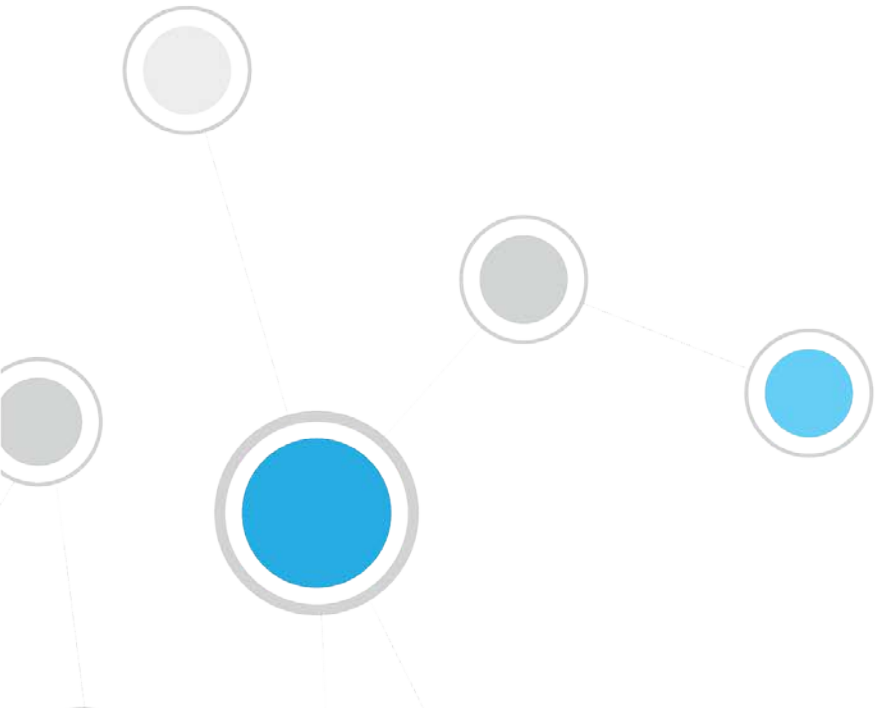
ForeScout CounterACT®

Einzelne CounterACT-Appliance

Kurzanleitung für die Installation

Version 8.0



Inhaltsverzeichnis

Willkommen zu CounterACT Version 8.0

Die CounterACT-Plattform bietet Infrastruktur- und Gerätetransparenz, Richtlinienmanagement, Orchestrierung und Workflow-Rationalisierung, um die Netzwerksicherheit zu erhöhen. CounterACT versorgt Unternehmen mit Echtzeit-Kontextinformationen über Geräte und Benutzer im Netzwerk. Richtlinien werden in CounterACT unter Verwendung dieser Kontextinformationen definiert, die dazu beitragen, die Einhaltung der Richtlinien, die Behebung von Problemen, den angemessenen Netzwerkzugriff und die Rationalisierung des Servicebetriebs zu gewährleisten.

In diesem Handbuch wird die Installation einer einzelnen, eigenständigen CounterACT-Appliance erläutert.

Nähere Einzelheiten oder Informationen zur Bereitstellung mehrerer Appliances für unternehmensweiten Netzwerkschutz erhalten Sie im *CounterACT Installation Guide (CounterACT-Installationshandbuch)* und dem *CounterACT Administration Guide (CounterACT-Administrationshandbuch).* Siehe Zusätzliche CounterACT-Dokumentation für Informationen über den Zugang zu diesen Handbüchern.

Darüber hinaus haben Sie über die Support-Website unter: http://www.forescout.com/support Zugriff auf die neusten Dokumentationen, Artikel in der Wissensdatenbank und Aktualisierungen für Ihre Appliance.

Lieferumfang Ihres CounterACT-Pakets

Ihr CounterACT-Paket enthält die folgenden Komponenten:

- Die CounterACT-Appliance
- Frontrahmen
- Schienen-Bausatz (Montagehalterungen)
- Netzkabel
- Anschlusskabel für die DB9-Konsole (nur für seriellen Anschluss)
- Sicherheits-, Umwelt- und Regulierungsinformationen für Unternehmensprodukte
- Dokument „Erste Schritte“ (nur für 51xx Geräte)

Übersicht

Zum Einrichten von CounterACT sind die folgenden Schritte erforderlich:

1. Erstellen eines Bereitstellungsplans

Vor der Installation sollten Sie überlegen, wo die Appliance bereitgestellt werden soll. Zudem sollten Sie sich mit den Anschlüssen an der Appliance-Schnittstelle vertraut machen.

Auswählen des Bereitstellungsorts für die Appliance

Die Auswahl des richtigen Netzwerkstandorts für die Installation der Appliance ist von entscheidender Bedeutung für eine erfolgreiche Bereitstellung und eine optimale Leistung von CounterACT. Der geeignete Standort ist abhängig von Ihren jeweiligen Implementierungszielen und den gewünschten Netzwerkzugriffsrichtlinien. Die Appliance sollte in der Lage sein, den Datenverkehr zu überwachen, der für die gewünschte Richtlinie relevant ist. Wenn Ihre Richtlinie beispielsweise auf einer Überwachung der Autorisierungsereignisse zwischen den Endpunkten und den Authentifizierungsservern des Unternehmens beruht, muss die Appliance so installiert werden, dass sie auf den Datenverkehr zwischen Endpunkten und Authentifizierungsserver(n) zugreifen kann.

Weitere Informationen zu Installation und Bereitstellung erhalten Sie im *CounterACT Installation Guide (CounterACT-Installationshandbuch)*. Siehe Zusätzliche CounterACT-Dokumentation für Informationen über den Zugang zu diesem Handbuch.

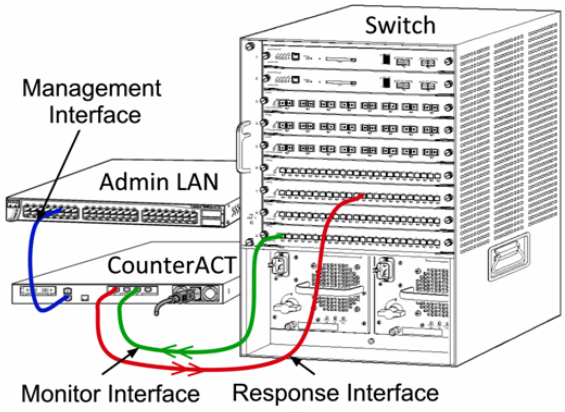
Verbindungen der Appliance-Schnittstelle

Die Appliance verfügt im Allgemeinen über drei Verbindungen zum Netzwerkswitch.

Verwaltungsschnittstelle

Über die Verwaltungsschnittstelle können Sie CounterACT verwalten sowie Anfragen und weitreichende Überprüfungen der Endpunkte durchführen. Die Schnittstelle muss mit einem Switchport verbunden sein, der Zugriff auf alle Endpunkte im Netzwerk ermöglicht.

Jede Appliance benötigt eine eigene Verwaltungsverbindung zum Netzwerk. Für diese Verbindung sind eine IP-Adresse im lokalen LAN sowie der Zugriff auf den TCP-Port 13000 von den Computern aus erforderlich, auf denen die CounterACT Console-Verwaltungsanwendung ausgeführt wird. Der Verwaltungsport muss auf die folgenden Komponenten Ihres Netzwerks zugreifen können.



Netzwerkzugriffsanforderungen

Port	Service	Von oder zu CounterACT	Funktion
22/TCP	SSH	Von	Ermöglicht die Remote-Inspektion von OS X- und Linux-Endpunkten. Ermöglicht CounterACT die Kommunikation mit Netzwerk-Switches und Routern.
		Zu	Ermöglicht Zugriff auf die CounterACT-Befehlszeilenschnittstelle.
2222/TCP	SSH	Zu	(Hochverfügbarkeit) Ermöglicht den Zugriff auf physische CounterACT-Geräte, die zum Hochverfügbarkeitscluster gehören. Verwenden Sie den TCP-Port 22, um auf die gemeinsame (virtuelle) IP-Adresse des Paares zuzugreifen.
25/TCP	SMTP	Von	Ermöglicht CounterACT den Zugriff auf das unternehmenseigene Mail-Relay.
53/UDP	DNS	Von	Ermöglicht CounterACT die Auflösung interner IP-Adressen.
80/TCP	HTTP	Zu	Ermöglicht HTTP-Umleitungen.
123/UDP	NTP	Von	Ermöglicht CounterACT den Zugriff auf einen lokalen Zeitserver oder ntp.forescout.net. CounterACT verwendet standardmäßig ntp.foreScout.net
135/TCP	MS-WMI	Von	Ermöglicht die entfernte Überprüfung von Windows-Endpunkten.
139/TCP	SMB, MS-RPC	Von	Ermöglicht die entfernte Überprüfung von Windows-Endpunkten (Für Endpunkte unter Windows 7 und älter).

Port	Service	Von oder zu CounterACT	Funktion
445/TCP			Ermöglicht die entfernte Überprüfung von Windows-Endpunkten.
161/UDP	SNMP	Von	Ermöglicht CounterACT die Kommunikation mit Netzwerk-Switches und Routern. Weitere Informationen zur Konfiguration von SNMP erhalten Sie im *CounterACT Administration Guide (CounterACT Administrationshandbuch)*.
162/UDP	SNMP	Zu	Ermöglicht CounterACT den Empfang von SNMP-Traps von Netzwerk-Switches und Routern. Weitere Informationen zur Konfiguration von SNMP erhalten Sie im *CounterACT Administration Guide (CounterACT Administrationshandbuch)*.
389/TCP (636)	LDAP	Von	Ermöglicht CounterACT die Kommunikation mit Active Directory. Ermöglicht die Kommunikation mit CounterACT webbasierten Portalen.
443/TCP	HTTPS	Zu	Ermöglicht HTTP-Umleitungen über TLS.
2200/TCP	SecureConnector für Linux	Zu	Ermöglicht SecureConnector die Herstellung einer sicheren (verschlüsselten SSH) Verbindung zur Appliance von Linux-Computern aus. *SecureConnector* ist ein skriptbasierter Agent, der die Verwaltung von Linux-Endpunkten ermöglicht, solange diese mit dem Netzwerk verbunden sind.

Port	Service	Von oder zu CounterACT	Funktion
10003/TCP	SecureConnector für Windows	Zu	Ermöglicht SecureConnector die Herstellung einer sicheren (verschlüsselten TLS) Verbindung zur Appliance von Windows-Computern aus. *SecureConnector* ist ein skriptbasierter Agent, der die Verwaltung von Windows-Endpunkten ermöglicht, solange diese mit dem Netzwerk verbunden sind. Weitere Informationen über SecureConnector erhalten Sie im *CounterACT Administration Guide (CounterACT Administrationshandbuch)*. Wenn SecureConnector eine Verbindung mit einer Appliance oder mit dem Enterprise Manager herstellt, wird er zu der Appliance umgeleitet, zu der sein Host zugeordnet ist. Um transparente Mobilität innerhalb Ihrer Organisation zu ermöglichen, achten Sie darauf, dass dieser Port für alle Appliances und Enterprise Manager offen ist.
10005/TCP	SecureConnector für OS X	Zu	Ermöglicht SecureConnector die Herstellung einer sicheren (verschlüsselten TLS) Verbindung zur Appliance von OS X-Computern aus. *SecureConnector* ist ein skriptbasierter Agent, der die Verwaltung von OS X-Endpunkten ermöglicht, solange diese mit dem Netzwerk verbunden sind. Weitere Informationen über SecureConnector erhalten Sie im *CounterACT Administration Guide (CounterACT Administrationshandbuch)*. Wenn SecureConnector eine Verbindung mit einer Appliance oder mit dem Enterprise Manager herstellt, wird er zu der Appliance umgeleitet, zu der sein Host zugeordnet ist. Um transparente Mobilität innerhalb Ihrer Organisation zu ermöglichen, achten Sie darauf, dass dieser Port für alle Appliances und Enterprise Manager offen ist.

Port	Service	Von oder zu CounterACT	Funktion
13000/TCP	CounterACT	Von/Zu	Für Umgebungen mit nur einer Appliance - von der Konsole bis zur Appliance. Für Umgebungen mit mehr als einem CounterACT Gerät – von der Konsole zum CounterACT Gerät und von einem CounterACT Gerät zum anderen. Die CounterACT Gerätekommunikation umfasst die Kommunikation mit dem Enterprise Manager und dem Recovery Enterprise Manager über TLS.

Überwachungsschnittstelle

Die Überwachungsschnittstelle ermöglicht die Überwachung und Nachverfolgung des Netzwerkdatenverkehrs durch die Appliance. Als Überwachungsschnittstelle kann jede verfügbare Schnittstelle verwendet werden.

Der Datenverkehr wird zu einem Port am Switch gespiegelt und von der Appliance überwacht. Je nach Anzahl der zu spiegelnden VLANs wird für den Datenverkehr VLAN-Tagging gemäß 802.1Q genutzt.

- ***Einzelnes VLAN***: Wenn der überwachte Datenverkehr von einem einzelnen VLAN stammt, ist für den gespiegelten Datenverkehr kein VLAN-Tagging erforderlich.
- ***Mehrere VLANs***: Wenn der überwachte Datenverkehr von mehr als einem VLAN stammt, muss für den gespiegelten Datenverkehr VLAN-Tagging gemäß 802.1Q verwendet werden.

Wenn zwei Switches als redundantes Paar miteinander verbunden sind, muss die Appliance den Datenverkehr von beiden Switches überwachen.

Die Überwachungsschnittstelle erfordert keine IP-Adresse.

Antwortschnittstelle

Über diese Schnittstelle beantwortet die Appliance den Datenverkehr. Der Antwortdatenverkehr dient dem Schutz vor schädlichen Aktivitäten und zur Durchführung von Aktionen im Rahmen der Richtlinie. Zu diesen Aktionen gehören beispielsweise die Umleitung von Webbrowsern oder die Blockierung einer Session. Die damit verbundene Konfiguration des Switchports ist abhängig vom zu überwachenden Datenverkehr.

Als Antwortschnittstelle kann jede verfügbare Schnittstelle verwendet werden.

- ***Einzelnes VLAN***: Wenn der überwachte Datenverkehr von einem einzelnen VLAN stammt, muss die Antwortschnittstelle so konfiguriert werden, dass sie zum selben VLAN gehört. In diesem Fall benötigt die Appliance eine einzige IP-Adresse in diesem VLAN.

- ***Mehrere VLANs***: Wenn der überwachte Datenverkehr von mehr als einem VLAN stammt, muss für die entsprechenden VLANs auf der Antwortschnittstelle VLAN-Tagging gemäß 802.1Q aktiviert werden. Die Appliance benötigt dann eine IP-Adresse für jedes geschützte VLAN.

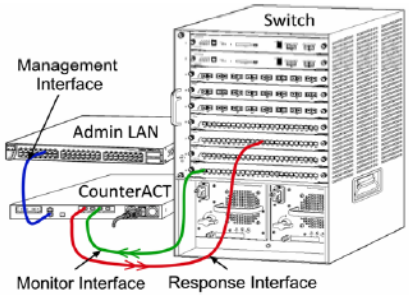
2. Einrichten Ihres Switches

A. Verbindungsoptionen für den Switch

Die Appliance wurde so entwickelt, dass sie nahtlos in eine Vielzahl von Netzwerkumgebungen integriert werden kann. Für eine erfolgreiche Integration der Appliance in Ihrem Netzwerk müssen Sie sicherstellen, dass Ihr Switch für die Überwachung des benötigten Datenverkehrs entsprechend eingerichtet ist.

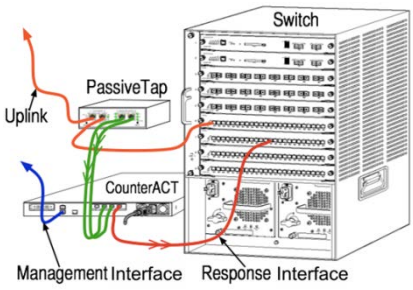
Ihnen stehen verschiedene Optionen zur Verfügung, um eine Verbindung zwischen Appliance und Switch herzustellen.

1 Standardbereitstellung (separate Schnittstellen für Verwaltung, Überwachung und Antwort)



Bei der empfohlenen Bereitstellungsart werden drei separate Ports verwendet. Diese Ports werden in Verbindungen der Appliance-Schnittstelle beschrieben.

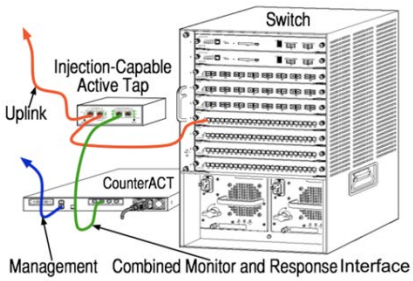
2 Passiver Inline-Tap



Statt die Verbindung zu einem Überwachungsport am Switch herzustellen, kann die Appliance auch einen passiven Inline-Tap verwenden.

Ein passiver Tap erfordert zwei Überwachungsports (einen für Upstream-Verkehr und einen für Downstream-Verkehr), es sei denn, es werden *Rekombinations*-Taps verwendet, welche die beiden Duplex-Streams zu einem einzelnen Port kombinieren. Beachten Sie, dass, wenn der Datenverkehr an dem angeschlossenen Port 802.1Q VLAN-getaggt ist, der Antwortport auch 802.1Q VLAN-getaggt sein muss.

3 Aktiver (für Einspritzung geeigneter) Inline-Tap



Die Appliance kann einen aktiven Inline-Tap verwenden. Wenn der Tap injektionsfähig ist, kombiniert die Appliance Überwachungs- und Antwort-Ports, so dass es nicht erforderlich ist, einen separaten Antwort-Port am Switch zu konfigurieren. Diese Option kann für jede Art von Upstream- oder Downstream-Switchkonfiguration verwendet werden.

4 Antwort über IP-Layer (für Installationen mit Layer-3-Switches)

Die Appliance kann ihre eigene Verwaltungsschnittstelle für die Beantwortung des Datenverkehrs nutzen. Obwohl diese Option für jeden überwachten Datenverkehr geeignet ist, wird sie für Situationen empfohlen, in denen die Überwachungsports der Appliance zu keinem VLAN gehören und die Appliance deshalb nicht über einen beliebigen anderen Switchport auf den überwachten Datenverkehr antworten kann. Dies ist in der Regel der Fall, wenn ein Link zwischen zwei Routern überwacht wird. Diese Option kann keine Anfragen über das Address Resolution Protocol (ARP) beantworten, sodass die Fähigkeit der Appliance zur Erkennung von Scanvorgängen, die auf IP-Adressen im überwachten Subnetz abzielen, eingeschränkt ist. Diese Einschränkung entfällt, wenn der Datenverkehr zwischen zwei Routern überwacht wird.

B. Hinweise zur Switcheinstellung

VLAN (802.1Q) Tags

- ***Überwachung eines einzelnen VLAN***: Wenn der überwachte Datenverkehr aus nur einem einzigen VLAN stammt, ist kein VLAN-Tagging gemäß 802.1Q erforderlich.
- ***Überwachung mehrerer VLANs***: Wenn der überwachte Datenverkehr aus zwei oder mehr VLANs stammt, muss *sowohl* für die Überwachungs- als auch die Antwortschnittstelle VLAN-Tagging gemäß 802.1Q aktiviert werden. Die Option für die Überwachung mehrerer VLANs wird empfohlen, da sie die beste Abdeckung gewährleistet und gleichzeitig die Anzahl der zur Spiegelung erforderlichen Ports minimiert wird.
- Wenn der Switch kein VLAN-Tagging gemäß 802.1Q an den zur Spiegelung verwendeten Ports nutzen kann, wählen Sie eine der folgenden Möglichkeiten:
  - Spiegeln eines einzigen VLAN
  - Spiegeln eines einzelnen, ungetaggten Uplink-Ports
  - Verwenden der Option für Antwort über IP-Layer
- Wenn der Switch nur einen Port spiegeln kann, nutzen Sie für die Spiegelung einen einzigen Uplink-Port. Dieser kann getaggt werden. Wenn der Switch die VLAN-Tags gemäß 802.1Q entfernt, müssen Sie im Allgemeinen die Option zur Antwort über den IP-Layer verwenden.

Weitere Richtlinien

- In den folgenden Fällen sollten Sie nur eine Schnittstelle spiegeln (die das Senden/Empfangen ermöglicht):
  - Wenn der Switch nicht den eingehenden und den ausgehenden Datenverkehr spiegeln kann
  - Wenn der Switch nicht den gesamten Switch-Datenverkehr spiegeln kann
  - Wenn der Switch nicht den gesamten Datenverkehr über ein VLAN spiegeln kann

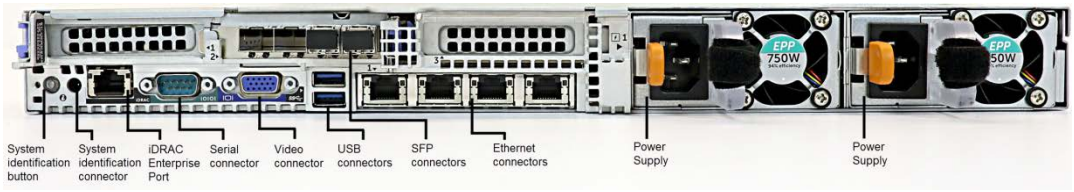
- Vergewissern Sie sich, dass Sie den zur Spiegelung verwendeten Port nicht überlasten.
- Bei einigen Switches (z. B. Cisco 6509) muss möglicherweise zunächst die vorherige Portkonfiguration vollständig gelöscht werden, bevor neue Einstellungen vorgenommen werden können. In vielen Fällen entfernt der Switch die 802.1Q-Tags, wenn die alten Portinformationen nicht gelöscht werden.

3. Anschließen der Netzwerkkabel und Einschalten

A. Auspacken der Appliance und Anschließen der Kabel

1. Nehmen Sie die Appliance und das Netzkabel aus der Verpackung
2. Entfernen Sie den im Lieferumfang der Appliance enthaltenen Schienen-Bausatz.
3. Montieren Sie den Schienen-Bausatz an der Appliance und die Appliance im Rack.
4. Verbinden Sie die Netzwerkschnittstellen auf der Rückseite der Appliance über Netzwerkkabel mit den Switchports.

Beispiele der Rückseite – CounterACT-Gerät



Sie können die von ForeScout gelieferten SFPs durch Finisar SFPs ersetzen, die von ForeScout geprüft und freigegeben wurden. Weitere Informationen erhalten Sie im *CounterACT Installation Guide (CounterACT-Installationshandbuch)*.

B. Notieren der Schnittstellenzuweisungen

Nachdem Sie die Installation der Appliance im Rechenzentrum abgeschlossen und CounterACT Console installiert haben, werden Sie aufgefordert, die Schnittstellenzuweisungen anzugeben. Diese als *Kanaldefinitionen* bezeichneten Zuweisungen werden mit Hilfe des Assistenten für die Anfangseinstellungen (Initial Setup Wizard) eingegeben, der beim erstmaligen Anmelden bei Console geöffnet wird.

Notieren Sie sich in der folgenden Tabelle die Schnittstellenzuweisungen, um sie beim Durchführen der Kanalkonfiguration in der Console schnell nachschlagen zu können.

Ethernet-Schnittstelle	Schnittstellenzuweisung (z. B. Verwaltung, Überwachung, Antwort)
Eth0	
Eth1	

Eth2	
Eth3	
Eth4	
Eth5	
Eth6	
Eth7	

C. Einschalten der Appliance

1. Verbinden Sie das Netzkabel mit dem Netzanschluss auf der Rückseite der Appliance.
2. Schließen Sie das andere Ende des Kabels an eine geerdete Wechselstromsteckdose an.
3. Schließen Sie dann entweder eine Tastatur und einen Monitor an die Appliance an, oder konfigurieren Sie die Appliance für eine serielle Verbindung. Weitere Informationen erhalten Sie im *CounterACT Installation Guide (CounterACT-Installationshandbuch)*.
4. Schalten Sie die Appliance auf der Vorderseite ein.

4. Konfigurieren der Appliance

Halten Sie die folgenden Informationen bereit, wenn Sie mit der Konfiguration der Appliance beginnen.

Hostname der Appliance	
CounterACT-Administratorkennwort	Bewahren Sie das Kennwort an einem sicheren Ort auf
Verwaltungsschnittstelle	
IP-Adresse der Appliance	
Netzwerkmaske	
IP-Adresse des Standard-Gateways	
DNS-Domänenname	
DNS-Serveradressen	

Nach dem Einschalten werden Sie mit folgender Meldung aufgefordert, die Konfiguration durchzuführen:

```
CounterACT Appliance boot is complete (Starten der CounterACT-
Appliance ist abgeschlossen).
Press <Enter> to continue (Drücken Sie zum Fortfahren die
Eingabetaste).
```

1. Drücken Sie **Enter (Eingabetaste)**. Wenn Sie ein 51xx CounterACT-Gerät besitzen, erscheint das folgende Menü:

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

1) Configure CounterACT (CounterACT konfigurieren)
2) Restore saved CounterACT configuration (Gespeicherte
CounterACT-Konfiguration wiederherstellen)
3) Identify and renumber network interfaces
(Netzwerkschnittstellen ermitteln und neu nummerieren)
4) Configure keyboard layout (Tastaturlayout konfigurieren)
5) Turn machine off (Computer ausschalten)
6) Reboot the machine (Computer neu starten)

Choice (1-6) :1
```

   Wenn Sie ein CT-xxxx CounterACT-Gerät besitzen, sehen Sie entweder CounterACT 7.0.0 oder CounterACT 8.0.0 als Version oben im Menü aufgelistet.

- Wenn Sie CounterACT 7.0.0 sehen, können Sie entweder auf die Version 8.0.0 upgraden oder eine Neuinstallation durchführen. Nähere Informationen erhalten Sie im *CounterACT Installation Guide (CounterACT-Installationshandbuch)*. Nach dem Upgrade oder der Installation auf die Version 8.0.0 sehen Sie das oben aufgeführte Menü.
- Wenn Sie CounterACT 8.0.0 sehen, bietet das Menü die Möglichkeit, CounterACT 7.0.0 zu installieren oder CounterACT 8.0.0 zu konfigurieren, wie unten gezeigt. Wenn Sie CounterACT 7.0.0 wählen, können Sie CounterACT 8.0.0 nicht über das Konfigurationsmenü neu installieren. Weitere Informationen zur Konfiguration von CounterACT 7.0.0. finden Sie im *CounterACT Installation Guide version 7.0.0 (CounterACT-Installationshandbuch Version 7.0.0)*.

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


1) Install CounterACT 7.0.0-<build> (CounterACT 7.0.0 Aufbau
installieren)
2) Configure CounterACT 8.0.0-<build> (CounterACT 8.0.0-<build>
konfigurieren)
3) Restore saved CounterACT configuration (Gespeicherte
CounterACT-Konfiguration wiederherstellen)
4) Identify and renumber network interfaces
(Netzwerkschnittstellen ermitteln und neu nummerieren)
5) Configure keyboard layout (Tastaturlayout konfigurieren)
6) Turn machine off (Computer ausschalten)
7) Reboot the machine (Computer neu starten)

Choice (1-7) :
```

Wenn die Konfiguration unterbrochen wird oder wenn Sie die falsche CounterACT-Version gewählt haben, müssen Sie die Appliance mit der entsprechenden Version der ISO-Datei neu abbilden. Nähere Informationen zum Abbilden einer Appliance erhalten Sie im CounterACT Installation Guide (CounterACT-Installationshandbuch).

2. Wählen Sie **Configure CounterACT (CounterACT konfigurieren)**. Auf die Aufforderung hin:

   Continue (Fortfahren): (yes/no) (Ja/Nein)?

   Press **Enter** to continue (Drücken Sie die Eingabetaste, um mit dem Einrichten zu beginnen).

3. Das Menü High Availability Mode (Hochverfügbarkeitsmodus) wird geöffnet. Wählen Sie durch Drücken von **Enter (Eingabetaste)** die Standardinstallation aus.

4. Die Aufforderung CounterACT Initial Setup (CounterACT-Anfangseinstellungen) wird angezeigt. Drücken Sie zum Fortfahren **Enter (Eingabetaste)**.

5. Das Menü Select CounterACT Installation Type (CounterACT-Installationstyp auswählen) wird geöffnet. Geben Sie **1** ein, und drücken Sie dann **Enter (Eingabetaste),** um die Standardinstallation der CounterACT-Appliance durchzuführen.

Die Einstellungen werden initialisiert. Dies kann einige Zeit dauern.

6. Das Menü Select Licensing Mode (Lizenzmodus auswählen) wird geöffnet. Wählen Sie den Lizenzmodus, den Ihre Implementierung verwendet. Der Lizenzmodus wird beim Kauf festgelegt. ***Geben Sie erst dann einen Wert ein, wenn Sie sich vergewissert haben, welchen Lizenzierungsmodus Ihre Implementierung verwendet***. Wenden Sie sich an Ihren ForeScout-Vertreter, um Ihren Lizenzmodus zu überprüfen oder wenn Sie den falschen Modus gewählt haben.

7. Wenn die Aufforderung Enter Machine Description (Computerbeschreibung eingeben) erscheint, geben Sie einen kurzen beschreibenden Text für das Gerät ein, und drücken Sie dann **Enter (Eingabetaste)**.

   Die folgende Meldung wird angezeigt:

```
>>>>>> Set Administrator Password (Administratorkennwort
festlegen)<<<<<<
This password will be used to log in as „root“ to the machine
Operating System and as „admin“ to the CounterACT Console
(Dieses Kennwort wird benötigt, um sich als Root-Benutzer
(„root“) beim Betriebssystem des Computers und als Administrator
(„admin“) bei CounterACT Console anzumelden).
The password must be between 6 and 15 characters long and should
contain at least one non-alphabetic character (Das Kennwort muss
zwischen 6 und 15 Zeichen lang sein und mindestens ein
nichtalphabetisches Zeichen enthalten).
Administrator password (Administratorpasswort):
```

8. Wenn die Aufforderung Set Administrator Password prompt (Administratorpasswort festlegen) erscheint, geben Sie das gewünschte Passwort (die eingegebene Zeichenkette wird auf dem Bildschirm nicht angezeigt) ein, und drücken Sie dann **Enter (Eingabetaste)**. Sie werden aufgefordert, das Passwort zu bestätigen. Das Passwort muss zwischen 6 und 15 Zeichen lang sein und mindestens ein nicht-alphabetisches Zeichen enthalten.

   Melden Sie sich an der Appliance als root *und bei Console als* admin *an.*

9. Wenn die Aufforderung Set Host Name (Hostname festlegen) erscheint, geben Sie den gewünschten Hostnamen ein, und drücken Sie dann **Enter (Eingabetaste)**. Der Hostname kann zur Anmeldung bei Console verwendet werden und wird in Console angezeigt, um Ihnen die Bestimmung der aktuell angezeigten CounterACT-Appliance zu erleichtern. Der Hostname sollte nicht länger als 13 Zeichen sein.

10. Im Fenster Configure Network Settings (Netzwerkeinstellungen konfigurieren) werden Sie aufgefordert, eine Reihe von Konfigurationsparametern einzustellen. Geben Sie für jede Aufforderung einen Wert ein, und drücken Sie **Enter (Eingabetaste)**, um die nächste Aufforderung anzuzeigen.

    – Die Kommunikation zwischen den CounterACT-Komponenten erfolgt über Verwaltungsschnittstellen. Die Anzahl der aufgelisteten Verwaltungsschnittstellen ist abhängig vom jeweiligen Appliance-Modell.

- Die **Management IP address (IP-Adresse für die Verwaltung)** ist die Adresse der Schnittstelle, über die die CounterACT-Komponenten miteinander kommunizieren. Geben Sie für diese Schnittstelle nur dann eine VLAN-ID ein, wenn die für die Kommunikation der CounterACT-Komponenten verwendete Schnittstelle mit einem getaggten Port verbunden ist.
- Wenn unter **DNS server address (DNS-Serveradresse)** mehr als eine Adresse eingegeben werden muss, verwenden Sie jeweils ein Leerzeichen als Trennzeichen. Die meisten internen DNS-Server lösen externe und interne Adressen auf, jedoch müssen Sie möglicherweise einen DNS-Server zum Auflösen externer Adressen hinzufügen. Da sich fast alle DNS-Anfragen der Appliance auf interne Adressen beziehen, sollte der DNS-Server für externe Adressen zuletzt eingegeben werden.

11. Das Fenster Setup Summary (Zusammenfassung der Einrichtung) wird angezeigt. Sie werden aufgefordert, entweder allgemeine Konnektivitätstests durchzuführen, Einstellungen neu zu konfigurieren oder das Einrichten abzuschließen. Geben Sie **D** ein, um die Einrichtung abzuschließen.

Lizenz

Stellen Sie nach der Konfiguration sicher, dass Ihr CounterACT-Gerät über eine gültige Lizenz verfügt. Der Standard-Lizenzierungsstatus Ihres CounterACT-Geräts hängt davon ab, welchen Lizenzierungsmodus Sie verwenden.

- Wenn Ihre CounterACT-Implementierung im ***Per-Appliance Licensing Mode (Pro-Appliance Lizenzmodus)*** läuft, können Sie nun mit der Demo-Lizenz arbeiten, die 30 Tage gültig ist. Während dieser Zeit sollten Sie eine permanente Lizenz von ForeScout erhalten und diese in einem zugänglichen Ordner auf Ihrer Festplatte oder Ihrem Netzwerk ablegen. Installieren Sie die Lizenz von diesem Ort aus, bevor die 30-Tage-Demo-Lizenz abläuft (Falls erforderlich, können Sie eine Verlängerung der Demo-Lizenz beantragen).

  Sie werden benachrichtigt, dass Ihre Demo-Lizenz in mehrfacher Hinsicht abläuft. Weitere Informationen über Benachrichtigungen zur Demo-Lizenz erhalten Sie im *CounterACT Administration Guide (CounterACT Administrationshandbuch)*.

  Wenn Sie mit einem virtuellen CounterACT-System arbeiten:

  - Die Demo-Lizenz wird zu diesem Zeitpunkt nicht automatisch installiert. Sie müssen die Demo-Lizenz installieren, die Sie von Ihrem ForeScout-Vertreter per E-Mail erhalten haben.
  - Mindestens ein CounterACT-Gerät muss einen Internetzugang aufweisen. Diese Verbindung wird verwendet, um CounterACT-Lizenzen gegen den ForeScout-Lizenzserver zu validieren. Lizenzen, die einen Monat lang nicht authentifiziert werden können, werden widerrufen. CounterACT sendet einmal täglich eine Warnmeldung per E-Mail, die auf einen Kommunikationsfehler mit dem Server hinweist.

    Weitere Informationen erhalten Sie im *CounterACT Installation Guide (CounterACT-Installationshandbuch)*.

- Wenn Ihre CounterACT-Implementierung im ***Centralized Licensing Mode (zentralisierten Lizenzierungsmodus)*** läuft, sollte der *Entitlement administrator (Berechtigungsadministrator)* eine E-Mail erhalten, wenn die Lizenzrechte erstellt und im ForeScout-Kundenportal verfügbar sind. Sobald diese verfügbar sind, kann der *CounterACT administrator (CounterACT-Administrator)* der Implementierung die Lizenz in CounterACT Console aktivieren. Solange die Lizenz nicht aktiviert ist, funktionieren die CounterACT-Funktionen nicht einwandfrei. So werden zum Beispiel keine Richtlinien evaluiert und keine Aktionen durchgeführt. *Bei der Systeminstallation wird keine Demo-Lizenz automatisch installiert.*

Weitere Informationen zur Lizenzverwaltung erhalten Sie im *CounterACT Administration Guide (CounterACT Administrationshandbuch)*.

5. Remoteverwaltung

iDRAC-Einrichtung

Integrated Dell Remote Access Controller (iDRAC) ist eine integrierte Serversystemlösung, die Ihnen unabhängig von Standort-Betriebssystem via LAN oder Internet den Remotezugriff auf CounterACT-Appliances ermöglicht. Über das Modul erhalten Sie KVM-Zugriff und können Computer ein-/ausschalten/zurücksetzen sowie Aufgaben in Verbindung mit Fehlerbehebung und Wartung durchführen.

Für die Arbeit mit dem iDRAC-Modul sind die folgenden Schritte erforderlich:

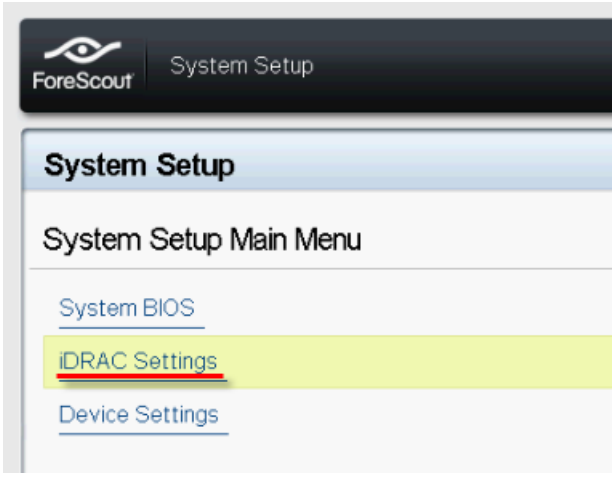
- Aktivieren und Konfigurieren des iDRAC-Moduls
- Herstellen einer Verbindung zwischen Modul und Netzwerk
- Anmelden bei iDRAC

Aktivieren und Konfigurieren des iDRAC-Moduls

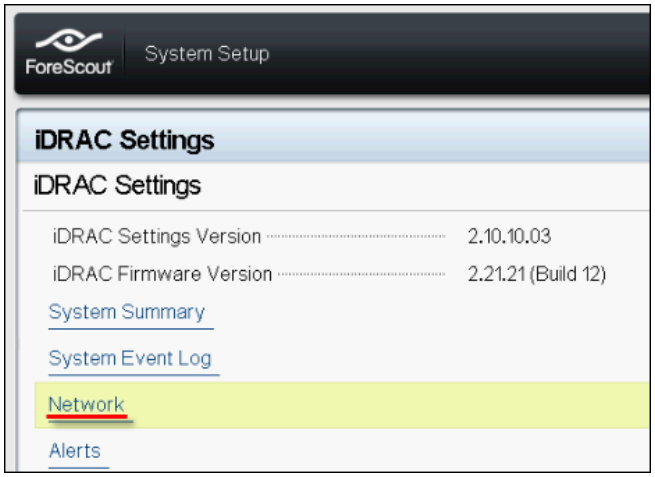
Ändern Sie die iDRAC-Einstellungen so, dass ein Remotezugriff auf das CounterACT-Gerät möglich ist. In diesem Abschnitt werden die grundlegenden Integrationseinstellungen für die Arbeit mit CounterACT beschrieben.

So konfigurieren Sie iDRAC:

1. Aktivieren Sie die verwaltete Appliance.
2. Drücken Sie während des Boot-Vorgangs F2.
3. Wählen Sie auf der Seite System Setup Main Menu (Hauptmenü für die Systemeinrichtung) **iDRAC Settings (iDRAC-Einstellungen)**.

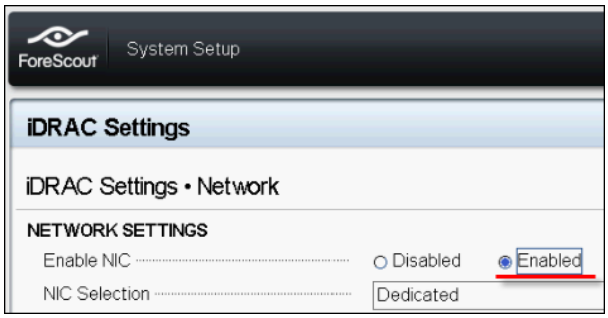


4. Wählen Sie auf der Seite iDRAC Settings (iDRAC-Einstellungen) **Network (Netzwerk)**.



5. Konfigurieren Sie die folgenden Netzwerkeinstellungen:

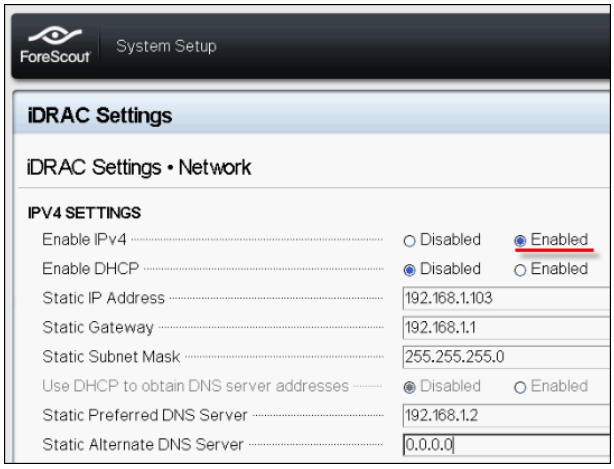
   – ***Network Settings (Netzwerkeinstellungen)***. Vergewissern Sie sich, dass das Feld **Enable NIC (NIC aktivieren)** auf **Enabled (Aktiviert)** eingestellt ist.



   – ***Common Settings (Allgemeine Einstellungen)***. Im Feld DNS DRAC Name (DRAC-Name im DNS) können Sie die Informationen für ein dynamisches DNS aktualisieren (optional).

   – ***IPV4 Settings (IPV4-Einstellungen)***. Vergewissern Sie sich, dass das Feld **Enable IPv4 (IPv4 aktivieren)** auf **Enabled (Aktiviert)** eingestellt ist.

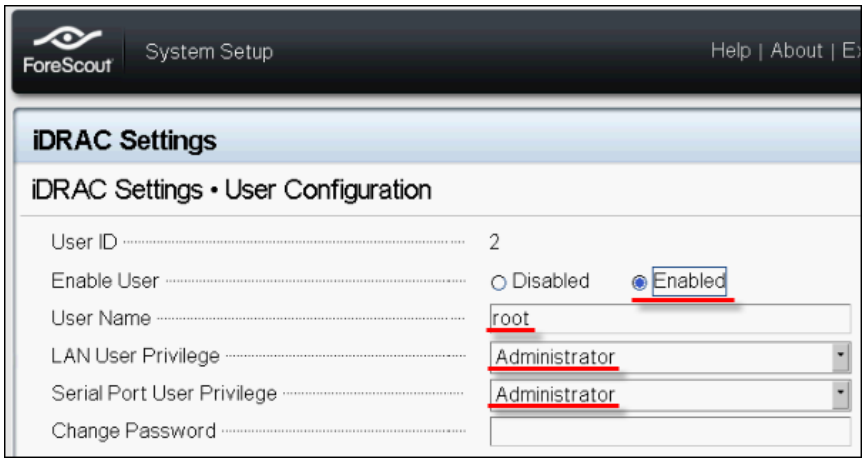
     Stellen Sie das Feld **Enable DHCP (DHCP aktivieren)** auf **Enabled (aktiviert)** um eine dynamische IP-Adressvergabe zu verwenden, oder **Disabled (deaktiviert),** wenn Sie statische IP-Adressen vergeben. Bei Aktivierung von DHCP werden iDRAC die IP-Adresse, das Gateway und die Subnetzmaske automatisch zugewiesen. Wenn DHCP deaktiviert ist, müssen Sie die entsprechenden Werte unter **Static IP Address (Statische IP-Adresse)**, **Static Gateway (Statischer Gateway)** und **Static Subnet Mask (Statische Subnetzmaske)** eingeben.



6. Wählen Sie dann **Back (Zurück)**.
7. Wählen Sie **User Configuration (Benutzerkonfiguration)**.
8. Konfigurieren Sie unter User Configuration (Benutzerkonfiguration) die folgenden Felder für root user (root-Benutzer):
   - ***Enable User (Benutzer aktivieren)***. Vergewissern Sie sich, dass dieses Feld auf Enabled (Aktiviert) eingestellt ist.

     Der hier konfigurierte Benutzername stimmt nicht mit dem CounterACT-Benutzernamen überein.

   - ***LAN and Serial Port User Privileges (Benutzerrechte für LAN und serielle Schnittstelle)***. Setzen Sie die Berechtigungsstufen auf Administrator.
   - ***Change Password (Passwort ändern)***. Legen Sie ein Passwort für die Benutzeranmeldung fest.



9. Wählen Sie **Back (Zurück)** und dann **Finish (Fertigstellen)**. Bestätigen Sie die Änderungen der Einstellungen.

   Die Netzwerkeinstellungen werden gespeichert, und das System wird neu gestartet.

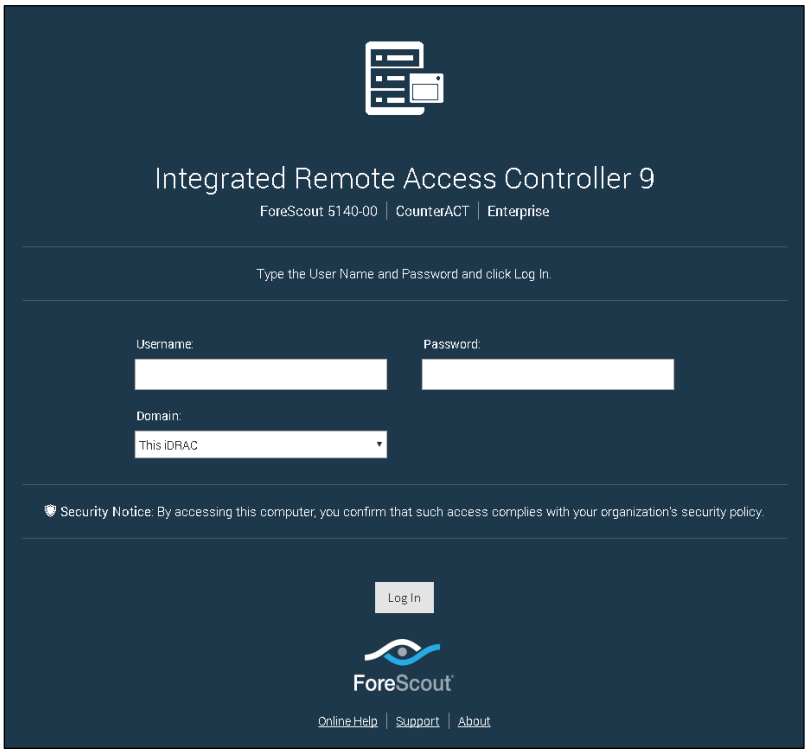
Herstellen einer Verbindung zwischen Modul und Netzwerk

Das iDRAC muss mit einem Ethernet-Netzwerk verbunden werden. Üblicherweise wird die Verbindung zu einem Verwaltungsnetzwerk hergestellt. Die nachfolgende Abbildung zeigt die Position des iDRAC-Ports auf der Rückseite der CT-1000-Appliance:

Anmelden bei iDRAC

So melden Sie sich bei iDRAC an:

1. Navigieren Sie zu der IP-Adresse oder dem Domänennamen, den Sie unter **iDRAC Settings** > **Network (iDRAC-Einstellungen Netzwerk)** konfiguriert haben.



2. Geben Sie den Benutzernamen und das Passwort ein, die Sie zuvor unter User Configuration (Benutzerkonfiguration) im Einrichtungsmenü für das iDRAC-System festgelegt haben.
3. Wählen Sie **Submit (Senden)**.

Weitere Informationen zu iDRAC erhalten Sie im *iDRAC User's Guide (Benutzerhandbuch von iDRAC)*. Sie können auf dieses Handbuch an einem der folgenden Orte zugreifen, je nachdem, welchen Lizenzmodus Ihre Installation verwendet:

- Per-Appliance Licensing Mode (Lizenzierungsmodus pro Appliance) – https://updates.forescout.com/downloads/support/iDRAC_user_guide.pdf
- Centralized Licensing Mode (Zentralisierter Lizenzmodus) – Kundenportal, Documentation Page (Dokumentationsseite).

Unter Zusätzliche CounterACT-Dokumentation (*Identifying Your Licensing Mode in the Console (Identifizieren des Lizenzierungsmodus in Console)*) erfahren Sie, welchen Lizenzierungsmodus Ihre Implementierung verwendet.

Es ist sehr wichtig, das Standard-Root-Passwort zu aktualisieren, falls Sie dies noch nicht getan haben.

6. Prüfen der Verbindungen

Prüfen der Verbindung zur Verwaltungsschnittstelle

Um die Verbindung zur Verwaltungsschnittstelle zu testen, melden Sie sich an der Appliance an und führen Sie den folgenden Befehl aus:

`fstool linktest`

Die folgenden Informationen werden angezeigt:

```
Management Interface status (Status der
Verwaltungsschnittstelle)
Pinging default gateway information (Pingtest für
Standardgatewayinformationen durchführen)
Ping statistics (Pingstatistik)
Performing Name Resolution Test (Test für die Namensauflösung
ausführen)
Test summary (Testzusammenfassung)
```

Pingtest ausführen

Führen Sie den folgenden Befehl von der Appliance zu einem Netzwerk-Desktop aus, um die Konnektivität zu überprüfen:

`Ping <network_desktop_IP_address>`

7. Einrichten von CounterACT Console

Installieren von CounterACT Console

Console ist die CounterACT-Verwaltungsanwendung, mit der wichtige Detailinformationen zu Endpunkten angezeigt und kontrolliert werden können. Diese Informationen werden von CounterACT-Geräten gesammelt. Weitere Informationen erhalten Sie im *CounterACT Administration Guide (CounterACT Administrationshandbuch)*.

Sie müssen einen Computer zur Verfügung stellen, auf dem die Anwendungssoftware CounterACT Console ausgeführt wird. Mindestanforderungen an die Hardware:

- Nicht-dedizierter Computer, auf dem Folgendes läuft:
  - Windows 7/8/8.1/10
  - Windows Server 2008/2008 R2/2012/2012 R2/2016
  - Linux RHEL/CentOS 7
- 2 GB RAM
- 1 GB freier Speicherplatz

Die Console-Anwendung kann auf zwei verschiedene Arten installiert werden:

Mit Hilfe der integrierten Installationssoftware Ihrer Appliance.

1. Öffnen Sie auf dem Computer mit Console ein Browserfenster.
2. Geben Sie die folgende Adresse ein:

   `http://<Appliance_ip>/install`

   Wobei <Appliance ip> der IP-Adresse Ihrer Appliance entspricht. Im Browser wird das Fenster für die Console-Installation angezeigt.
3. Befolgen Sie die Anweisungen auf dem Bildschirm.

Anmelden

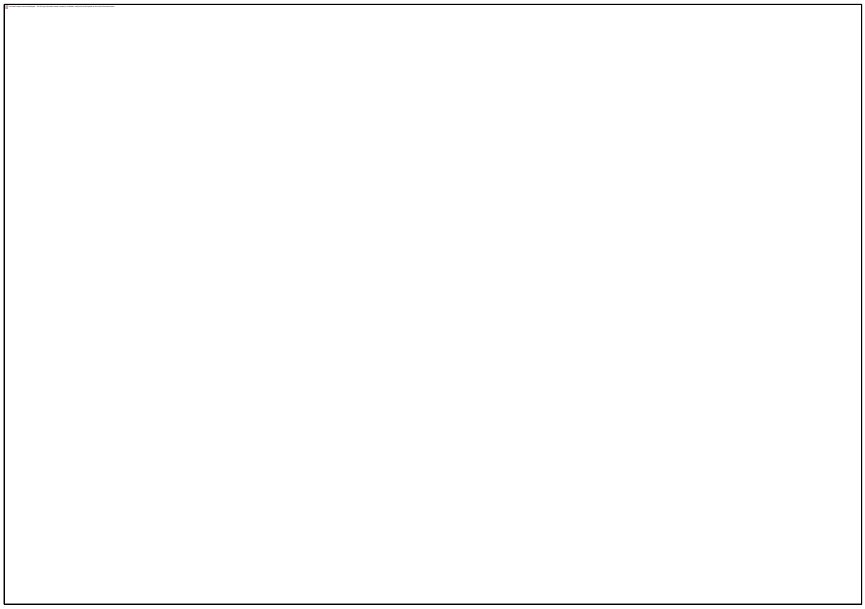
Nach Abschluss der Installation können Sie sich bei CounterACT Console anmelden.

1. Wählen Sie dazu das CounterACT-Symbol aus, das Sie zuvor als Verknüpfung an dem von Ihnen gewünschten Speicherort erstellt haben.

2. Geben Sie im Feld **IP/Name** die IP-Adresse oder den Hostnamen der Appliance ein.
3. Geben Sie im Feld **User Name (Benutzername)** admin ein.
4. Geben Sie im Feld **Password (Passwort)** das Passwort ein, das Sie während der Installation der Appliance erstellt haben.
5. Wählen Sie **Login (Anmelden)**, um Console zu starten.

Durchführen der Anfangseinstellungen

Wenn Sie sich zum ersten Mal anmelden, wird der Assistent für die Anfangseinstellungen geöffnet. Der Assistent führt Sie durch die grundlegenden Konfigurationsschritte, damit CounterACT schnell einsatzbereit ist und effizient ausgeführt wird.



Vor Beginn der Anfangseinstellungen

Halten Sie die folgenden Informationen bereit, wenn Sie mit dem Assistenten beginnen:

Vom Assistenten benötigte Informationen	Wert
Adresse des von Ihrem Unternehmen verwendeten NTP-Servers (optional)	
IP-Adresse für die interne E-Mail, um die Zustellung von E-Mail-Benachrichtigungen zu ermöglichen, wenn SMTP-Verkehr von der Appliance aus nicht zulässig ist (optional)	
E-Mail-Adresse des CounterACT-Administrators	
Überwachungs- und Antwortschnittstellen	
Für Segmente oder VLANs ohne DHCP benötigen Sie das Netzwerksegment oder die VLANs, mit denen die Überwachungsschnittstelle direkt verbunden ist, sowie eine permanente IP-Adresse für jedes VLAN, das mit CounterACT verwendet wird	
IP-Adressbereiche, die durch die Appliance überwacht werden (alle internen Adressen, einschließlich nicht verwendeter)	
LDAP-Benutzerkontoinformationen und die IP-Adresse des LDAP-Servers	
Anmeldedaten für die Domäne, einschließlich Kontoname und Passwort für die Domänenadministration	
Authentifizierungsserver, damit CounterACT analysieren kann, welche Netzwerkhosts erfolgreich authentifiziert	

wurden	
Switch-IP-Adresse, Anbieter- und SNMP-Parameter	

Weitere Informationen zur Arbeit mit dem Assistenten erhalten Sie im *CounterACT Administration Guide (CounterACT Console-Benutzerhandbuch)* oder in der Online-Hilfe.

Zusätzliche CounterACT-Dokumentation

Informationen zu weiteren CounterACT-Features und -Modulen finden Sie in den folgenden Ressourcen:

- Downloads von Dokumentationen
- Dokumentationsportal
- CounterACT-Hilfe-Tools

Downloads von Dokumentationen

Der Download von Dokumentationen kann über eines von zwei ForeScout-Portalen erfolgen, je nachdem, welchen Lizenzmodus Ihre Anwendung verwendet.

- ***Per-Appliance Licensing Mode (Lizenzierungsmodus pro Appliance)*** - Portal für Produkt-Updates
- ***Centralized Licensing Mode (zentralisierter Lizenzierungsmodus)*** - Kundenportal

Software-Downloads sind ebenfalls über diese Portale erhältlich.

Unter Identifizieren Ihres Lizenzierungsmodus in Console erfahren Sie, welchen Lizenzierungsmodus Ihre Implementierung verwendet.

Portal für Produkt-Updates

Das Produkt-Update-Portal bietet Links zu CounterACT-Versionen, Basis- und Content-Modulen und Erweiterungsmodulen sowie die dazugehörige Dokumentation. Darüber hinaus bietet das Portal eine Vielzahl von zusätzlichen Dokumentationen.

Um auf das Portal für Produkt-Updates zuzugreifen:

1. Gehen Sie zu https://updates.forescout.com/support/index.php?url=counteract.
2. Wählen Sie die CounterACT-Version aus, die Sie kennenlernen möchten.

Kundenportal

Auf der Download-Seite des ForeScout-Kundenportals finden Sie Links zu gekauften CounterACT-Versionen, Basis- und Content-Modulen und Erweiterungsmodulen sowie die dazugehörige Dokumentation. Software und die dazugehörige Dokumentation erscheinen nur dann auf der Download-Seite, wenn Sie über eine Lizenz für die

Software verfügen. Auf der Dokumentationsseite des Portals finden Sie eine Vielzahl zusätzlicher Dokumentationen.

Um auf die Dokumentation des ForeScout-Kundenportals zuzugreifen:

1. Gehen Sie zu https://forescout.force.com/support/.
2. Wählen Sie **Downloads** oder **Documentation (Dokumentation)**.

Dokumentationsportal

Das ForeScout Dokumentationsportal ist eine durchsuchbare, webbasierte Bibliothek, die Informationen über CounterACT-Werkzeuge, Features, Funktionen und Integrationen enthält.

Wenn Ihre Implementierung den zentralen Lizenzmodus verwendet, verfügen Sie möglicherweise nicht über die erforderlichen Zugangsdaten für den Zugriff auf dieses Portal.

Um auf das Dokumentationsportal zuzugreifen:

1. Gehen Sie zu www.forescout.com/docportal.
2. Verwenden Sie Ihre Kunden-Support-Anmeldeinformationen, um sich einzuloggen.
3. Wählen Sie die CounterACT-Version aus, die Sie kennenlernen möchten.

CounterACT-Hilfe-Tools

Greifen Sie direkt von CounterACT Console auf Informationen zu.

Hilfe-Schaltflächen für Console

Verwenden Sie kontextsensitive *Help* buttons (Hilfe-Schaltflächen), um schnell auf Informationen über die Aufgaben und Themen zuzugreifen, mit denen Sie arbeiten.

CounterACT Administrationshandbuch

Wählen Sie **CounterACT Help (CounterACT Hilfe)** aus dem **Help** menu (Hilfemenü).

Plugin Help Files (Plugin-Hilfedateien)

1. Wählen Sie nach der Installation des Plugins **Options (Optionen)** aus dem **Tools** menu (Werkzeugmenü) und dann **Modules (Module)**.
2. Wählen Sie das Plugin aus und wählen Sie dann **Help (Hilfe)**.

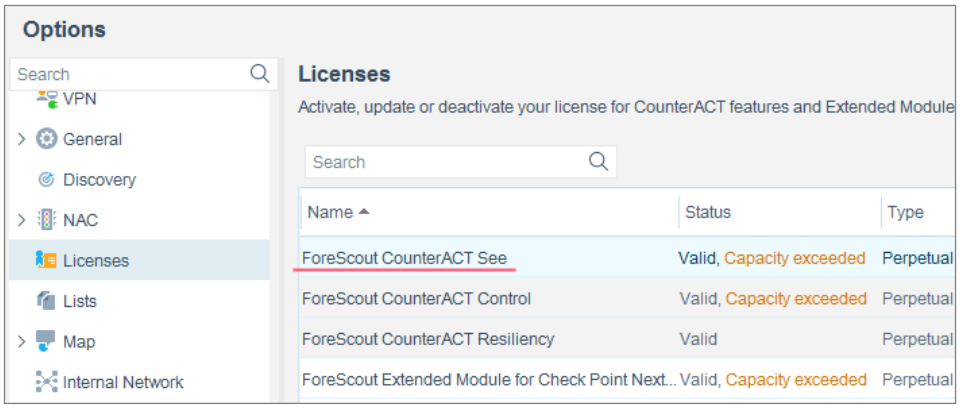
Dokumentationsportal

Wählen Sie **Documentation Portal (Dokumentationsportal)** aus dem **Help** menu (Hilfemenü).

Identifizieren Ihres Lizenzierungsmodus in Console

Wenn Ihr Unternehmens-Manager über eine Lizenz von *ForeScout CounterACT* verfügt, die in Console aufgelistet ist, läuft die Implementierung im zentralen Lizenzierungsmodus. Ist dies nicht der Fall, wird die Implementierung im Lizenzierungsmodus pro Appliance ausgeführt.

Wählen Sie **Options > Licenses (Optionen > Lizenzen)** um zu sehen, ob Sie eine *ForeScout CounterACT-Lizenz* besitzen, die in der Tabelle aufgeführt ist.



Wenden Sie sich an Ihren ForeScout-Vertreter, wenn Sie Fragen zur Identifizierung Ihres Lizenzmodus haben.

Rechtliche Hinweise

Senden Sie Kommentare und Fragen zu diesem Dokument an: support@forescout.com

2018-03-27 15:05