CounterACT 7.0

Single CounterACT Appliance

Quick Installation Guide

Table of Contents

Welcome to CounterACT™ Version 7.0

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.

This guide describes the installation for a single stand-alone CounterACT Appliance.

For more detailed information or information about deploying multiple Appliances for enterprise-wide network protection, refer to the *CounterACT Installation Guide* and *Console User Manual*. These documents are located on the CounterACT CD in the /docs directory.

Additionally, you can navigate to the support website located at: http://www.forescout.com/support for the latest documentation, knowledge base articles, and updates for your Appliance.

Included in your CounterACT Package

- CounterACT Appliance
- Quick Installation Guide
- CounterACT CD with Console software, CounterACT Console User Manual and Installation Guide
- Warranty document
- Mounting brackets
- Power cable
- DB9 Console connecting cable (for serial connections only)

Overview

Perform the following to set up CounterACT:

1. Create a Deployment Plan
2. Set Up your Switch
3. Connect Network Cables and Power
4. Configure the Appliance
5. Remote Management
6. Verify Connectivity
7. 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.

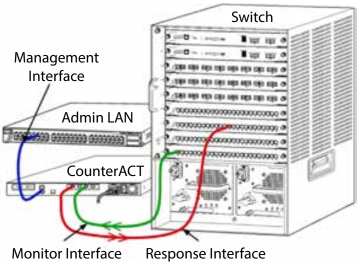
Decide Where to Deploy the Appliance

Selecting the correct network location where the Appliance will be installed is crucial for successful deployment and optimal performance of CounterACT. The correct location will depend on your desired implementation goals and network access policy. The Appliance should be able to monitor the traffic that is relevant to the desired policy. For example, if your policy depends on monitoring authorization events from endpoints to corporate authentication servers, the Appliance will need to be installed so that it sees endpoint traffic flowing into authentication server(s).

For more information about installation and deployment, refer to the CounterACT Installation Guide, located on the CounterACT CD you received with this package.

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) IP address of the cluster.

Port	Service	To or From CounterACT	Function
445/139	RPC	From	Allows CounterACT to perform deep investigation and control of Windows endpoints using RPC.
135	WMI	From	Allows CounterACT to perform deep investigation and control of Windows endpoints using WMI.
10003	Secure Connector	To	Allows SecureConnector to create a secure (encrypted SSL) connection to the Appliance from Windows machines. SecureConnector receives inspection and action requests and responds to them via this connection; all CounterACT traffic between SecureConnector and the Appliance is transmitted via the secure connection.
2200/TCP	Secure Connector	To	Allows SecureConnector to create a secure (encrypted SSH) connection to the Appliance from Macintosh/Linux machines. SecureConnector enables access to unmanageable endpoints via a shell script that runs at the desktop while the host is connected to the network.
22	SSH	From	Allows CounterACT to perform deep investigation and control of Macintosh and Linux endpoints.
25/TCP	SMTP	From	Used to send mail from CounterACT
80/TCP	HTTP	To	Allows HTTP redirection.
443/TCP	HTTPS	To	Allows HTTP redirection using SSL.
13000/TCP	CounterACT	To	Allows connection from the Console to the Appliance. For systems with multiple CounterACT Appliances, allows connection 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 an NTP time server. By default, CounterACT uses ntp.foreScout.net.
161/UDP	SNMP	From	Allows CounterACT to communicate with network infrastructure gear, such as 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 infrastructure gear, such as switches and routers. For information about configuring SNMP, refer to the *CounterACT Console User Manual*.

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 802.1Q 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 802.1Q VLAN tagged.

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

Typically, the monitoring interface does not require an IP address.

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.

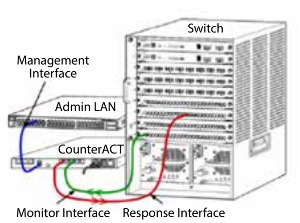
- **Single VLAN (untagged):** When monitored traffic is generated from a single VLAN, the response interface must be configured to be part of the same VLAN. In this case, the Appliance requires a single IP address on that VLAN.
- **Multiple VLANs (tagged):** If monitored traffic is from more than one VLAN, the response interface must also be configured with 802.1Q tagging for the same VLANs. The Appliance requires an IP address for each protected VLAN.

2. Set Up Your Switch

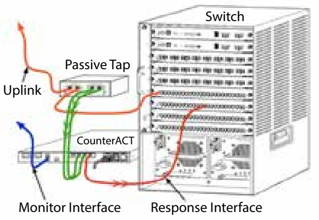
A. Switch Connection Options

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

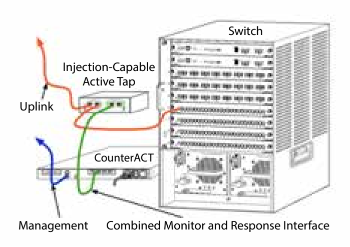
1. **Standard Deployment (Separate Management, Monitoring and Response Interfaces)**
   The recommended deployment uses three separate ports. These ports are described in *Appliance Interface Connections.*



2. **Passive Inline Tap**
   Instead of connecting to a 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 configured in the same way. For example, if the traffic on the tapped port is VLAN tagged (802.1Q), the response interface must also be a VLAN tagged 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.


Switch
Injection-Capable Active Tap
Uplink
CounterACT
Management
Combined Monitor and Response Interface

4. **IP Layer Response (for Layer-3 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 (802.1Q) Tags

- **Monitoring a Single VLAN (untagged traffic)** If the monitored traffic is from a single VLAN, traffic does not need 802.1Q 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 802.1Q 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 use an 802.1Q VLAN tag on the mirroring ports, do one of the following:
    - 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 802.1Q VLAN tags, you will need to use the IP Layer response option.

Additional

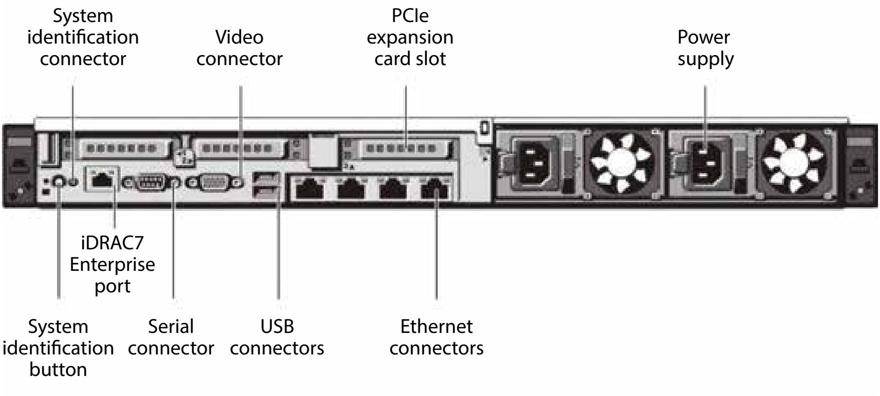
- If the switch cannot mirror both transmit and receive traffic, then monitor the entire switch, complete VLANs (this provides transmit/receive), or just one interface (which does allow transmit/receive). Verify that you do not overload the mirroring port.
- Some switches (e.g. Cisco 6509) may need former 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 802.1Q tags.

3. Connect Network Cables and Power On

A. Unpack the Appliance and Connect Cables

1. Remove the Appliance and power cable from the shipping container.
2. Remove the rail kit you received with the Appliance.
3. Assemble the rail kit on the Appliance and mount the Appliance to the rack.
4. Connect the network cables between the network interfaces on the Appliance rear panel and the switch ports.

Rear Panel Sample — CounterACT Device



B. Record the Interface Assignments

After completing the Appliance installation at the data center 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 physical interface assignments below and use them when completing the Channel setup at the Console.

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

C. Power On the Appliance

1. Connect the power cable to the power connector on the Appliance rear panel.
2. Connect the other end of the power cable to a grounded AC outlet.
3. Connect the keyboard and monitor to the Appliance or set up the Appliance for serial connection. Refer to the *CounterACT Installation Guide* located on the CounterACT CD.
4. Power on the Appliance from the front panel.

Important: Power off the machine before unplugging.

4. Configure the Appliance

Prepare the following information before you configure the Appliance.

□ Appliance host name	
□ CounterACT Admin password	Keep the password in a secure location
□ Management interface	
□ Appliance IP address	
□ Network mask	
□ Default Gateway IP address	
□ DNS Domain Name	
□ DNS server addresses	

After power on, you will be prompted to start configuration with the following message:

```
CounterACT Appliance boot is complete.
Press <Enter> to continue.
```

1. Press **Enter** to display the following menu:

```
1) Configure CounterACT
2) Restore saved CounterACT configuration
3) Identify and renumber network interfaces
4) Configure keyboard layout
5) Turn machine off
6) Reboot the machine
Choice (1-6) :1
```

2. Select **1** – Configure CounterACT. At the prompt:

   ```
   Continue: (yes/no)?
   ```

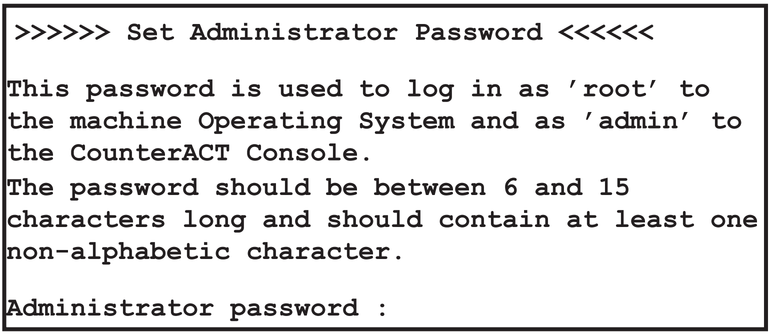
   Press **Enter** to initiate the setup.

3. The `High Availability Mode` menu opens. Press **Enter** to select Standard Installation.

4. The `CounterACT Initial Setup` prompt is displayed. Press **Enter** to continue.

5. 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.

6. 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 :
```

7. 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 a*s root, *and log on to the Console as* admin.

8. 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 at the Console to help you identify the CounterACT Appliance that you are viewing.

9. The `Configure Network Settings` screen prompts you for a series of configuration parameters. Type a value at each 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.

10. The `Setup Summary` screen is displayed. You are prompted to perform general connectivity tests, reconfigure settings or complete the setup. Type **D** to complete setup.

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 that cannot be validated for an extended period of time will be revoked. Refer to the CounterACT Installation Guide for more details about licenses.

Network Connection Requirements

At least one CounterACT device (Appliance or Enterprise Manager) must be able to access the Internet. This connection is used to validate CounterACT licenses against the ForeScout License server.

Licenses that can't be authenticated for an extended period of time will be revoked. CounterACT will send a warning email once a day indicating there is a communication error with the server.

5. Remote Management

iDRAC7 Setup

The Integrated Dell Remote Access Controller 7 (iDRAC7) is an integrated server system solution that gives you location-independent/OS-independent remote access over the LAN or Internet to CounterACT Appliances/Enterprise Managers. Use the module to carry out KVM access, power on/off/reset and perform troubleshooting and maintenance tasks.

Perform the following to work with the iDRAC module:

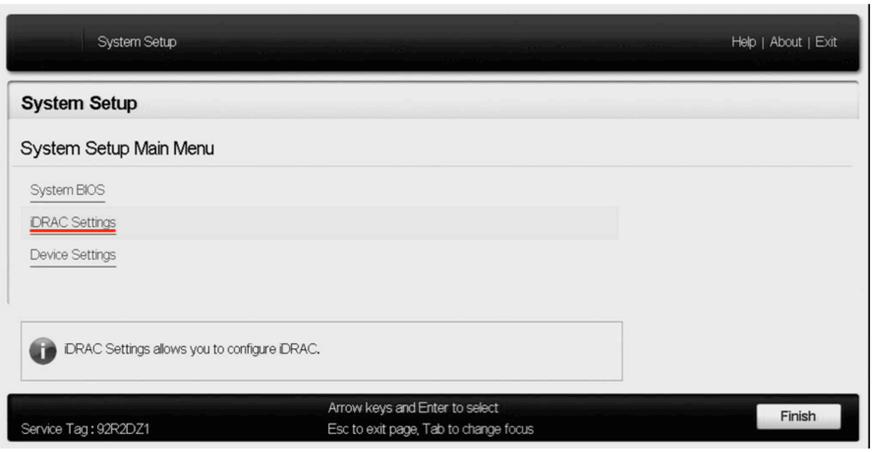
- *Enable and Configure the iDRAC Module*
- *Connect the Module to the Network*
- *Login to iDRAC*

Enable and Configure the iDRAC Module

Change the iDRAC settings to enable remote access on the CounterACT device. This section describes basic integration settings required for working with CounterACT.

To configure iDRAC:

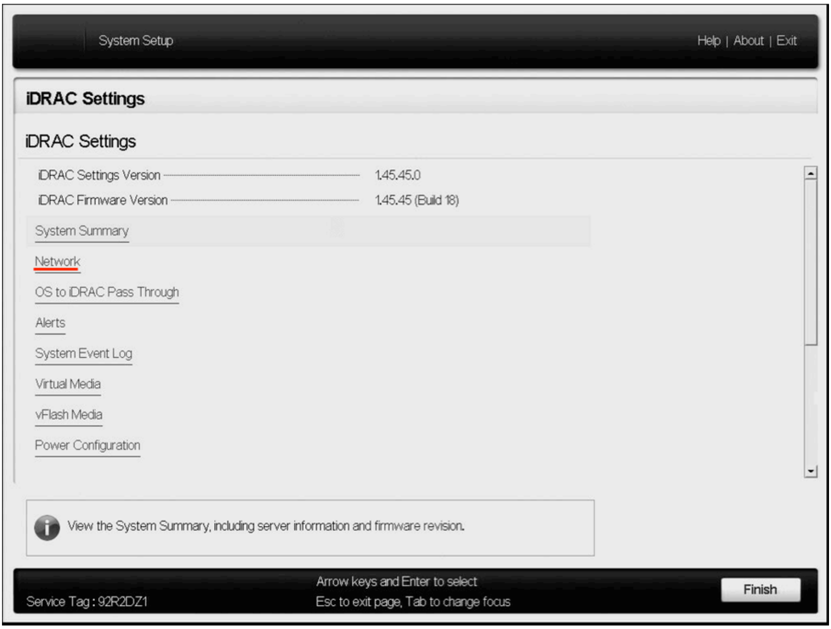
1. Turn on the managed system.
2. Select F2 during Power-on Self-test (POST).
3. In the System Setup Main Menu page, select **iDRAC Settings**.



iDRAC Settings allows you to configure iDRAC.

Service Tag : 92R2DZ1
Arrow keys and Enter to select
Esc to exit page, Tab to change focus
Finish

4. In the iDRAC Settings page, select **Network**.



iDRAC Settings

iDRAC Settings

iDRAC Settings Version 1.45.45.0

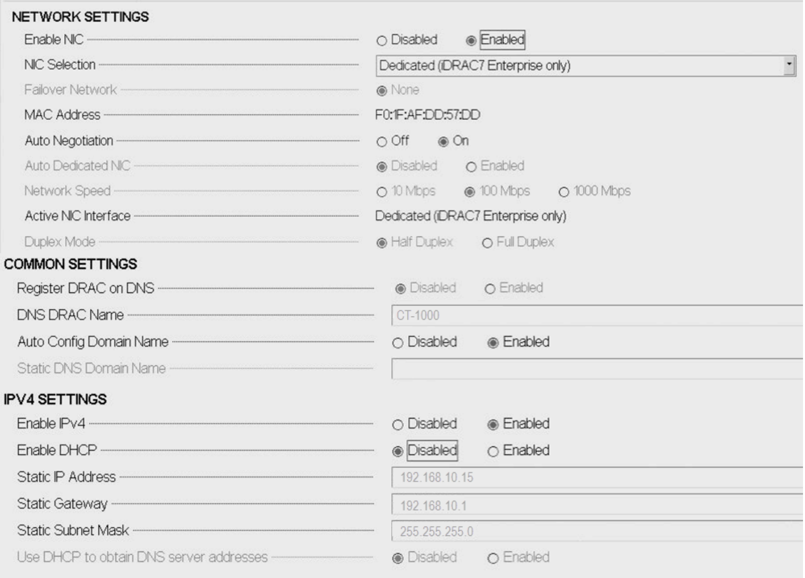
iDRAC Firmware Version .... 1.45.45 (Build 18)

View the System Summary, including server information and firmware revision.

Service Tag : 92R2DZ1

Arrow keys and Enter to select
Esc to exit page, Tab to change focus

5. Configure the following Network settings:
   - ***Network Settings.*** Verify that the **Enable NIC** field is set to **Enabled**.
   - ***Common Settings.*** In the DNS DRAC Name field, you can update a dynamic DNS (Optional).
   - ***IPV4 Settings.*** Verify that the **Enable IPv4** field is set to **Enabled**. Set the **Enable DHCP** field to **Enabled** to use Dynamic IP Addressing or to Disabled to use Static IP Addressing. If enabled, DHCP will automatically assign the IP address, gateway and subnet mask to iDRAC7. If disabled, enter values for the **Static IP Address, Static Gateway** and **Static Subnet Mask** fields.



NETWORK SETTINGS

Enable NIC ○ Disabled ● Enabled

NIC Selection Dedicated (iDRAC7 Enterprise only)

Failover Network ● None

MAC Address F0:1F:AF:DD:57:DD

Auto Negotiation ○ Off ● On

Auto Dedicated NIC ● Disabled ○ Enabled

Network Speed ○ 10 Mbps ● 100 Mbps ○ 1000 Mbps

Active NIC Interface Dedicated (iDRAC7 Enterprise only)

Duplex Mode ● Half Duplex ○ Full Duplex

COMMON SETTINGS

Register DRAC on DNS ● Disabled ○ Enabled

DNS DRAC Name CT-1000

Auto Config Domain Name ○ Disabled ● Enabled

Static DNS Domain Name

IPV4 SETTINGS

Enable IPv4 ○ Disabled ● Enabled

Enable DHCP ● Disabled ○ Enabled

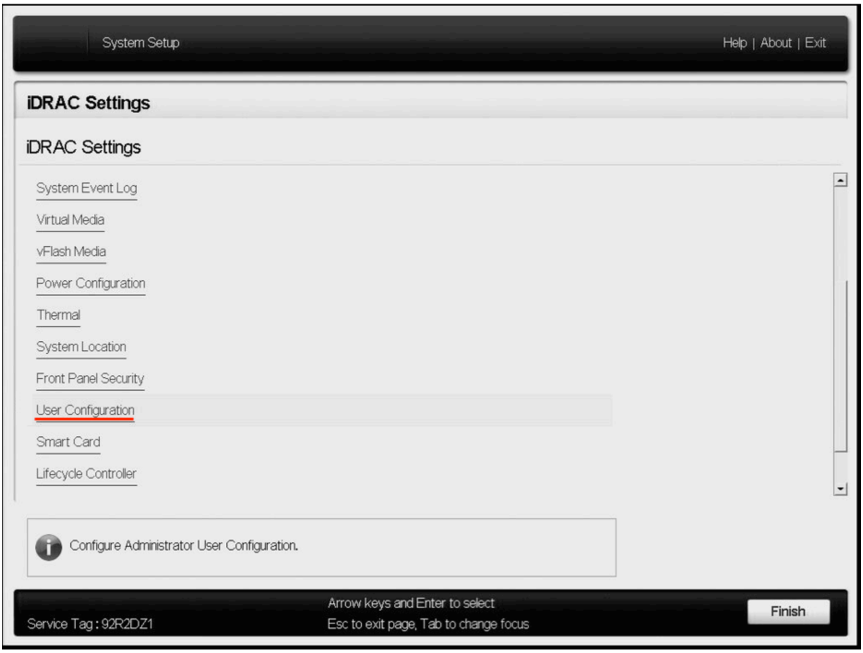
Static IP Address 192.168.10.15

Static Gateway 192.168.10.1

Static Subnet Mask 255.255.255.0

Use DHCP to obtain DNS server addresses ● Disabled ○ Enabled

6. Select **Back**.
7. Select **User Configuration**.



iDRAC Settings

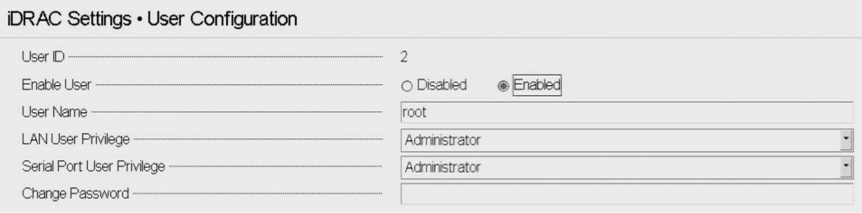
iDRAC Settings

Configure Administrator User Configuration.

Service Tag : 92R2DZ1

Arrow keys and Enter to select
Esc to exit page, Tab to change focus

8. Configure the following User Configuration fields:
    - ***Enable User.*** Verify that this field is set to Enabled.
    - ***User Name.*** Enter a user name.
    - ***LAN and Serial Port User Privileges.*** Set privilege levels to Administrator.
    - **Change Password.** Set a password for user login.



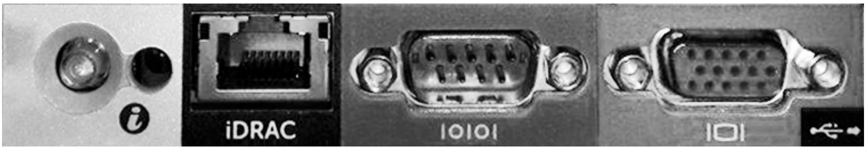
iDRAC Settings • User Configuration

User ID	2
Enable User	○ Disabled ● Enabled
User Name	root
LAN User Privilege	Administrator
Serial Port User Privilege	Administrator
Change Password	

9. Select **Back** and then select **Finish**. Confirm the changed settings. The network settings are saved and the system reboots.

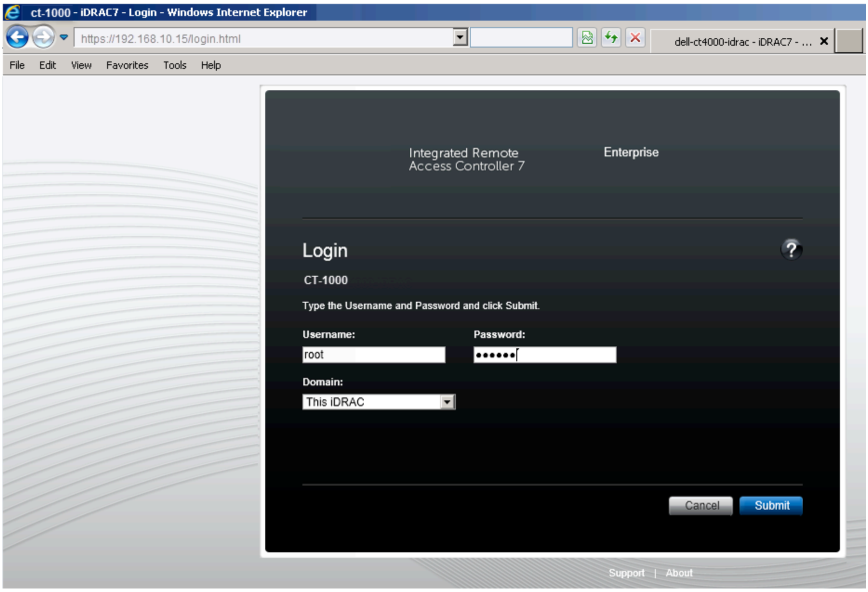
Connect the Module to the Network

The iDRAC connects to an Ethernet network. It is customary to connect it to a management network. The following image shows the iDRAC port location on the rear panel of the CT-1000 appliance:



Login to iDRAC

To login to iDRAC:


ct-1000 - iDRAC7 - Login - Windows Internet Explorer

https://192.168.10.15/login.html

dell-ct4000-idrac - iDRAC7 - ...

Integrated Remote Access Controller 7

Enterprise

Login

CT-1000

Type the Username and Password and click Submit.

Username: root

Password: ••••••

Domain: This iDRAC

1. Browse to the IP Address or domain name configured in **iDRAC Settings > Network.**
2. Enter the Username and Password configured in the User Configuration page of the iDRAC system setup.
3. Select **Submit**.

For further information about iDRAC, refer to the iDRAC 7 User's Guide.

It is very important to update the default credentials.

6. 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.

7. 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 policies 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/7, Linux
- RAM
  1 GB for up to 10,000 devices
  2 GB for more than 10,000 devices
- Disk space — 1GB

Two methods are available for performing the Console installation:

Use the installation software built into your Appliance.

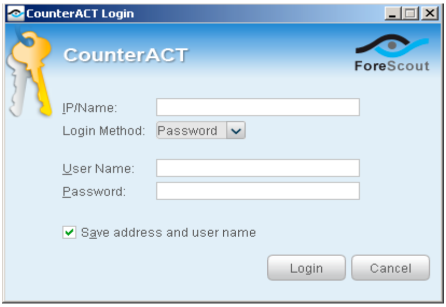
1. Open a browser window from the Console computer.
2. Type the following into the browser address line
   `http://x.x.x.x/install`
   Where x.x.x.x is the IP address of this Appliance. The browser displays the Console installation window.
3. Follow the on-screen instructions.

Install from CounterACT CD-ROM

1. Insert the CounterACT CD ROM into the DVD drive.
2. Open the **`ManagementSetup.htm`** file from the CD ROM with a browser.
3. Follow the on-screen instructions.

Log In

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



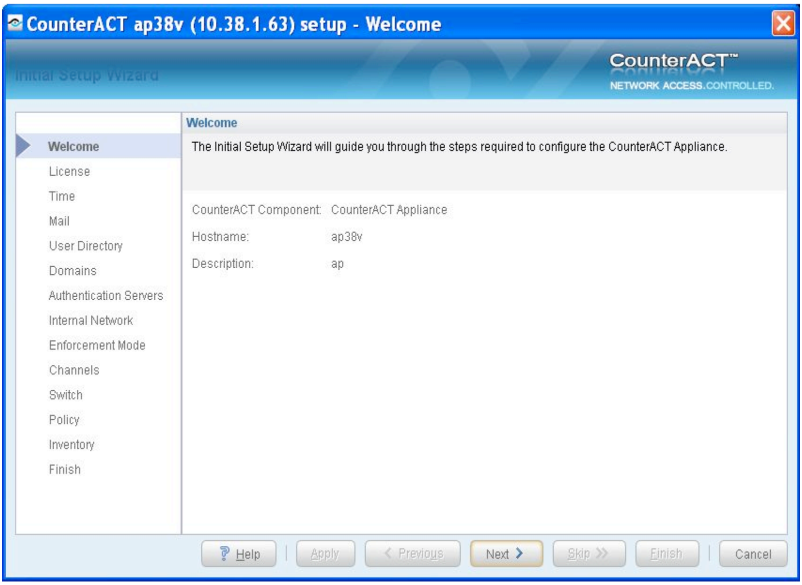
Login Method: Password

☑ Save address and user name

1. Select the CounterACT icon from the shortcut location you created.
2. Enter the IP address or host name of the Appliance in the **IP/ Name** field.
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 launch the 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.



Welcome

The Initial Setup Wizard will guide you through the steps required to configure the CounterACT Appliance.

CounterACT Component: CounterACT Appliance

Hostname: ap38v

Description: ap

Before You Start the Initial Setup

Prepare the following information before working with the Wizard:

Information	Values
□ NTP server address used by your organization (optional).	
□ Internal mail relay IP address. This allows delivery of email from CounterACT if SMTP traffic is not allowed from the Appliance (optional).	
□ CounterACT administrator's e-mail address.	
□ Monitor and response interface assignments defined at the Data Center.	
□ 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.	
□ Core switch IP address, vendor and SNMP parameters.	

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 one of the following numbers:

- Toll-Free (US): 1.866.377.8771
- Phone (Intl): 1.408.213.3191
- Support: 1.708.237.6591
- Fax: 1.408.371.2284

Illustration courtesy of Dell Corporation.

ForeScout Technologies
900 E. Hamilton Ave., Suite 300
Campbell, CA 95008 USA

Toll Free: 1.866.377.8771
Phone (Intl): 1.408.213.3191
www.forescout.com