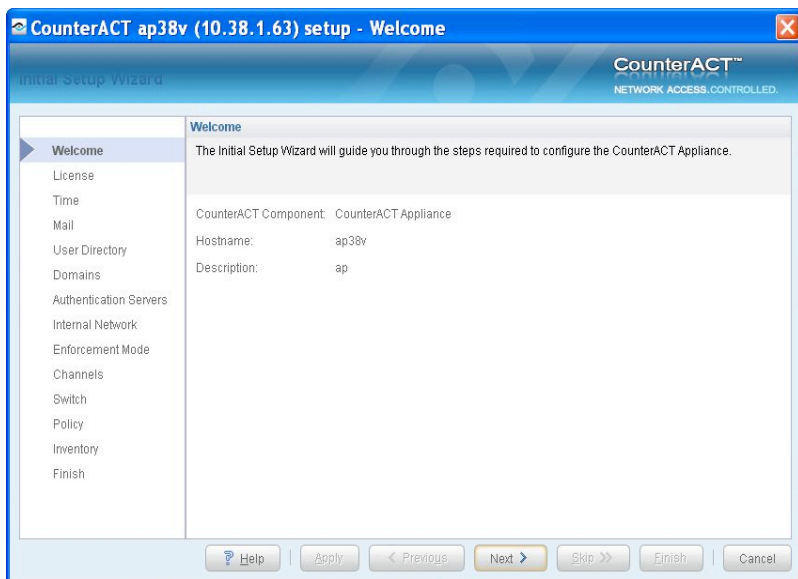
Dopo aver completato l'installazione è possibile effettuare l'accesso alla Console CounterACT.

1. Selezionare l'icona CounterACT dal collegamento rapido creato.
2. Inserire l'indirizzo IP o il nome host dell'Appliance nel campo **IP/Name** (IP/Nome).
3. Nel campo **User Name** (Nome utente), immettere **admin**.
4. Nel campo **Password**, immettere la password creata durante l'installazione dell'Appliance.
5. Selezionare **Login** (Accedi) per avviare la Console.



Esecuzione della configurazione iniziale

Dopo il primo accesso, viene visualizzata la Procedura guidata di configurazione iniziale, che guida l'utente attraverso le fasi essenziali della configurazione per fare sì che CounterACT sia impostato e funzionante con rapidità ed efficienza.



Prima di avviare la configurazione iniziale

Prima di utilizzare la procedura guidata, preparare le seguenti informazioni.

Informazione	Valori
<input type="checkbox"/> Indirizzo server NTP utilizzato dall'organizzazione (facoltativo).	
<input type="checkbox"/> Indirizzo IP inoltro posta interna. Ciò consente la consegna delle e-mail da CounterACT se non è consentito il traffico SMTP dall'Appliance (facoltativo).	
<input type="checkbox"/> Indirizzo e-mail amministratore CounterACT.	
<input type="checkbox"/> Assegnazioni interfacce di monitoraggio e risposta definite nel Centro dati.	
<input type="checkbox"/> Per i segmenti o le VLAN senza DHCP, il segmento di rete o le VLAN ai quali è collegata direttamente l'interfaccia di monitoraggio e un indirizzo IP permanente che CounterACT deve utilizzare in ciascuna di queste VLAN. Questa informazione non è necessaria per la configurazione di Enterprise Manager.	
<input type="checkbox"/> Intervalli indirizzi IP che l'Appliance proteggerà (tutti gli indirizzi interni, anche quelli inutilizzati).	
<input type="checkbox"/> Informazioni account directory utente e indirizzo IP server directory utente.	
<input type="checkbox"/> Credenziali di dominio, inclusi nome utente e password dell'amministratore del dominio.	
<input type="checkbox"/> Server di autenticazione in modo che CounterACT possa analizzare quali host di rete sono stati autenticati correttamente.	
<input type="checkbox"/> Indirizzo IP switch core, parametri fornitore e SNMP.	

Per informazioni sull'utilizzo della procedura guidata, consultare il *Manuale utente della Console CounterACT* o la Guida in linea.

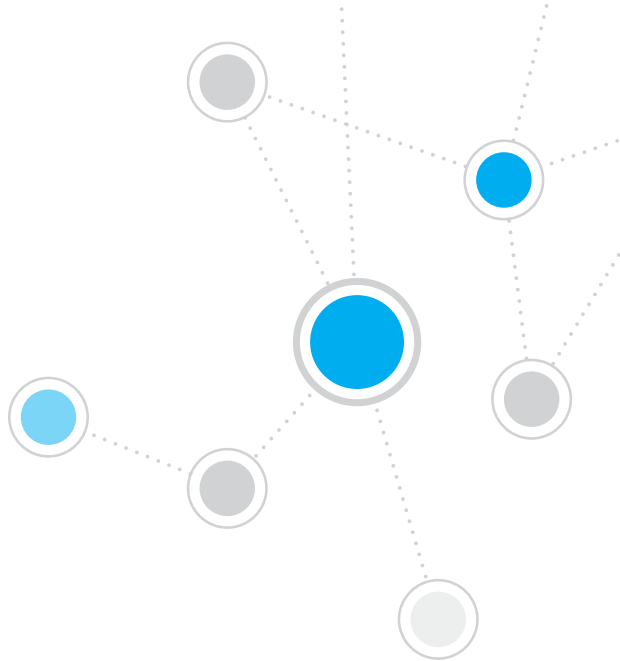
Informazioni di contatto

Per l'assistenza tecnica ForeScout, scrivere a support@forescout.com o chiamare:

- Numero verde (Stati Uniti): 1.866.377.8771
- Telefono (internazionale): 1.408.213.3191
- Assistenza: 1.708.237.6591
- Fax: 1.408.371.2284

©2016 ForeScout Technologies, Inc. Prodotti protetti dai brevetti USA n. 6.363.489, n. 8.254.286, n. 8.590.004 e n. 8.639.800. Tutti i diritti riservati. ForeScout Technologies e il logo ForeScout sono marchi commerciali di ForeScout Technologies, Inc. Tutti gli altri marchi commerciali appartengono ai rispettivi titolari.

L'utilizzo di qualsiasi prodotto ForeScout è soggetto ai termini del Contratto di licenza per l'utente finale ForeScout disponibile su www.forescout.com/eula.



ForeScout®

ForeScout Technologies, Inc.
900 E. Hamilton Avenue #300
Campbell, CA 95008 USA

Numero verde (Stati Uniti): 1.866.377.8771

Telefono (internazionale): 1.408.213.3191

Assistenza: 1.708.237.6591

Fax: 1.408.371.2284

400-00020-01