ForeScout

CounterACT Edge

Single CounterACT Edge Appliance

Quick Installation Guide

Table of Contents

Welcome to CounterACT™ Edge

What if you could stop attackers before they attack your network?

Now you can!

ForeScout Technologies delivers automatic Threat Prevention systems that operate according to a simple, powerful principle: identify attackers before they reach your network and use this knowledge to stop attacks before they inflict damage.

Based on a patented technology, CounterACT Edge provides "Protection by Proven Intent", a process that identifies and blocks attackers — with extremely high accuracy — enabling the confidence to turn on automatic blocking. Simple to deploy and maintain, CounterACT Edge provides dynamic threat protection against known and unknown attacks.

This Quick Installation Guide provides basic installation procedures for the CounterACT Edge Site solution. On-screen instructions on the installation disc will also guide you through the installation.

Notes: *For CounterACT Edge Enterprise solution installation procedures, refer to the CounterACT Edge Installation Guide, located under the /docs folder on the CounterACT Edge disc.*

The CounterACT Edge Site Manager and Enterprise Manager User's Manuals are also included on the CounterACT Edge disc, and provide you with a product description as well as user instructions.

What is Included in the CounterACT Edge Package

- CounterACT Edge
- Quick Install Guide
- CounterACT Edge Installation Disc
- Warranty Document
- Mounting Brackets
- Power Cable
- DB9 Site Manager Connecting Cable
- Rail Kit
- License Request Form

Note: *The CounterACT Edge license key will expire thirty (30) days after the initial installation. To extend your evaluation license or obtain a license for product purchase, contact your reseller or ForeScout representative at support@forescout.com. Licenses will be issued within two (2) business days from the time of the request.*

CounterACT Edge Components

Product Components

The CounterACT Edge site solution consists of the following components:

CounterACT Edge

CounterACT Edge is located outside the perimeter firewall, monitors traffic coming from the Internet for pre-attack activity and engages in dialogs with potential attackers. It also monitors legitimate traffic to the Internet in order to map the protected networks and its services. CounterACT Edge then identifies attackers and blocks them.

Site Manager

The Site Manager is a management application used to control a single CounterACT Edge appliance. Site Manager management tools allow the user to control how CounterACT Edge detects and responds to threats. The Site Manager also enables real–time monitoring and provides tools for analyzing attack events detected by CounterACT Edge. The Site Manager is typically installed on a non-dedicated machine. Refer to the ***CounterACT Edge Site Manager User's Manual*** for information about working with the Site Manager. The manual is located on the CounterACT Edge disc in the /docs directory.

Note: *A CounterACT Edge and a CounterACT Edge Site Manager are required for single CounterACT Edge deployment. You can, however, deploy multiple appliances for enterprise-wide network protection. Refer to the user documentation for more information.*

Topologies and Configurations

Network Topology Options

The CounterACT Edge Site solution protects a single network entry point. This section describes common network topology options, including:

- **Basic** — requires one NIC and an external IP address
- **Stealth** — requires two NICs and an internal IP address

Basic Topology — Single NIC & External IP Address

This is the simplest topology to implement. The single NIC should have an external IP address in order to communicate with the Site Manager and enable features that require communication with the outside world, such as geographic location resolution, time synchronization, etc.

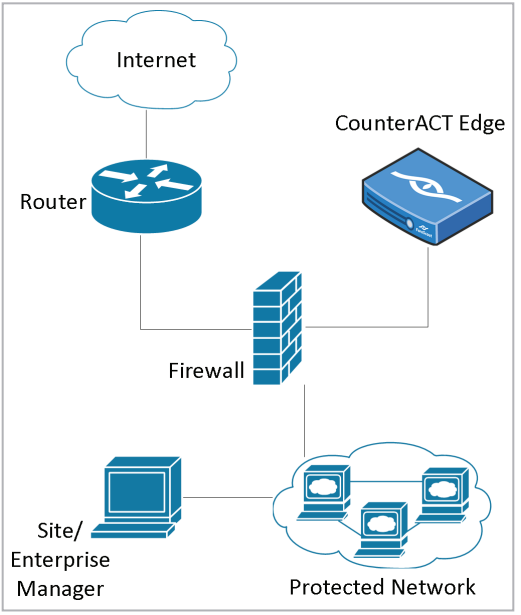


Figure 1: Basic Topology - Single NIC and External IP address

Note: *Refer to the CounterACT Edge Installation Guide for other possible topologies. The guide is located on the CounterACT Edge disc in the /docs folder.*

Stealth Topology — Two NICs & Internal IP Address

This topology requires two NICs.

External NIC

- The external NIC has no IP address (stealth)

Internal NIC

- The internal NIC is assigned an internal IP address and communicates with the Site Manager. The internal IP address should be able to communicate with the Internet (i.e. through NAT) in order for certain CounterACT Edge features to operate (see Pre-Installation Preparations).

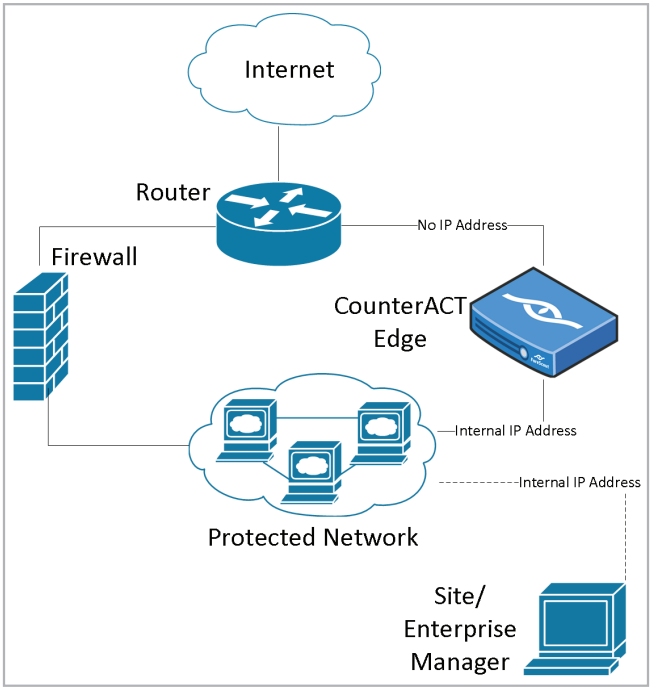


Figure 2: Stealth Topology - 2 NICs & Internal IP Addres

Communication Equipment Interface Options

CounterACT Edge must see 100% of the traffic flowing between the protected network and the outside world. Three common interface options include:

- Using a monitoring ("SPAN") port
- Using a network tap
- Connecting to a hub

Using a Monitoring ("SPAN") Port

In this option, CounterACT Edge is connected to a switch port. CounterACT Edge needs to monitor all traffic flowing between the protected network and the rest of the network. Therefore, the switch port into which CounterACT Edge is connected must be configured to mirror all communication flowing through the switch. This configuration is referred to as copy, mirror, tap, monitor, or span port, depending on your vendor.

In certain switch models (for example, Extreme Networks, Cisco — as of IOS version 12.1), mirroring ports cannot accept the outgoing packets that CounterACT Edge injects. CounterACT Edge requires a way to inject packets into the communication channel. If you are using a switch model with a mirroring port that does not accept incoming packets, you must use an additional switch port for traffic injection into the communication channel. This configuration requires an additional NIC in CounterACT Edge. The NIC that handles the outgoing traffic should have the IP address.

Using a Network Tap

Some switch models do not support mirroring. In such cases, you can monitor all traffic flowing between the protected network and the router by inserting a network tap between the switch and the router. CounterACT Edge is then connected to the tap, therefore monitoring all traffic. For passive taps, you must use an additional switch port for traffic injection into the communication channel. This configuration requires an additional NIC in CounterACT Edge. The NIC that handles the outgoing traffic should have the IP address.

Connecting to a Hub

In this option, CounterACT Edge is directly connected to a hub port. The same hub is connected to the router, therefore allowing CounterACT Edge to monitor all traffic going to and from the network segments that are protected. Do not use a 10/100 auto-sensing hub, unless it is configured to use one speed only.

Pre-Installation Preparations

Network Access Policy Requirements

Deploying the CounterACT Edge Site solution requires TCP/IP communication among the product's various components. Specifically:

- *Management — Port 13000 TCP*
  Allow port 13000 TCP from the Site Manager to the CounterACT Edge management interface, i.e., the NIC that has an IP address.
- *Geographical Resolution — Port 9292 UDP*
  For the geographic rendering of threats, CounterACT Edge consults a geographic database maintained by ForeScout Technologies. Allow port 9292 UDP connectivity between the CounterACT Edge management interface and geo.forescout.net.
- *WHOIS Service — Port 43 TCP*
  For determining source information from WHOIS servers, CounterACT Edge requires WHOIS connectivity (port 43 TCP) from its management interface to the Internet.
- *NTP — Port 123 UDP (Optional)*
  For time synchronization, CounterACT Edge requires NTP connectivity (port 123 UDP) from its management interface to ntp.forescout.net.

Networking Requirements

Required Information

Provide the following information regarding the dedicated CounterACT Edge server:

- CounterACT Edge IP address.
- Subnet mask.
- CounterACT Edge host name.
- Default gateway IP address.
- List of the organization's DNS server addresses — to allow resolving of internal IP addresses to their DNS names.
- Internal mail relay IP address — to allow delivery of e-mail alerts if SMTP traffic is not allowed from CounterACT Edge to the Internet.
- IP address range of the protected network. These are the internal addresses CounterACT Edge will protect.
- Ethernet interface through which CounterACT Edge will monitor traffic to and from the protected network (for systems with two or more NICs).
- Ethernet interface through which CounterACT Edge will send packets to potential attackers (for systems with two or more NICs).

- The network segment to which the monitoring interface is directly connected, as a list of IP address range(s).
- If necessary, VLAN IDs required for CounterACT Edge to handle VLAN-tagged packets and the IP address ranges of the VLANs.
- The network segment/VLANs to which the monitoring interface is directly connected, and a permanent IP address to be used by CounterACT Edge at the specific VLAN.
- E-mail addresses in which to send alerts regarding attack attempts.
- IP address of Site Manager that will be allowed to connect to CounterACT Edge.
- List of IP addresses from which SSH access should be allowed. SSH access allows you to remotely control CounterACT Edge. Allowing broad access to SSH is inherently less secure. It is therefore recommended to limit SSH access.

Setting up CounterACT Edge

Unpacking

Remove the following items from the shipping container:

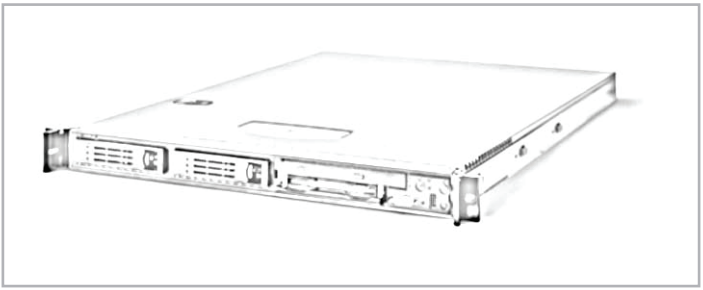


Figure 3: CounterACT Edge Appliance

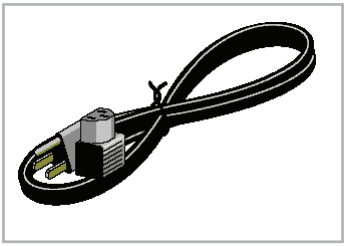


Figure 4: Power Cord

Powering up CounterACT Edge

Complete the steps below to power up CounterACT Edge:

- Connect the power cable to the power connector on the appliance's back panel. See Connecting CounterACT Edge to the Network for more information.
- Connect the other end of the power cable to a grounded AC outlet.
- Setup the keyboard, mouse and monitor to the appliance or set up CounterACT Edge for serial connection. Refer to the ***CounterACT Edge Installation Guide*** for information about setting up a serial connection.
- Power up the appliance from the front panel.

Note: If the appliance is installed at the location at which it will operate, it is recommended that it be connected network now. For information about performing this connection see Connecting CounterACT Edge to the Network. If the appliance is not at this location, continue with the CounterACT Edge configuration and later connect CounterACT Edge to the network. After network connection, perform a network connectivity test. Refer to the Site/Enterprise Manager User manuals for information about this test.

Configuring CounterACT Edge

After CounterACT Edge is powered up, a prompt appears to start the configuration.

1. The following message appears:
   CounterACT Edge 3.2.X boot is complete.
   Press <Enter> to continue.
2. Press <Enter>. The following menu opens:
   1. Configure CounterACT Edge-3.2.X
   2. Restore saved CounterACT Edge-3.2.X configuration
   3. Identify network interfaces
   4. Configure keyboard layout
   5. High Availability Setup
   6. Turn machine off
3. During CounterACT Edge configuration, you are asked to choose network interfaces by their logical name (eth0..). Select option 3 (Identify network interfaces) to identify all network interfaces and their logical names.
4. After identification of the network interfaces is completed, choose option 1 – Configure CounterACT Edge Appliance.
5. Press <Enter>. The CounterACT Edge Component selection prompt appears.
6. Type 1 at the prompt and press <Enter>. A message appears indicating that you are about to install CounterACT Edge. Press <Enter> to continue.
7. At the prompt Appliance Administrator Password: enter the password for the root user and press <Enter>.
   This password is used to login as "root" to the CounterAct Edge appliance, and as "Admin" to the Site Manager.
8. Retype the password at the prompt that follows and press <Enter>. The user will need the root credentials when connecting to CounterACT Edge via SSH.
9. At the prompt Setting Time Zone: define a time zone by geographic location or by GMT offset. At the prompt: Set time-zone to XXX? (yes/no) [yes] : press <Enter> to accept the defined time zone. The system time is configured.
10. At the prompt: Are the date and time accurate (yes/no)?: type yes (if accurate) and press <Enter>.
11. At the prompt Host name: assign a hostname to CounterACT Edge that is unique within the user's organization, and press <Enter>.
12. Now enter network parameters. After each parameter is defined, press <Enter> to continue.

13. At the prompt DNS Domain Name, enter the domain name required, machine domain name [your.domainname.com]: and press <Enter>.

14. At the prompt DNS server addresses ('none' for empty list): enter the required address. The DNS should be able to resolve internal IP addresses.

    An evaluation license is now set for 30 days. A permanent license must be installed before this period expires. An e-mail will be sent regarding the expiration date. See the CounterACT Edge Site/Enterprise Manager User's Manual located on the CD in the/docs folder for information about installing the license.

15. At the prompt Protected Network: type the range of internal IP addresses of the network that CounterACT Edge will protect, including all unused internal IP addresses. Press <Enter>.

16. A channel is a pair of logical interfaces (Monitoring and Outgoing) that are used by CounterACT Edge to attach to a network segment. The monitoring interface is used to monitor network traffic going to and from the protected network segment, while the outgoing interface (which may or may not be the same as the monitoring one) is used to send packets generated by CounterACT Edge. There is a prompt to define a single channel.
    Additional channels and VLANs can be configured. These tasks are performed from the Configuration dialog box, accessed from the Settings menu. Refer to the CounterACT Edge Site/Enterprise Manager User's Manual for more information.

17. At the prompt Monitoring interface (one of: eth0, eth1. eth2, eth3): enter the Ethernet interface that monitors traffic to and from the network protected by CounterACT Edge and press <Enter>.

18. At the prompt outgoing interface (one of: eth0, eth1, eth2,) [eth1]: enter the interface that will be used by CounterACT Edge to send packets back to potential attackers, and press <Enter> or just press <Enter> to accept the default. The default is the same as the monitoring interface. In most cases, this is the same as the monitoring interface. An exception is when the monitoring interface is connected to a switch that is unable to receive packets on a monitor (copy) port (e.g. some Extreme Networks switches).

19. Now choose mark language settings. At the prompt: Choose locale: 1. English, 2. French, 3. German 4. Hindu 5. Italian 6. Japanese 7. Spanish. Choice (1-7) [1]: select <Enter> to generate marks in English, or type in another option and select <Enter>.

20. There is now a request to set CounterACT Edge policy regarding attack attempts detected by CounterACT Edge. At the prompt Choice (1-3): enter a value and press <Enter>, or just press <Enter> to select the default value.

21. At the prompt Enter bandwidth of outgoing connection in KB per second: type the value you need, and press <Enter>.

22. At the prompt Mail relay address ('none' to disable mail-relay): type the full qualified host name, and press <Enter>.
23. At the prompt Administrator e-mail address: type an e-mail address(es) to send alerts when an attack event occurs and press <Enter>.
24. At the prompt Would you like to check your E-mail settings now (yes/no)? [yes]: select <Enter> to send a mail test. Or, if you do not want to send the test, type no and press <Enter>.
25. At the prompt List of IP addresses allowed to access this CounterAct Edge Appliance (Site Manager): type the IP address(es) of the Site Managers that are allowed to connect to and manage CounterACT Edge. Press <Enter>. (If the desktop's IP address is not in this range, the user will not be able to manage CounterACT Edge. If the Basic Topology is deployed and the user's desktop is behind a NAT device, make sure that this NAT IP address is included in this list.)
26. At the prompt List of IP addresses allowed to access SSH (none to disable SSH): indicate the IP addresses of computers allowed to access CounterACT Edge through the SSH protocol, and press <Enter>. Enter a list of addresses separated by spaces. You cannot enter a range of addresses . Alternatively, select <Enter> to disable external control through SSH.

Note: If the "geotest" failed, make sure CounterACT Edge is connected to the network.

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 to CounterACT Edge. Use the module to carry out KVM access, mount remote installation media, power on/off/reset and perform troubleshooting and maintenance tasks.

Perform the following to work with the iDRAC module:

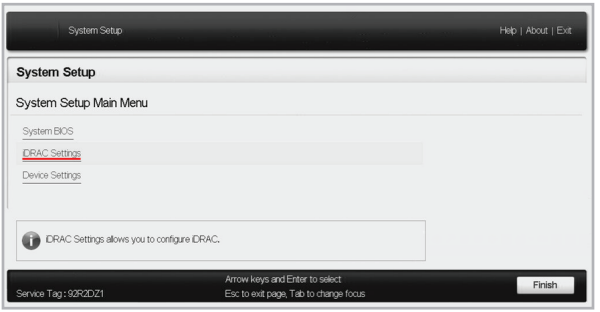
1. Enable and Configure the iDRAC Module
2. Connect the Module to the Network
3. Login to iDRAC

Enable and Configure the iDRAC Module

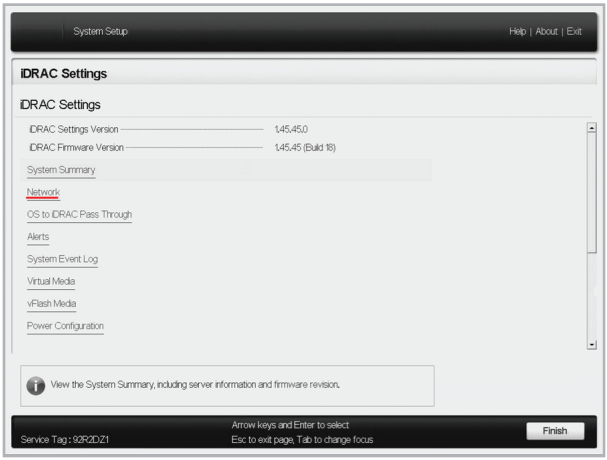
Change the iDRAC settings to enable remote access on CounterACT Edge. This section describes basic integration settings required for working with CounterACT.

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.



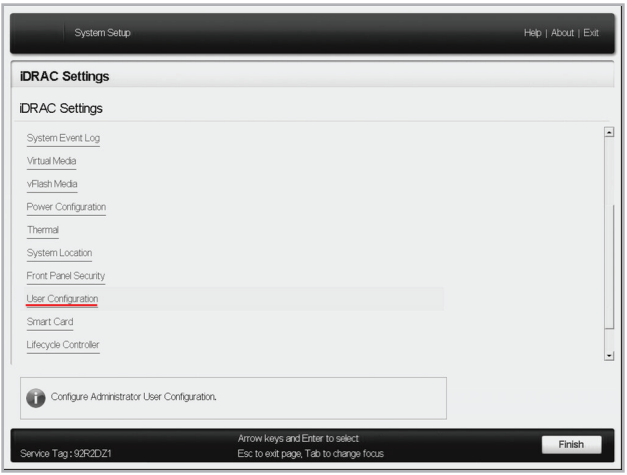
4. In the iDRAC Settings page, select Network.



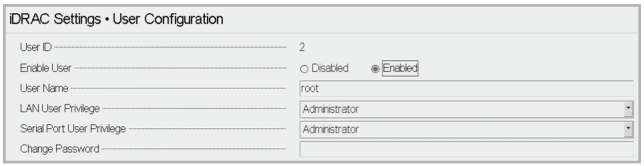
5. Configure the following Network settings:
   - Network Settings. Verify that the Enable NIC field is set to Enabled.
   - Common Settings. In the DNS DRAC Name field, you can update a dynamic DNS (Optional).
   - IPV4 Settings. Verify that the Enable IPv4 field is set to Enabled.

     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.

6. Select Back.
7. Select User Configuration.



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. Make sure you set a password different from the supplied default.



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

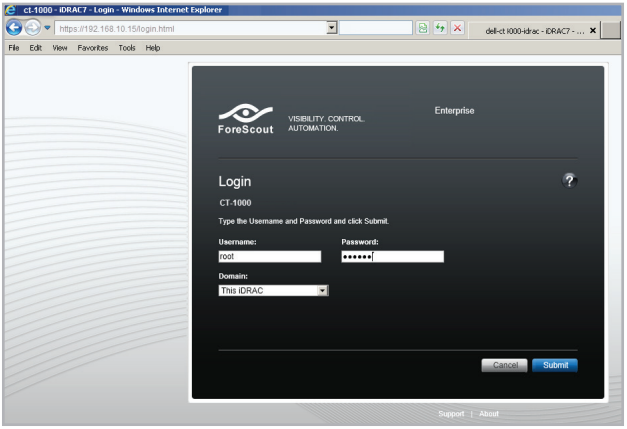
Connect the Module to the Network

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:

1. Browse to the IP Address or domain name configured in iDRAC Settings > Network.



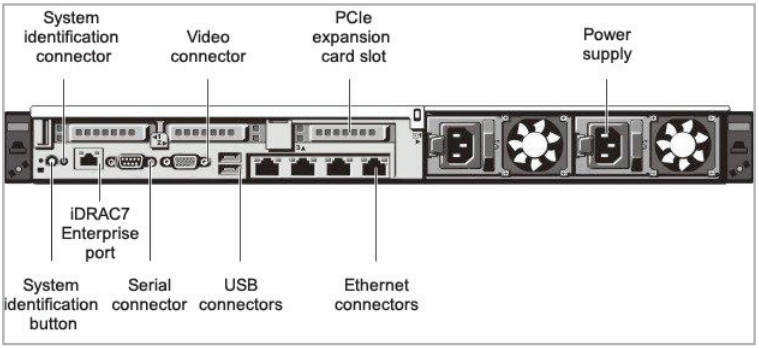
2. Enter the Username and Password configured in the User Configuration page of the iDRAC system setup.
3. Select Submit.

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

Connecting CounterACT Edge to the Network

During CounterACT Edge configuration there is a request to specify the Ethernet monitoring interface and outgoing (injection) interface. Once these parameters are determined, connect the interface cables to the associated Ethernet port on the back panel of the appliance.

Back Panel Sample



Installing the Site Manager

Installing the Site Manager

1. Insert the CounterACT Edge disc into the drive.
2. Open the AS_management_setup.htm file from the disc with a browser.
3. Follow the on-screen instructions.

Logging In

After completing the installation, log in to the Site Manager from the shortcut location created during the installation.

1. Select the Site Manager icon from the shortcut location you created.
2. In the Scout Address field, enter the IP address or host name of the CounterACT Edge appliance.
3. In the User field, enter desired user name (default: Admin).
4. In the Password field, enter the password defined in the CounterACT Edge installation process.
5. Select Login to open the main window of the Site Manager.

Note: The system is installed with a predefined "Admin" user. The Admin user password and Scout address are defined during CounterACT Edge installation. However, the password can be updated using an external management utility. Refer to the CounterACT Edge Site Manager User's Manual for more information regarding the utility or for more detailed information about how to use the Site Manager.

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

CT-E3.2.1-QIG01-May-14

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

400-00040-00