CounterACT 7.0

Quick Installation Guide
for a Single Virtual CounterACT Appliance

Table of Contents

Welcome to CounterACT Version 7.0.0

ForeScout's Network Access Control (NAC) solution lets customers gain complete control over network security without disrupting corporate and end-user productivity. CounterACT combines cutting edge NAC and intrusion prevention technologies in a single Appliance. CounterACT performs complete endpoint inspection and access control of every network device—and seamlessly integrates with any existing IT infrastructure

CounterACT Virtual Appliances

CounterACT virtual devices (Appliances/Enterprise Managers) can be installed and managed in virtual data centers and IT environments, and provide capabilities identical to Appliance and Enterprise Manager software installations carried out on dedicated machines. Using virtual CounterACT devices lets you:

- Simplify and ease product distribution and deployment, especially for distributed remote sites.
- Reduce IT costs, space, energy consumption, maintenance by using less hardware.
- Comply with green IT requirements.

- This guide describes the installation for a single CounterACT Appliance. For more detailed information or information about deploying multiple Appliances for enterprise-wide network protection, refer to the *CounterACT Installation Guide*.

Chapter 7 of the *Installation Guide* provides more details about working with Virtual CounterACT devices, including:

- Supported VM Hardware Specification Requirements
- Virtual Environment Setup
- Post Deployment Verification
- CounterACT Virtual Device Installation
- Licensing Information
- Connecting to the ForeScout License Server

Overview

Perform the following to set up CounterACT:

1. ***Create a Deployment Plan***
2. ***Set Up your Switch***
3. ***Pre-installation Setup***
4. ***Configure the Appliance***
5. ***Verify Connectivity***
6. ***Set Up the CounterACT Console***

1. Create a Deployment Plan

Before performing the installation, you should decide where to deploy the Appliance and learn about Appliance interface connections.

Decide Where to Deploy the Appliance

The Appliance should be deployed at a central location, where it sees all vital network traffic and has access to your network devices. Selecting the right location is important for successful deployment.

Notes

- It is recommended to monitor the authentication traffic between end users and authentication servers.
- In order to notify end users via their web browsers, the Appliance must monitor HTTP traffic between end users and the Internet/Intranet.

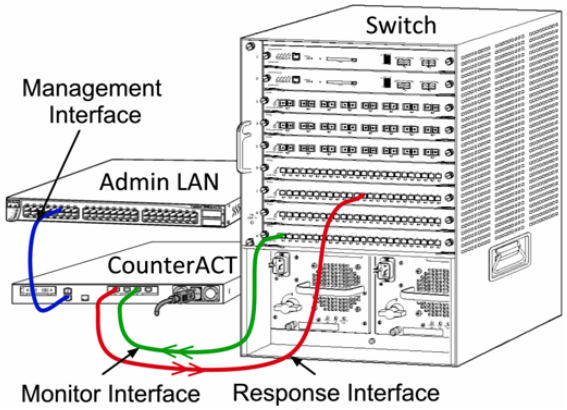
Learn about Appliance Interface Connections

The Appliance is generally configured with three connections to the network switch.

Management Interface

This interface allows you to manage CounterACT and perform queries and deep inspection of endpoints. The interface must be connected to a switch port that has access to all network endpoints.

Each Appliance requires a single management connection to the network. This connection requires an IP address on the local LAN and port 13000/TCP access from machines that will be running the CounterACT Console management application. The management interface must have access to the following on your network:



Port	Service	To or From CounterACT	Function
22/TCP	SSH	To	Allows access to the CounterACT command line interface.
2222/TCP			(High Availability) Allows access to the physical CounterACT devices that are part of the High Availability cluster. Use 22/TCP to access the shared (virtual)

Port	Service	To or From CounterACT	Function
			IP address of the cluster.
25/TCP	SMTP	From	Allows CounterACT access to the enterprise mail relay.
80/TCP	HTTP	To	Allows HTTP redirection.
443/TCP	HTTPS	To	Allows HTTP redirection using SSL.
13000/TCP	CounterACT	To	For systems with only one Appliance – from the Console to the Appliance For systems with more than one CounterACT Appliance – from the Console to the Enterprise Manager and from the Enterprise Manager to each Appliance.
53/UDP	DNS	From	Allows CounterACT to resolve internal IP addresses.
123/UDP	NTP	From	Allows CounterACT access to a local time server or ntp.forescout.net By default CounterACT accesses ntp.foreScout.net
161/UDP	SNMP	From	Allows CounterACT to communicate with network switches and routers. For information about configuring SNMP, refer to the *CounterACT Console User Manual*.
162/UDP	SNMP	To	Allows CounterACT to receive SNMP traps from network switches and routers For information about configuring SNMP, refer to the *CounterACT Console User Manual*.
10003/TCP	SecureConnector	To	Allows a SecureConnector tunnel between endpoints and an Appliance. *SecureConnector* enables access to unmanageable endpoints via a secure executable file that runs at the desktop while the host is connected to the network. Refer to the *CounterACT Console User Manual* for more information about SecureConnector. When SecureConnector connects to an Appliance or to the Enterprise Manager it is redirected to the Appliance to which its host is assigned. Arrange connectivity of this port to all Appliances and to the Enterprise Manager to allow transparent

Port	Service	To or From CounterACT	Function
			mobility within the organization. Port 10003 is the default; you can change this.

Monitor Interface

This connection allows the Appliance to monitor and track network traffic.

Traffic is mirrored to a port on the switch and monitored by the Appliance. Depending on the number of VLANs being mirrored, the traffic may or may not be 801.2Q VLAN tagged.

- Single VLAN (untagged) When monitored traffic is generated from a single VLAN, the mirrored traffic does not need to be VLAN tagged.
- Multiple VLANs (tagged) When monitored traffic is from more than one VLAN, the mirrored traffic must be 801.2Q VLAN tagged.

When two switches are connected as a redundant pair, the Appliance *must* monitor traffic from *both* switches.

No IP address is required on the monitor interface.

Response Interface

The Appliance responds to traffic using this interface. Response traffic is used to protect against malicious activity and carry out NAC policy actions. These actions may include, for example, redirecting Web browsers or performing firewall blocking. The related switch port configuration depends on the traffic being monitored.

- Single VLAN\untagged: When monitored traffic is generated from a single VLAN, the response interface must belong to the same VLAN. In this case, the Appliance requires a single IP address on that VLAN.
- Multiple VLANs\tagged: If monitored traffic is from more than one VLAN, the response interface must also be configured with 801.2Q tagging for the same VLANs. The Appliance requires an IP address for each protected VLAN.

2. Set Up your Switch

A. Switch Connection Options

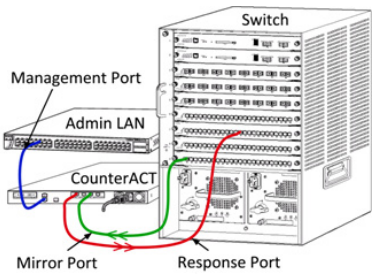
The Appliance was designed to seamlessly integrate into a wide variety of network environments. To successfully integrate the Appliance into your network, verify that your switch is set up to monitor required traffic. Verify that the VMware server on which the Appliance is installed is configured with three interface connections to the network switch.

Select a host on which you want to install the Virtual Appliance, and define virtual switches for the management, monitor and response NICs on the host.

Several options are available for connecting the Appliance to your switch.

1 Standard Deployment (Separate Management, Monitoring and Response Interface

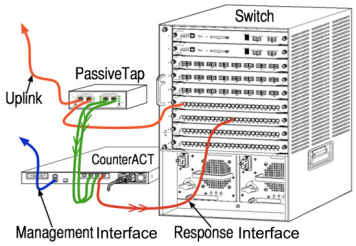
The recommended deployment uses three separate ports. These ports are described in *Learn about Appliance Interface Connections*.



2 Passive Inline Tap

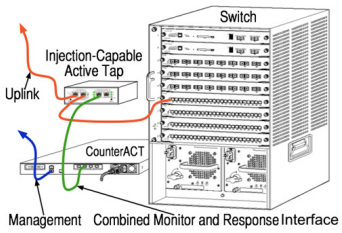
Instead of connecting to the switch monitoring port, the Appliance can use an inline tap.

A passive tap requires two monitor ports, except in the case of "recombination" taps, which will combine the two duplex streams into a single port. The traffic on the tapped port and response interface must be on matching VLANs. For example, if the traffic on the tapped port is VLAN tagged (801.2Q), then the response interface must also be a VLAN tagged port. In summary, the response interface must be configured the same way as the monitored port.



3 Active (Injection-Capable) Inline Tap

When the Appliance uses an inline tap that is *injection capable*, monitor and response interfaces can be combined. There is no need to configure a separate response port on the switch. This option can be used for any type of upstream or downstream switch configuration.



4 IP Layer Response (for Layer-3-only Core Switch Installations)

The Appliance can use its own management interface to respond to traffic. Although this option can be used with any monitored traffic, it is recommended when the Appliance monitors ports that are not part of any VLAN, and thus the Appliance cannot respond to monitored traffic using any other switch port. This is typical when monitoring a link connecting two routers.

This option cannot respond to Address Resolution Protocol (ARP) requests, which limits the ability of the Appliance to detect scans aimed at the IP addresses included in the monitored subnet. This limitation does not apply when traffic between two routers is being monitored.

B. Switch Setting Notes

VLAN (801.2Q) Tags

- **Monitoring a Single VLAN (untagged traffic)** If the monitored traffic is from a single VLAN, then traffic does not need 801.2Q tags.
- **Monitoring Multiple VLANs (Tagged traffic)** If the monitored traffic is from two or more VLANs, then *both* the monitor and response interfaces must have 801.2Q tagging enabled. Monitoring multiple VLANs is the recommended option as it provides the best overall coverage while minimizing the number of mirroring ports.
- If the switch cannot VLAN tag the mirroring ports, then either
  - mirror only a single VLAN
  - mirror a single, untagged uplink port
  - use the IP Layer response option
- If the switch can only mirror one port, then mirror a single uplink port. This may be tagged. In general, if the switch strips the VLAN tags, you will need to use the IP Layer response option.

Additional

- If the switch cannot mirror both transmit and receive traffic, then monitor the entire switch, complete VLANs (this provides transmit/receive), or just one interface (which does allow transmit/receive). Verify that you do not overload the mirroring port.
- Some switches (e.g. Cisco 6509) may need former port configurations completely cleared out before entering new configurations. The most common result when not clearing out old port information is that the switch strips 801.2Q tags.

3. Pre-installation Setup

Record the Interface Assignments

After completing the Appliance installation and installing the CounterACT Console, you will be prompted to register interface assignments. These assignments, referred to as *Channel definitions*, are entered in the Initial Setup Wizard that opens when you first log on to the Console.

Record the interface assignments of the virtual Appliance below and use them when completing the Channel setup at the Console.

Eth Interface	Interface Assignment (e.g. Management, Monitor, Response)
Eth0	
Eth1	
Eth2	
Eth3	
Eth4	
Eth5	
Eth6	
Eth7	
Eth8	

4. Configure the Appliance

Prepare the following information before you configure the Appliance.

Appliance host name	
CounterACT Admin password	
Management interface	
Appliance IP address	
Network mask	
Default Gateway IP address	
DNS Domain name	
DNS server addresses	

1. From your VMware management console (VMware vSphere Client) power-on the virtual Appliance and open the console to connect to it. After power on, you will be prompted to start configuration with the following message:

```
CounterACT Appliance boot is complete.

Press <Enter> to continue.
```

2. Press <Enter> to display the following menu:

```
1) Configure CounterACT-6.3.X
2) Restore saved CounterACT-6.3.X configuration
3) Identify network interfaces
4) Configure keyboard layout
5) High Availability Setup
6) Turn machine off
Choice (1-6) :1
```

3. Select 1 – Configure 6.3.X. At the prompt Continue: (yes/no)? press <Enter> to initiate the setup.
4. The High Availability Mode menu opens. Press **Enter** to select Standard Installation.
5. The CounterACT Initial Setup prompt is displayed. Press **Enter** to continue.
6. The Select CounterACT Installation Type menu opens. Type 1 and press Enter to install a standard CounterACT Appliance.

   The setup is initialized. This may take a moment.
7. At the Enter Machine Description prompt, enter a short text identifying this device, and press **Enter**.

   The following is displayed:

```
>>>>>> Set Administrator Password <<<<<<

This password is used to log in as 'root' to the
machine Operating System and as 'admin' to the
CounterACT Console.
The password should be between 6 and 15 characters long
and should contain at least one non-alphabetic
character.

Administrator password :
```

8. At the Set Administrator Password prompt, type the string that is to be your password (the string is not echoed to the screen) and press **Enter**. You are prompted to confirm the password. The password must be between 6 and 15 characters long and should contain at least one non-alphabetic character.

Log on to the Appliance as root*, and log on to the Console as* admin*.*

9. At the Set Host Name prompt, type a host name and press **Enter**. The host name can be used when logging into the Console, and is displayed in the Console to help you identify the CounterACT Appliance that you are viewing.
10. The **`Configure Network settings`** screen prompts you for a series of configuration parameters. Type a value at the prompt and press **Enter** to display the next prompt.
    - CounterACT components communicate through *management interfaces*. The number of management interfaces listed depends on the Appliance model.
    - The **Management IP address** is the address of the interface through which CounterACT components communicate. Add a VLAN ID for this interface only if the interface used to communicate between CounterACT components is connected to a tagged port.
    - If there is more than one **DNS server address**, separate each address with a space—Most internal DNS servers resolve external and internal addresses but you may need to include an external-resolving DNS server. As nearly all DNS queries performed by the Appliance will be for internal addresses, the external DNS server should be listed last.
11. The Setup Summary screen is displayed. You are prompted to perform general connectivity tests, reconfigure settings, or complete the setup.

You will be prompted to start the configuration. The following menu opens:

```
1) Configure CounterACT- X.X.X
2) Restore saved CounterACT- X.X.X configuration
3) Identify network interfaces
4) Configure keyboard layout
5) High Availability Setup
6) Turn machine off
7) Reboot the machine

Choice (1-8) : 3
```

License

After installation, you must install the initial demo license provided by your CounterACT representative. The license is installed during the initial Console setup. This initial demo license is valid for a certain number of days. You must install a permanent license before this period expires. You will be contacted via e-mail regarding the expiration date. In addition, information about the expiration date and status license is displayed in the Console, Appliances/Devices pane.

Once you receive a permanent license, the license is validated daily by the ForeScout License Server. License alerts and violations are displayed in the Device Details pane.

Licenses are authenticated via the ForeScout License Server once a day. Licenses that can not be authorized for a month will be revoked. When this happens, significant CounterACT functionality will stop. Refer to the *CounterACT Installation Guide* for more details about licenses.

Network Connection Requirements

At least one CounterACT device must have an Internet connection. This connection is used to authenticate CounterACT licenses against the ForeScout License server.

Licenses that can't be authenticated for one month will be revoked. You will receive a warning email once a day indicating there is a communication error with the server.

5. Verify Connectivity

Verify the Management Interface Connection

To test the management interface connection, log in to the Appliance and run the following command:

```
fstool linktest
```

The following information is displayed:

```
Management Interface status

Pinging default gateway information

Ping statistics

Performing Name Resolution Test

Test summary
```

Verify Switch /Appliance Connectivity

Verify that the switch is properly connected to the Appliance before leaving the data center. To do this, run the **`fstool ifcount`** command at the Appliance for each interface detected.

```
fstool ifcount eth0 eth1 eth2
(Separate each interface by a space.)
```

This tool continuously displays network traffic on the specified interfaces. It works in two modes: per interface or per VLAN. The mode can be changed from the display. The total bits per second and the percentage of each of the following traffic categories is shown:

- The monitoring interface should primarily see mirrored traffic- above 90%.
- The response interface should primarily see broadcast traffic.
- Both the monitor and response interface should see the expected VLANs.

Command options:

```
v – display in VLAN mode
I – display in interface mode
P – show previous
N – show next
q – quit displaying
```

VLAN Mode:

```
update=[4]       [eth3: 14 vlans]
Interface/Vlan   Total       Broadcast   Mirrored    *To my MAC   *From my
MAC
eth3.untagged    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
```

Interface Mode:

```
update=[31]      [eth0: 32 vlans] [eth1: 1 vlans]
Interface        Total      Broadcast  Mirrored   *To my MAC *From my MAC
eth0             3Kbps        42.3%       0.0%        14.1%      43.7%
eth1             475bps       0.0%        100.0%      0.0%       0.0%
```

*To my MAC - Destination MAC is the Appliance's MAC.
*From my MAC - Traffic sent by this Appliance (Source MAC is the Appliance's MAC. Destination can be broadcast or unicast).

If you do not see any traffic, verify that the interface is up. Use the following command at the Appliance:

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

Perform Ping Test

Run a ping test from the Appliance to a network desktop to verify connectivity.

To run the test:

1. Log in to the Appliance.
2. Run the following command: **Ping [network desktop IP]**
   By default, the Appliance itself does not reply to ping.

6. Set Up the CounterACT Console

Install the CounterACT Console

The CounterACT Console is a central management application used to view, track, and analyze the activity detected by the Appliance. NAC, Threat Protection, Firewall and other polices can be defined from the Console. Refer to the *CounterACT Console User Manual* for more information.

Minimum requirements are:

- Non-dedicated PC, running Windows NT/2000/2003/XP/Vista, Linux or Windows 7.
- 512MB RAM for up to 10,000 devices
- 1Gig RAM for more than 10,000 devices
- Disk space - 100 MB
- CD ROM drive

To install the Console using the installation software built into your Appliance:

1. Open a browser window from the Console computer.
2. Type the following into the browser address line:

   `http://x.x.x.x/install`

   where the IP address is the address of this Appliance. The browser displays the Console installation window.
3. Follow the on-screen instructions.

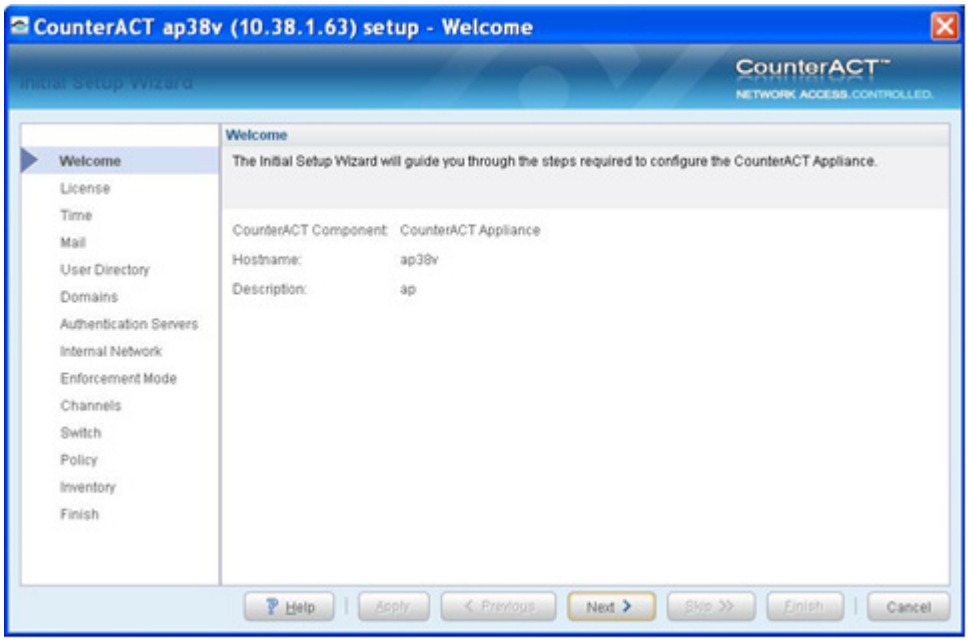
Log In

After completing the installation, you can log in to the CounterACT Console.

1. Select the CounterACT icon from the shortcut location you created.
2. In the **IP/Name** field, enter the IP address or host name of the Appliance.
3. In the **User Name** field, enter **admin**.
4. In the **Password** field, enter the password you created during Appliance installation.
5. Select **Login** to open Console.

Perform Initial Setup

After logging in for the first time, the Initial Setup Wizard appears. The Wizard guides you through essential configuration steps to ensure that CounterACT is up-and-running quickly and efficiently.



Before You Begin

Prepare the following information before working with the Wizard:

Information	Values
NTP server address used by your organization.	
Internal mail relay IP address. This allows delivery of email alerts if SMTP traffic is not allowed from the Appliance.	
CounterACT administrator's email address.	
Monitor and response interfaces assignments defined at the Data Center. The monitors interface tracks traffic going through your network. The response interface is used to protect against malicious activity, carrying out Virtual Firewall blocking and HTTP redirection. This information is not required for Enterprise Manager setup.	
For segments or VLANs with no DHCP, the network segment or VLANs to which the monitoring interface is directly connected and a permanent IP address to be used by CounterACT at each such VLAN. This information is not required for Enterprise Manager setup.	
IP address ranges that the Appliance will protect (all the internal addresses, including unused addresses).	

User Directory account information and the User Directory server IP address.	
Domain credentials, including domain administrative account name and password.	
Authentication servers so that CounterACT can analyze which network hosts have successfully authenticated.	

Refer to the *CounterACT Console User Manual* or Online Help for information about working with the Wizard.

Contact Information

For ForeScout technical support send email to support@forescout.com or call the following toll-free numbers:

International: (708) 237-6591

North America: 1 (866) 377-8771

Illustration courtesy of Intel Corporation. ©2005 Intel Corporation.

CT7.0-QIG3/16/11