CounterACT Installation Guide

Versions 6.x.x

POC Name:	
Email:	
Phone:	
Customer Address:	
Delivery Dates:	

Company Proprietary Information

COUNTERACT™ INSTALLATION

STEP-BY-STEP GUIDE

GETTING STARTED

Read and complete the following steps to install the CounterACT appliance onto your network.

Please refer to the Help boxes, Appendices, User Console Manual, and your network equipment's user guides for additional help and documentation. This guide was designed as a standalone help to install CounterACT with the basic plugins and policies configured.

1. Complete the Customer Evaluation Checklist.

The Customer Evaluation Checklist helps you gather essential information before you start.

See Appendix A for an abbreviated version of the Evaluation Checklist.

---

2. Rack-mount the appliance.

3. Configure the switch.

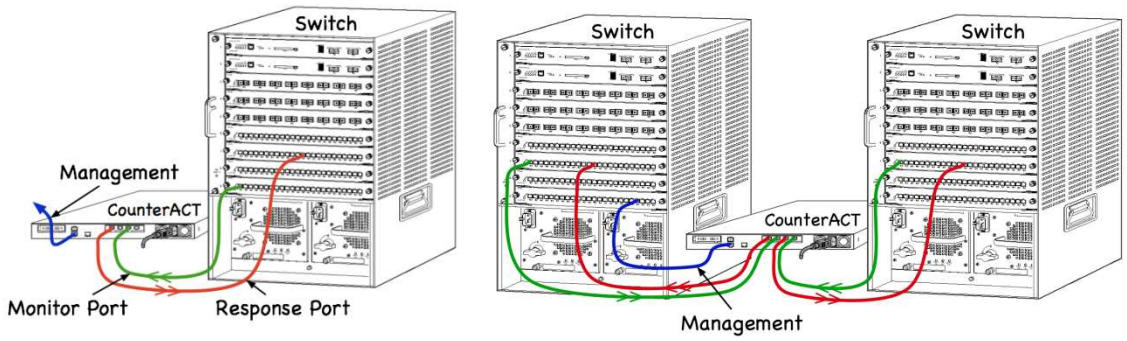
The CounterACT appliance is generally configured with three connections to the switch.

1. **Monitor Port:** This trunked and tagged connection allows CounterACT to watch traffic on the wire. Include the VLANs you wish to monitor. Make sure to span both in/out traffic.
2. **Response Port:** This trunked and tagged connection allows CounterACT to redirect browsers, send resets, and spoof addresses. Include the same VLANs used for the Monitor Port.
3. **Management Port:** This connection serves as the management interface, and additionally queries and communicates with hosts, switches, and other infrastructure according to the plugins you install and configure.

Help with this step:

Refer to Appendix B at the end of this guide for example switch configurations.

Make absolutely sure to set up the Monitor, Response, and Management ports as they are discussed here.



If the switch is one of a redundant pair, traffic from both switches must be mirrored to the same CounterACT appliance as illustrated in the configuration on the right. Configure both switches in exactly the same manner, with Monitor and Response ports on each switch.

SWITCH CONFIGURATION GOTCHAS

Take the time to read through the following list. Proper switch configuration is essential.

Be careful with your switch configuration!

Setup

- If the switch to monitor is redundant, then both switches must be monitored.
- If the switch cannot mirror in/out, then either [1] monitor the entire switch (this provides in/out) or [2] monitor just one port (which does allow in/out)
- Some switches (e.g. Cisco 6509) may need old port configurations completely cleared out before entering new configurations. The most common result from not clearing out old port information is that the switch strips 802.1q tags.

Tags

- If the monitored traffic is from a single VLAN then traffic doesn't need 802.1q tags.
- If the monitored traffic is from two or more VLANs then BOTH the monitored and response traffic must have 802.1q tagging enabled.
- If the switch cannot VLAN tag the Monitor port then mirror only a single VLAN or mirror a single, untagged uplink port.
- If the switch can only mirror one port, then mirror a single uplink port. This may be tagged. In general, do not mirror a trunked port if the switch strips the tags or you will hinder the full capabilities of CounterACT.

Appliance Sizing and Port Capacity Chart

	CTR	CT-100	CT-1000	CT-2000	CT-4000
Concurrent Devices	50	250	1000	2500	4000
Bandwidth	100Mbs	100Mbs	1Gbs	2Gbs	4Gbs
Copper Ports	4	6	8	8	8
Fiber Ports	N/A	Avail up to 2	Avail up to 4	Avail up to 4	Avail up to 4
VLAN	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited

This initial command line and setup wizards guide you through the basic setup required to connect CounterACT to your network. CounterACT is highly customizable, and additional recommended setup options and information on creating NAC policies are located later in this document.

You can configure the initial command line setup using a connected monitor and keyboard or by using a serial connection. See Appendix D for more information on using a serial connection.

4. Complete the Command Line Interface (CLI) setup

First, **Select Option 1) Configure CounterACT-6.x.x.** Next, **select YES and then select Option 1) CounterACT Appliance** to begin the installation.

Separate multiple values using a space or **enter a range** using a dash.

Use the following table to guide you through the command line installation questions. Obvious settings are not discussed below in order to keep this guide short.

STEP	SETTING	NOTES
Administrator Password	See note.	Use this password for logging into the client GUI, the web portal, and the console. You can set separate root and administrator passwords later if necessary. See Appendix D.
Management Interface	eth0	Most installations use eth0 for management.
DNS Server Addresses	See note.	**Always use an internal DNS server.** The listed DNS server should be able to resolve internal IP addresses. **Put DNS servers in order of internal to external.** While most internal DNS servers may resolve external addresses as well, some may not, so it may be necessary to include an externally-resolving DNS server at the end of the list. 99% of DNS queries by the CounterACT will be for internal addresses, so the **internal servers should be listed first.**

5. Verify proper connectivity prior to leaving the data center.

Verify the configuration works as expected prior to leaving the data center. Once CounterACT has started, log in as root and perform the following tests. You should resolve any issues before continuing if any of these tests fail.

FSTOOL IFCOUNT

Verify the switch configuration from the CounterACT console using `fstool ifcount`:

```
[root@CounterACT root]# fstool ifcount eth0 eth1 eth2
```

- **The Monitor Port** should have primarily UNICAST traffic – and lots of it.
- **The Response Port** should have primarily BROADCAST traffic (with some UNICAST).
- The **Monitor** and **Response Ports** should display the expected VLANs.

FSTOOL LINKTEST

Run the following command to test the configuration and connectivity of the Management Port:

```
[root@CounterACT root]# fstool linktest
```

- Check the duplex setting!! Half duplex can kill a connection without warning.
- Check speed of all interfaces.
- Gateway test may fail ping, but succeed with arping
- If gateway ping fails, ask for IP that will answer to ping.
- If gateway arping fails, something is wrong with IP address, mask and gateway.
- DNS to forescout.com may fail if there is an internal-only DNS
- Use `host [IP Address]` lookup to validate DNS manually

6. Connect to CounterACT using the Console client.

You can download the client GUI (Graphical User Interface) from the appliance using a web browser or install the client from the CD under the `InstData` directory. Use the default settings and installation paths during the GUI installation process.

http://CounterACT IP Address/install

The **Admin password** is used for logging into the appliance when using the GUI client and for logging into the web portal. Refer to Chapter 2 of the Console-User-Manual for a short tour and more information covering the GUI console.

7. Complete the CounterACT Initial Setup Wizard

Use the following table to guide you through the Initial Setup Wizard.

STEP	COMMENTS
Time	• If the time is set incorrectly, the enterprise manager may not synchronize properly with the appliance.
Mail	• The appliance will send alert emails using its own internal SMTP server. If your network requires all mail servers to use a mail relay, please configure it to receive emails from the appliance IP and enter the relay address here. • If a mail relay is used, it may be necessary to configure the mail relay to allow incoming mail from the CounterACT IP. • If in doubt, deselect the mail relay setting . This can always be changed later.
LDAP	• This step allows CounterACT to query Active Directory or LDAP for information. **Skip this step** if using a local account to query the endpoint (this is not common). • The **Fully Qualified Domain Name** (FQDN) does not include the name of the server. Correct examples include MYCOMPANY.COM, MILITARYDOMAIN.MIL, PUBLIC.GOV, and SCHOOLDOMAIN.EDU. Use capital letters when you enter the FQDN. • This is often the same account used for the Host Property Scanner. You can use a user account with read access to Active Directory. • Verify you can read information using the test feature under Configuration in the main console,
Domains	The step allows CounterACT to query the endpoint for information. 1. Enter the appropriate Domain Administrator (username), Domain Name (mycompany.com), and Domain Password (make sure this is correct!) for each set of credentials you would like to use to access the host. 2. This account may be a service account that is part of the host's Administrators Group. You can verify CounterACT can query hosts using the test feature after the setup wizard is completed under Main Console | Options | Plugins | Host Property Scanner | Test.
Authentication Services	• Set the Authentication Servers information to allow CounterACT policy to verify that network hosts were properly authenticated. It's recommended to define all valid Authentication Services that exist in your network such as AD, LDAP, Mail, and others as appropriate. • Add **Mail** servers by entering the **IP Address** and selecting the appropriate **Port** such as **MAPI(0/TCP), IMAP(143/TCP), or POP3(110/TCP)**. You can

	add the same server more than one time looking for different authentication events on different ports. • **Add LDAP or Active Directory** servers by entering the **IP Address** and selecting the appropriate **Port** such as **Microsoft-DS(445/TCP).** • Make sure to add comments for every server added.
Internal Network	• The Internal Network defines the: 1. Network range CounterACT can interrogate for NAC Policies. 2. Default network range with IPS Detection and Protection. ▪ This was previously called the Protected Network and is now called the Active Response Range. ▪ See **CounterACT Options | IPS Policy | Advanced | Active Response Range** from the main console to change the scope of the Active Response Range. 3. Default network range for Auto-Discovery policies. ▪ See **CounterACT Options | Discovery** from the main console to change the scope of the Discovery Policies. • Enter an appropriate address range scoped for the evaluation or installation. These are typically user segments. • Avoid including internet routable addresses unless they are truly a part of the network. • Address ranges must be assigned to an appliance when using the Enterprise manager for active Policy and Auto-Discovery interrogation.
Operation Mode	• You can leave this in **Normal Mode** in most cases. **Listen Only Mode** disables the packet engine for IPS marks and the Virtual Firewall capabilities. • NAT detection is an active technology and the default is to NOT use it. • Disable Auto Discovery if you have a requirement to prevent CounterACT from interrogating hosts or you need to define your own Discovery options.
Channels	1. Select **Channel | Add** and then **select your Monitor and Response interfaces** for the first channel. 2. The Advanced options allow monitoring tagged or untagged traffic. 3. **Select Enabled** checkbox after adding each of the channels.
Switch	1. Select **Add.** 2. Enter appropriate information using the following as a guideline: a. **IP Address** of the switch b. **Connecting Appliance** will be the CounterACT box responsible for communicating with the switch. c. Select the **switch vendor** and **SNMP version** (e.g. 1, 2, 3)

	d. **RO or RW Community string**: Either will work for READING information. We need the RW community string to switch block or move hosts into different VLANs. Notice the second text box for entering the string again for confirmation. e. **Switches** need the **three Read options** under the Permissions section and the **Write option** if you want to enable the actions switch block or assign to VLAN. f. **Routers** only need the third option selected, **Read – Query switch ARP table for new hosts**, which lets CounterACT learn host MAC addresses from the Router. g. The **auto-discovery** feature is available for Cisco, HP, and Nortel switches. HP and Nortel switches can perform dual discovery, meaning that they can discover Cisco switches. Discovered switches are not enabled by default. 3. **Close, save settings**, and **run the Test**. 4. You can select multiple switches, right click, and change parameters across the selected switches. 5. Refer to the plugin documentation for more details if needed.
Finish	• Review the results of the Initial Setup Wizard and **select Finish**.

8. Check for updates.

Verify the plugins are the most current version available by navigating to **Tools | Check for Updates**. The update icon will indicate that there is an update available by appearing in the lower left hand corner of the GUI console.

9. Review steps for legitimizing traffic and reducing false positives.

Take the time to look through Malicious Sources in the main console and legitimize them by hand as necessary. Your attention here will greatly reduce the likelihood that CounterACT will interfere with **legitimate events** on the network.

CounterACT is equipped with a powerful IPS engine that requires some minimal tuning. Find the **Network Policies viewing pane** in the main console and **select IPS**.

Begin by selecting a known good host that appears as a Malicious Source. **Right click one of these hosts | select Exceptions | Add to Legitimate Traffic.** The Source Address is the host you right-clicked. **Enter an appropriate Target Address, range, or segment. Verify the Service Port information, add comments, and select OK.** These are then added to the Legitimate Traffic list located under **CounterACT Options | IPS Policy | Legitimate Scan.**

Help with this step:

Consult the **Console User's Guide** for more information about how the IPS works, including legitimizing necessary traffic and reducing false positives.

COMMON SCANNING ENTERPRISE APPLICATIONS

Known good applications should be legitimized by the administrator. You can trigger CounterACT to see a host as malicious using GFI LanGaurd (http://www.tucows.com/preview/213719) or by using ForeScout's Worm Simulator. If these tools don't trigger a malicious event then you should review your installation (e.g. switch configuration, logical channels (VLANs) enabled.

USING THE LEGITIMATE TRAFFIC TUNING WIZARD

You may have to wait several hours after the initial installation before CounterACT has enough data to effectively run the Tuning Wizard. This is another powerful tool and greatly reduces false positives over time. Run the Legitimate Traffic Tuning Wizard periodically by navigating to **CounterACT Options | IPS Policy | Legitimate Scan.** Choose the **Tuning Wizard** and follow the prompts.

NOTES ABOUT DISABLING THE IPS

You can rapidly shut off CounterACT's IPS three different ways: [1] place CounterACT into Listen Mode, [2] stop the CounterACT service, or [3] disable the response port:

- **Listen Only Mode**: **CounterACT Options | General | Operation Mode**
- **Stop the CounterACT service**:
  - From the Console: **CounterACT Options | Appliance | Stop …or…**
  - From the Command line: `fstool service stop`
- **Disable the Response Port**:
  - **Unplug the physical response cable …or…**
  - Command Line: `ifconfig eth2 down` (assumes eth2 is the response port)

10. Add Network Segments.

Create network segments and name them accordingly. This is an excellent way to show value because it ties the hosts in the interface to specific network segments.

1. Find the **Network Segments** viewing pane in the main console, **right click All IPs** and **select New**.
2. **Name the segment** and **enter IP addresses** for that segment
3. **Repeat the process** for each segment you would like to add
4. **Network segments can be nested**. Create the hierarchy up front, starting with the largest container (e.g. Rochester Building) and then creating the member containers underneath it (e.g. Rochester 1ST Floor, Rochester 2ND Floor, etc..)
5. **Network segments will act like a filter for viewing information in the main viewing pane**. You can try this by selecting All under Network Policies and then selecting different Network Segments. *Don't forget to select All IPs if you want to see everything in the main viewing pane! The Network Segments act as a filter so that if you select any of the segments then you are limited in what you can see under the policies by the scope of that segment.*

11. Customize Network Host Discovery Options.

Navigate to **Policy | Discovery** to enter the Network Host Discovery Manager. This is where you define the information CounterACT automatically gathers for each host, regardless of whether a policy is set for that information or not.

1. You can disable the default policy by deselecting the checkbox.
   a. You cannot change the default discovery options, but you can disable them.
   b. View selected discovery options by highlighting the policy and selecting Edit.
2. You can create a new Host Discovery Policy by selecting Add using the wizard. Remember that you can create custom discovery options for different portions of the network using the network segments you created in the previous step.

12. Customize HTTP NAC Preferences

CONFIGURE HTTP PROXY TO ALLOW CHECKING FOR UPDATES

You may have to add proxy information **only if an HTTP proxy is used** to access the Internet you're you have updates available and you already installed them then you do not need to configure this. Navigate to **CounterACT Options | Console | HTTP Proxy** and enter your proxy settings here.

MONITOR HTTP PROXY PORTS FOR HTTP REDIRECT

Navigate to **CounterACT Options | NAC | HTTP** tab:

1. **Enable Let Me In**
    a. **Select Enable Let Me** checkbox and enter a **password**
2. **Monitor Proxy Ports**
    a. **Select Monitor Proxy Ports** for **HTTP Notifications** and enter **any appropriate ports you may use for your network.** If the organization is configured to access the Web through an HTTP proxy, you must configure the proxy in order to perform HTTP redirecting.

CREATE EXCEPTIONS FOR THE HTTP REDIRECT

Go to **CounterACT Options | NAC | HTTP tab | HTTP Hijack Exceptions. Select Add** and enter in the appropriate URL information. The Text field is looking for URL information – NOT an IP Address.

CUSTOMIZE THE HTTP REDIRECT WEB PAGE

You can customize the header and footer of the HTTP redirects, and even apply your own style sheet to match the look and feel of your company's web pages. There are two methods to do this:

Navigate to `https://CounterACT_IP_Address/precustomize`. Select Advanced if you would like to add your own HTML code to the header and footer of the CounterACT messages shown to end users. Changes made to the header and footer are maintained when performing software upgrades.

See Appendix D for advanced methods you can use to customize the HTTP redirect web page. These should only be used by knowledgeable administrators.

13. Integrate CounterACT Logon with Active Directory

Navigate to **CounterACT Options | Users | Single Sign-On Server** and enter the appropriate LDAP information. You can then test the CounterACT logon integration with Active Directory using your username and password.

Add Active Directory users and their privileges to CounterACT by navigating to **CounterACT Options | Users** and **select Add**. Fill in the appropriate username and password information and then select the Authenticate with LDAP Server option.

14. Optional CounterACT Settings

You may find the following settings or options helpful. Some of these provide additional functionality, solve particular business concerns, or improve the performance of CounterACT.

A. EMAIL SERVER LEARNING

CounterACT by default will attempt to learn the email serversWe sometimes find customers prefer to identify their own email servers and you may want to disable this feature. Navigate to the Main Console | Options Button | IPS Policy | Legitimate Email and uncheck Enable Auto learn Email server if you would like to disable this feature.

B. SECURE CONNECTOR

The SecureConnector is the name of the available client. There are several methods available for deploying the SecureConnector. The purpose of the SecureConnector is to establish a secure encrypted connection between the host and the appliance that allows CounterACT to query the host without using domain credentials.

1. Experiment with and install the Secure Connector by visiting http://Appliance-IP-Address/sc. Note the options for persistence and the system tray icon. You can also use this link for guests on your network.
2. Deploy the Secure Connector using any standard software deployment mechanism by downloading the executable from http://Appliance-IP-Address/sc. Keep the name intact when you download the file.

C. HOST PROPERTY SCANNER PERFORMANCE TUNING

Host Property Scanner Tuning Values

Performance Tuning Parameters	CT4000	CT2000	CT1000	CT100	CTR
Concurrent Property Scanner Processes	150	100	50	30	15
Concurrent NMAP Processes	50	30	20	10	5
Concurrent MS Processes	150	100	50	30	5

15. Learn how to configure NAC Policies.

NAC Policies quickly add value and help administrators answer questions about manageability, compliance, and device inventory.

The steps and policies below are discussed at a very high level and designed to illustrate how NAC Policies are created.

Help with this step:

Start with **clicking the Help icon** in the upper far right of the NAC Policy Manager. This catapults you straight into **Chapter 10: NAC Policy Management of the Console-Users-Manual**.

How to Build Policies

1. Click the **NAC Policy Icon** in the main console to open the Policy Manager.
2. Click **Add** to start a new policy and follow the guidelines below.

POLICY STEP	COMMENTS
Name	• Keep the name short and add any necessary comments.
IP Ranges	• Consider the IP Range as the scope of the policy. • You can enter multiple ranges or specify a single IP address. • Use Network Segments as much as possible.
Trigger	• The Trigger defines when the policy is activated to force a check or recheck of a host. Some of these can include: DHCP request, IP Address change, New IP detected, New VPN user detected, Secure Connector connected, 802.1x admission event, Switch port change, MAC address -IP address pairing change, NetBIOS host identity change, and timed events. • **Decrease** the periodicity or remove the **continual check** unless you feel it's necessary to continually *check every device that does not match the top level policy or one of the sub policies*. • Notice the options under the Customized setting. The option to **Activate on Any Admission** includes each of these. • All "Event Conditions" under the Conditions section of the policy will act as real-time triggers.
Conditions	• Each condition has the option to MEET or NOT MEET (match or not match) the criteria you specified in the condition statement.

	• 'AND' and 'OR' statements along with brackets allow you to group conditions using Boolean logic. • Each condition has options for how to evaluate irresolvable criteria. For example, if we cannot log into a host to verify a condition, you can choose how to treat that host. Make absolutely sure to define what to do with irresolvable results when working with sub-policies. This is defined at the bottom of each of the conditions with *Evaluate Irresolvable Criteria* as (Matched) or (Unmatched). • Device Classification Tip: You can add any **groups created** as a result of a policy to the conditions of the same policy to ensure anything you add to groups manually show up under matched hosts for your classification policy. • Use the simple construct of **.*** to create a wildcard and check the regular expression box. The **<dot>** means any character, and the **<asterisk>** means any number of the preceding character. • **Domain User** and **NetBIOS properties** use a combination of host registry queries using the Host Property Scanner, NetBIOS Scans, and watching traffic to determine Domain, Host, and User properties. • **NMAP OS** and **Network Function** use passive fingerprinting first and then NMAP as necessary. Console indications of NMAP properties when you never ran NMAP are from passive fingerprinting. • **LDAP queries** are lightweight and have little impact on the network.
Actions	• Leaving this empty will perform an audit of the conditions you select. • Notice the Recheck Policy button. This is used to define how often you want to recheck hosts that *have already matched* the conditions you specified. The default time-based recheck is every 30 minutes. Change or disable the time-based recheck as you see fit. • You should generally leave the Recheck on any admission selected. • If you use the Action: Add to Group feature, then you generally should also add this as a condition to the policy to look for the group the policy is built for. This sounds like circular logic, but it allows you to see any devices manually added to the group.
Sub Policies	• Sub Policies cascade, like a waterfall or hierarchy from top to bottom. As soon as they match a set of conditions defined by a sub-policy then the policy stops for that device. Hosts that don't match the top or previous rule will be addressed by the next Sub Policy. • Sub Policies should be placed in order of Size (number of expected matches) and then Cost (expected processing hit). Sub-policies should apply to the largest groups first, and then use sub-policies that have the lowest overhead processing cost for CounterACT and the network. Consult with your local ForeScout engineer to fine-tune policies for large deployments.

	• Make sure to move and adjust the order of the Sub Policies as necessary to get the results you need. • **Evaluate Irresolvable sub policies as UNMATCHED.** Define what to do with irresolvable results when or the irresolvable endpoints will not move to the next sub policy working with sub-policies. Some conditions cannot be resolved with the information CounterACT has about the host. Define how to handle these situations at the bottom of each of the conditions using *Evaluate Irresolvable Criteria* as (Matched) or (Unmatched).
Advanced	• Leave the settings in the Advanced tab at their default values for new installations. • Click on the Exceptions button and become familiar with different ways to exclude a host. Notice that Groups can be used (and created) under the Groups tab.

CREATING A NAC POLICY FRAMEWORK AND TUNING NAC POLICIES

The NAC framework hinges on the correct identification of end points, adding end points to groups, and then performing actions on the group's members.

- Carefully read the comments in the Guidelines for Building Policies table.
- In a large site you can set the number of process threads to be in the hundreds to help speed things up. This is set under Options | Host Property Scanner | Tuning | Concurrent Property Scanner Processes.

16. Learn how to use Groups for classification and policy exceptions.

Select Groups in the **main console** or the **NAC Policy Manager** to open the **Group Manager**.

Groups can be used as containers for classified endpoints or policy exceptions. Add any groups created as a result of a policy *to the conditions of the same policy*. This ensures anything you add to groups manually show up under MATCHED hosts for that policy.

USE IP ADDRESS GROUPS

Use IP Address groups in situations where we may not know the MAC address. If you don't have the MAC address then the add-to-group action for a MAC group will fail.

The groups in CounterACT are dynamic when you use the option "*Remove from group when host no longer matches policy*" under the policy Action | Add to Group. Note you can manually add devices in the main console to groups by selecting devices and choosing Group | Add to Group.

BUILDING EXCEPTIONS

Create groups using the Group Manager and then use those groups as exceptions in your policies. Navigate to the Advanced tab when creating policies to view your exceptions. You may even want a separate policy that automatically adds users to the new group based on criteria you select.

17. Determine whether hosts are Domain Members.

Begin a new policy by selecting NAC Policy | Add. After defining the Name, IP Range, and Trigger for your policy, select the condition **Windows OS | Domain Member**. There may be additional options that work in your environment for identifying domain members such as watching for Authentication Events and verifying information using the Secure Connector.

OPTIONS FOR HANDLING NON-DOMAIN MEMBERS

There are several ways our customers handle managed and unmanaged hosts, depending on their internal policies and needs. **Some** of these include:

- Move host with VLAN reassignment to a restricted VLAN.
- Block host with Virtual Firewall (VFW) to prevent access to sensitive resources
- Force domain logon through an HTTP hijack
- Force local host logon through an HTTP hijack
- Block user with an OPSEC compliant firewall
- Block user at the switch from accessing the network at all
- Notify administrator with email
- Add user to a group to be managed later or for reporting purposes
- Ignore the host based on host properties such as the MAC address

18. Determine host compliance to corporate policy.

CONFIGURE HOST CONNECTIVITY

There are two methods ForeScout uses to access information on the host. The first method is clientless and requires the proper configuration of the Host Property Scanner plugin. Make sure to use the test feature to verify the plugin is working correctly. The second method uses the SecureConnector lightweight client.

1. **Clientless:** Configure the Host Property Scanner plugin under options | Plugins.
2. **Lightweight Client:** Install the Secure Connector by visiting `http://Appliance-IP-Address/sc`. Deploy the Secure Connector using any software deployment mechanism.

CHECK FOR COMPLIANCE

CounterACT can determine whether hosts are running anti-virus and whether the anti-virus definitions are up to date using the appropriate policy condition under **Windows Security**. CounterACT also has the capability to check services, registry keys, processes, run scripts, and several other items using policy conditions under **Windows OS**.

- Note that we find services based on the Display Name.
- You can use the regex constructs of .* before, in the middle, or at the end of your search string for many of the conditions. <dot> <asterisk> used together means “anything”.

Troubleshooting information is covered in the appendix. You can use `fstool hostinfo` and `fstool va_test host <Host IP>` tools to see what information CounterACT has for a host.

19. Review CounterACT logs and audit trails.

CounterACT contains several built-in logs and audit trails under the Log menu in the Main Console. Note you may also find information and build reports using the information in the previous section.

- **NAC Policy Log:** Contains policy auditing and execution details.
- **Host Details:** Contains detailed information for a single host.
- **Blocking Log:** Contains detailed information about NAC blocking events.
- **Event Viewer:** Contains detailed information about triggers and event processing.
- **Audit Trails:** Contains detailed user auditing.
- **Service Attack History:** Contains a detailed historical record of service attacks.

20. Build useful reports.

There are several methods for accessing meaningful data from the CounterACT appliance:

- **Option 1**: Access reports by logging onto the **web portal and then select NAC Reports**.
- **Option 2**: Select **Reports** in the main console viewing pane.
- **Option 3**: You can **query History** in the main console viewing pane and **export** the results.
- **Option 4**: You can **export the results of a NAC Policy**.

21. Backup system settings.

After an evaluation the customer may want to back up their data, policies, and settings for installation onto their production unit. Source events and your site structure (real and virtual hosts) are not saved. See the Console User's Manual if you need to backup source events. It's recommended that you review backing up each of the items in the following table.

Note that there are several configuration settings that can be individually exported and imported into the same or different CounterACT appliances that are NOT part of the same system.

DATA	HOW
Backup All System Settings	The backup feature saves all CounterACT configuration settings, as well as many settings defined via the Console, for example. • CounterACT IP address • Root and Admin passwords • Channel, e-mail, and Protected/Source network parameters • Basic and advanced policy definitions • Legitimate probe definitions • Report schedules

	In the main console window, **navigate to CounterACT Options	Appliance	select an appliance	Backup.** Choose a place to save your backup file.
NAC Policies	Right-click the policy and select **Export policy**. Backup all policies by backing up the system settings. Settings are exported as an XML file. Note that you can also create a PDF summary of the NAC Policies by selecting Reports	NAC Policy Summary Report in the main console.
Network Segments	Right-click **All IPs** under **Network Segments** and select **Export**. Settings are exported as an XML file.
Legitimate Probe Rules	Navigate to **Policy	Malicious Source Settings	Legitimate Probes**. Select **Export**. Settings are exported as an XML file.
Virtual Firewall Rules	Navigate to **Policy	Virtual Firewall**. Select **Export**. Settings are exported as an CSV file.

RESTORING DATA

The option to restore from backup is available during the new installation **after the appliance reboots**. Make sure to **select option 2) Restore saved CounterACT-x.x.x configuration**. Next, select your preferred restore option and CounterACT will automatically attempt to find the restore file. *Note that you must restore to the same version of CounterACT that you backed up.*

Additionally, use the command line `fstool restore` to restore from a file locally at the appliance.

```
fstool restore [-f] [-e directory] backup-file.
```

DOCUMENTATION AND TOOLS

22. Make sure the customer has appropriate documentation and tools.

Make sure the customer has copies of relevant software, documentation, and contact information such as the CounterACT Console User Manual and support contact information and procedures.

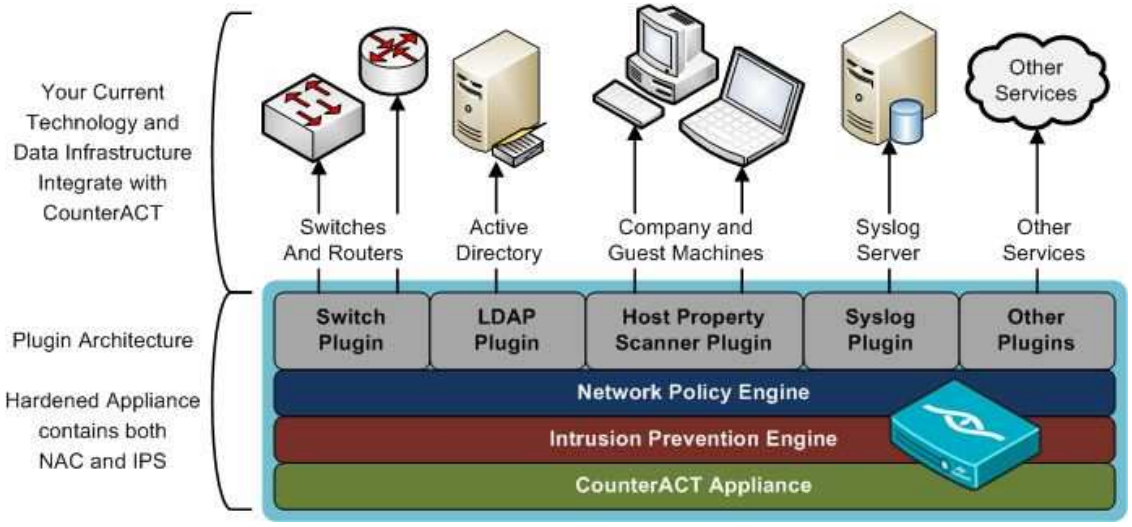
23. Write down the Serial Number and IP Address of the CounterACT install.

The license is tied to the Management IP Address of the CounterACT installation.

ADDITIONAL INFORMATION

APPENDIX A: PRE EVALUATION – CHECKLIST ITEMS

	Item	Comment
Active Directory or Sun Directory Setup – *Used to query LDAP for user information*		
☐	**Directory Server Address, Domain Account and Password:** Allows retrieving user information.	
Host Property Scanner Setup – *Used to query domain hosts for endpoint information*		
☐	**Domain Service Account and Password:** This username should have administrative credentials to log onto user machines with administrative rights.	
List of Authentication Servers – *Used to gather username information and for some policy conditions*		
☐	**Authentication Server List:** Includes servers yours users authenticate against such as Exchange, LDAP, Microsoft Active Directory, and Sun's Java System Directory	
Managed Switch SNMP Information – *Used to query network gear for L2/L3 information*		
☐	**Switch IP Address and Brand:** Please identify the IP address and brand of the switches to monitor.	
☐	**SNMP Community String Version and Type:** Discuss ReadOnly and ReadWrite abilities.	
☐	**Copper or Fiber Connectivity:** 10/100/1000 BaseT Copper or Fiber can be used,	
Appliance Configuration Information – *Used to configure CounterACT with basic setup information*		
☐	**Appliance hostname and domain name:** For example, COUNTERACT.COMPANY.COM	
☐	**Appliance IP/Mask/Gateway:** This is used both for management and interaction with endpoints. It should have unfiltered connectivity to all devices on the protected network.	
☐	**DNS server addresses:** DNS is used to perform reverse-name resolution of internal IP addresses.	
☐	**Administrator email address:** Administrative emails will be sent to this address.	
☐	**Mail relay address:** (optional) The appliance can also send alert emails using its internal SMTP server.	



APPENDIX B: CONFIGURING THE NETWORK

COMMON NETWORK ISSUES

Some of the most common network mistakes include:

- Incorrectly setting up the Switched Port Analyzer (SPAN) port
  - You should have bi-directional traffic
  - Traffic should be tagged if trunking multiple VLANs
- Incorrectly setting up the Response Port
  - Should be setup exactly like an uplink port when configured for multiple VLANs
  - The Response Port needs to be able to pull a DHCP address. You will see this when the GUI is configured. Each channel under Options | Channels should have an IP configured for each available enabled VLAN.

DOCUMENTATION FOR CONFIGURING SPAN

- **Cisco Documentation Home:** http://www.cisco.com/univercd/home/home.htm
- **Cisco SPAN**: http://www.cisco.com/warp/public/473/41.html
- **Foundry Switch and Router**: http://www.foundrynet.com/services/documentation/sribcg/index.html
- **Foundry FastIron X-Series**: http://www.foundrynet.com/services/documentation/fisx-user/index.html

NOTE ABOUT THE RESPONSE AND MANAGEMENT PORTS

The management and response interfaces work in tandem to communicate to end points. The **response interface** is responsible for spoofing addresses, injecting resets, and injecting HTTP redirects. The **management interface** is responsible for communications to switches, radius servers, desktop queries, nmap scans, and much more. Therefore, the management interface needs access to your switches, radius servers, Active Directory, etc. If you have switch management or devices on a private VLAN, you can add an additional management interface to communicate with these devices. This information is discussed in more detail under **Appendix 6: HTTP Redirect**, in the CounterACT Console User Manual.

CAT OS EXAMPLE

```
clear trunk 10/38 1,3,7,9,11-16,18-79,84-113,115-213,215-4094
set trunk 10/38 nonegotiate dot1q 2,4-6,8,10,17,80-83,114,214
clear trunk 10/40 1,3,7,9,11-16,18-79,84-113,115-213,215-4094
set trunk 10/40 nonegotiate dot1q 2,4-6,8,10,17,80-83,114,214

set span <vlans to monitor> <destination port>
set span 2,4-6,8,10,17,80-83,114,214 10/38
```

IOS EXAMPLE

```
interface FastEthernet 4/25
description "ForeScout Management"
no ip address
duplex full
switchport
switchport mode access
switchport access vlan xxx

interface GigabitEthernet7/16
description "ForeScout Monitor"
no ip address
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed all
switchport mode trunk
switchport nonegotiate

interface GigabitEthernet8/16
description "ForeScout Response"
no ip address
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed all
switchport mode trunk
switchport nonegotiate

monitor session 1 source vlan xxx-yyy
monitor session 1 destination interface Gi7/16
```

APPENDIX C: COMMAND LINE TOOLS

CONNECT TO COUNTERACT USING THE SSH CLIENT

The root password is used to log in using SSH for command line operations. The installation script sets the root password the same as your console administrator password.

Command line connection to the appliance provides advanced and quick troubleshooting. Install an SSH client that you feel comfortable using and connect to the appliance. Two popular and free SSH clients include:

- **Putty**: http://www.chiark.greenend.org.uk/~sgtatham/putty
- **SSH Communications**: http://ftp.ssh.com/pub/ssh or ftp://ftp.ssh.com/pub/ssh

FSTOOL COMMANDS:

fstool was built by ForeScout to help configure custom options and to help troubleshoot during installation. These tools can be found by typing `fstool help` at the command line. Some of the more commonly used commands are highlighted below.

Usage: `fstool command [options]`

Command	Function
Backup	Backup tool
Restore	Restore tool
Upgrade	Upgrade CounterACT
Version	Display CounterACT version information
config_sum	Display Configuration Summary CounterACT
Ethtest	Identify interfaces by blinking them one at a time
Ssh	Edit SSH client addresses
Clients	Edit CounterACT client addresses
Netportal	Edit Network Information Portal Access
Netconfig	Configure CounterACT machine network parameters
DNS	Configure CounterACT name server(s) (DNS)
mail_conf	Change/display mail configuration
Fw	Manage built-in firewall
ifcount	Show network traffic distribution per interface

linktest	Network link test tool
va_test	Test remote host for manageability
oneach	Execute a command on each of the CounterACT appliances
passwd	Change administrator password
nphalt	Suspend Network Integrity and clear sources
service	CounterACT application control
remote_support	Send a request for remote assistance and wait for connection
snapsend	Send files to ForeScout snapshot server
snapshot	Create and optionally send CounterACT snapshot

UNIX COMMANDS:

`ifup ethX` ←ensures all of our interfaces are enabled

`tcpdump -ni ethX | grep 'ip address'` ←dump for specific traffic from an IP

`tcpdump -nn ethX vlan1 and host 1.2.3.4` ←dump for a specific host and vlan tag

`tcpdump -I ethX -nn host 1.2.3.4 and port X` ←dump for a specific host and port

`arping -D -I ethX 1.2.3.4` ←arpping real IP address to verify response works properly

FSTOOL NETEST

Try running this test if you have issues with redirecting web pages or using the virtual firewall. The channels should be enabled to run this test.

```
[root@CounterACT root]# fstool netest -j 10 -m 300 -t 300 -v

j = injection test period
m = maximum symmetry test time
t = minimum symmetry test time
v = verbose
```

Look for the following passed tests:

```
Injection test summary: Passed!
       259 Symmetric pairs (100.0%)
         0 Asymmetric pairs (0.0%)

Symmetry test summary: Success!
Injection test summary: Passed!
```

APPENDIX D: TROUBLESHOOTING

This Section Covers:
A. Troubleshooting General Endpoint Connectivity
B. Troubleshooting CounterACT Channels
C. Troubleshooting HTTP Redirects with TCPDump

A. TROUBLESHOOTING GENERAL ENDPOINT CONNECTIVITY

The account must have sufficient rights to access the host. Make sure network configurations and firewalls allow our appliance to access the host. Note that the Host Property Scanner uses the Management Port for its heavy lifting and communications to end points.

- Use the **fstool va_test** tool from CounterACT's command line
- **Check network FW, client FW**
- Attempt to **Net Use** from another machine
- Verify the **account** is part of the Domain Administrator's Group.
- Verify ports **139** and/or **445** have remote access to the client
- Verify **Server Service**, **Remote RPC**, and **Remote Registry** are running
- Note that you can add more than one account to the Host Property Scanner.
- Listing the NetBIOS domain name (e.g. `DOMAIN`) as a separate login entry has helped in some cases. This entry would be in addition to the qualified domain (e.g. `DOMAIN.com`)
- Listing the DOMAIN NAME IN ALL CAPS has helped in some cases.
- Consider changing the **Network Admission Resolve Delay** to greater than 30 seconds (e.g. 90 seconds) if you have issues with not reporting hosts as manageable. This gives hosts more time to start services when waking or booting up. This is specific to the Domain Member or Manageable condition.

USING FSTOOL VA_TEST

This is a great way to test the connectivity of a system. Run this tool using the host switch (-h) to designate which host you want to test. Use the verbose switch (-v) for more information in the output.

```
fstool va_test -h 10.0.0.49
```

There are several options available. For example, you can look for services that include the word Symantec in them using the `fstool va_test` command piped into a `grep` command.

```
fstool va_test -h 10.0.0.49 -c services -v | grep -i Symantec
```

FORESCOUT BIN TOOLS

There are several tools tucked away under `/usr/local/forescout/bin` including the `SMBclient`, `RPCclient`, and `fsnbtscan`.

B. TROUBLESHOOTING COUNTERACT CHANNELS

65537 ERROR: CHANNEL INJECTION FAILED

CounterACT's verification of the response channel failed. This means packets sent from the response interface cannot communicate with the monitoring interface for this channel. Operating in this manner severely impairs or prevents CounterACT's ability to correctly interrogate endpoints, determine malicious sources, and provide protection for your network. Consider the following solutions:

1. Check that the Response cable is properly connected.
2. Ensure the switch port is properly configured to communicate with the monitored hosts by making sure the Response switch port is trunked, tagged, and at an appropriate place in the network.
3. If you are using a single CounterACT interface for both monitor and response, then verify the switch port you are monitoring allows bidirectional traffic. You can also consider separating the monitor and response functions into separate ports. Refer to the Console User's Manual for instructions on adding a separate response port.
4. If you respond into Layer 3, then you may have to use an active regeneration tap.
5. Use `fstool ifcount [interface]` from CounterACT's command line interface to view traffic in real time as you make changes to the switch. You can specify more than one interface separated by spaces.

65538 ERROR: CHANNEL ASYMMETRIC FAILED

CounterACT detected several asymmetric conversations. This means only one side of several TCP sessions is correctly monitored to CounterACT, resulting in CounterACT missing the other half of these TCP sessions. Operating in this manner severely impairs CounterACT's ability to correctly interrogate endpoints, determine malicious sources, and provide protection for your network. Consider the following solutions:

1. Review the network topology for possible asymmetric traffic paths and add separate monitoring interfaces as necessary.
2. Verify both switches in a redundant pair have their own monitoring interfaces.
3. Verify the switch port(s) you are monitoring allow(s) bidirectional traffic.
4. You can exclude non-essential portions of the network from the protected network and CounterACT will ignore asymmetric traffic from those hosts.
5. Use `fstool ifcount [interface]` from CounterACT's command line interface to view traffic in real time as you make changes to the switch. You can specify more than one interface separated by spaces.

65539 ERROR: NO CHANNEL TRAFFIC

CounterACT failed to detect traffic on the monitoring interface. Operating in this manner may impair CounterACT's ability to correctly detect hosts, determine malicious sources, and provide protection for your network. Consider the following solutions:

1. Check that the monitor cable is properly connected.
2. Verify the correct CounterACT interface is chosen to create the Channel.
3. Ensure the switch port is properly configured to communicate with the monitored hosts by making sure the switch port is trunked, tagged, and mirrors traffic to CounterACT.
4. Verify both CounterACT's interface and the switchport interface are "UP".
5. Use `fstool ifcount [interface]` from CounterACT's command line interface to view traffic in real time as you make changes to the switch. You can specify more than one interface separated by spaces.

C. TROUBLESHOOTING HTTP REDIRECTS WITH TCPDUMP

tcpdump is a simple and powerful tool for dumping and parsing traffic on an interface. tcpdump can be run locally or through the SSH connection. Remember when connecting with SSH to use the root account. Also see **Appendix 6: HTTP Redirect** in the CounterACT Console User Manual.

1. Run `tcpdump –i <Monitor Port> host <target IP>`
    a. Do you see any unicast traffic such as port 80?
        i. If no, problem with the Span Port not seeing the traffic check the switch.
2. Run `tcpdump –i <Response Port> host <target IP>`
    a. Do you see the host IP?
        i. If no, call support there is an issue with the CounterACT
        ii. If yes, verify the Response Port switch port is trunked and allowed on the same vlan as the client.
3. Run `tcpdump –i <Management Port> host <target IP>`
    a. Do you see the target ip address?
        i. If no, verify the target has access to the CounterACT management IP.
        ii. If yes, call support

APPENDIX E: MISC INFORMATION

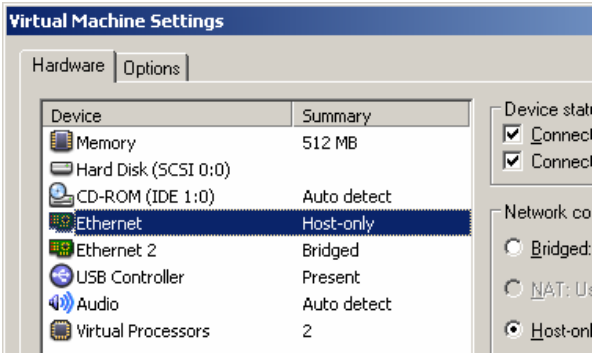
This Section Covers:
A. How to install CounterACT onto VMware (for learning only)
B. How to create a custom splash page
C. How to customize text in HTTP Redirect conditions
D. How to use regular expressions
E. How to upgrade CounterACT
F. How to configure CounterACT using a serial cable
G. How to install a private VLAN Management Interface
H. How to control CounterACT responses
I. Notes on open ports required for CounterACT
J. Options for a Hub

A. HOW TO INSTALL COUNTERACT ONTO VMWARE (FOR LEARNING ONLY)

CounterACT can be installed as a test platform onto other hardware but **this is not supported**. The OS will not install on anything less than 80GB without one of two workarounds. In Virtual OS software you can assign 80GB virtually and expect to use 4-5GB of real drive space. Another option is to force the install onto smaller drives during the CD installation. **Type the following in the first menu that appears. This menu has options to Install CounterACT or Boot from the Hard Drive:**

```
1 ks=file:/10
```

The number at the end of the line can be `10`, `20`, `40`, or `80`, corresponding to 10, 20, 40, and 80GB (default) disk space respectively.



ADDITIONAL CONSIDERATIONS FOR INSTALLING INTO VMWARE

- Create two NICs. One will be shared with the host and the other will be bridged.
- Choose untagged interfaces under **Advanced** options when adding channels. You can monitor and respond on the same interface.
- Become familiar with the command line `fstool netconfig` utility inside CounterACT. You will want to SSH into CounterACT using your favorite client. You will find that it's easier to work this way than to work within the VMWare interface. Here is an example of a configuration that allows the consultant to access the interface regardless of whether he is connected to a network or not (e.g. on a plane, in a conference room without internet access,

etc.). This is configured from `fstool netconfig` and assumes the host-only subnet is 192.168.10.0/24.

```
-------------------------------------------------
CounterACT Machine Network Interfaces Configuration
-------------------------------------------------
  * eth0      Address: 192.168.10.140    Netmask: 255.255.255.0
  * eth1      Address: 10.10.1.140       Netmask: 255.255.255.0
```

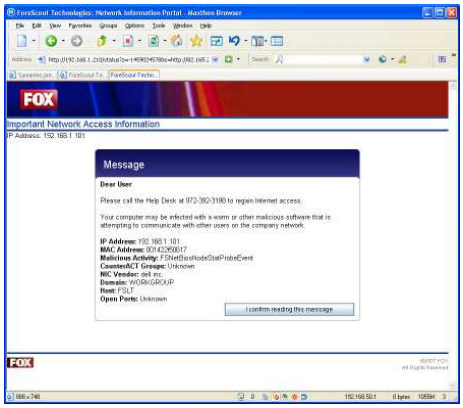
- Remember basic networking concepts. If you change to a new network, then you need to change the bridged interface to match the broadcast domain of the network you move into. Also remember that are limited by the traffic you can see in your VM session.

B. HOW TO CREATE A CUSTOM SPLASH PAGE

This is an advanced method for creating a customized HTML page that is only recommended for those comfortable with working with HTML editors and at the UNIX command line.

ADVANCED METHOD

Use the following steps to create a custom splash page using an external HTML editor:



CREATE CUSTOM HEADER AND FOOTER HTML FILES

1. Create two files called customizeFooter.html and customizeHead.html.
2. Edit appropriately.
3. Open customizeFooter.html and customizeHead.html in a text editor and add the following to the path of each image:

   `./customize/`

   For example, change `src="logosm.jpg"` to `src="./customize/logosm.jpg"`

4. Copy the files (e.g. using WinSCP) to the following directory on CounterACT:

   `/usr/local/forescout/webapps/portal/customize`

UPDATE THE STYLESHEET WITH A WHITE BACKGROUND

1. Open a web browser to https://CounterACT_IP_Address/precustomize.
2. Login and navigate down to Background Color.
3. Enter #FFFFFF into the text box next to the Color button.

C. HOW TO CUSTOMIZE TEXT IN HTTP REDIRECT CONDITIONS

Text can be formatted in the redirect text when creating the condition. Use simple tags indicating font size, type, format, and links. Here is an example of creating an internal link to a website:

```
<a HREF=http://prodsrv.comp.com/remediate.asp>Company Link</a>
```

This will create the text "Company Link" and will link to "http://prodsrv.comp.com/remediate.asp." This example also works with netbios links such as \\netapp\share\patches\install_patch123.exe.

D. HOW TO USE REGULAR EXPRESSIONS

Regular expressions (regex) parse data for your results in the Network Integrity Policies. For example, try this under **Device Information | MAC** to test for Cisco IP phone network interfaces:

```
003094.*    Test for Cisco IP phone network interfaces
```

Try using the regex constructs of **.*** before, in the middle, or at the end of your search string. The <dot> means any character, and the <asterisk> means any number of the preceding character. Together they make a true wildcard.

`Symantec.*`	Finds any service **beginning** with Symantec
`.*Antivirus.*`	Finds any service that **contains** the word "antivirus"
`.*Definition Watcher`	Finds any service **ending** with Definition Watcher

Using regex in Java: http://java.sun.com/j2se/1.4.2/docs/api/java/util/regex/Pattern.html

E. HOW TO UPGRADE COUNTERACT

It's possible to upgrade the appliance from the command line or from the console GUI interface after working through the command line installation.

HOW TO UPGRADE COUNTERACT USING THE CLIENT INTERFACE (GUI):

You can upgrade the appliance using the client console:

1. Navigate to **CounterACT Options | Appliance | Upgrade**.
2. Select the ForeScout Service Pack file (.fsp)
3. Select OK and the appliance will update.

HOW TO UPGRADE COUNTERACT LOCALLY USING A KEYBOARD AND MONITOR:

You can install the appliance by booting with the CD in the drive. If you have a keyboard and monitor installed, just follow the onscreen instructions. If you cannot boot from the CDROM but you can read from the CDROM, then you can upgrade the appliance.

1. Mount the CD-ROM in the CounterACT machine.
2. Change to the CD-ROM directory and run the "ca_setup" script.

```
mount /mnt/cdrom
cd /mnt/cdrom
./ca_setup
```

HOW TO UPGRADE COUNTERACT USING THE ENTERPRISE MANAGER:

You can also upgrade your appliances using the Enterprise Manager.

1. Download the upgrade file to your PC.
2. Open the console and navigate to **CounterACT Options | Appliance | Upgrade Management Server**.
3. Install the update .
4. Select an appliance to upgrade to the version and perform the updates.

F. HOW TO CONFIGURE COUNTERACT USING A SERIAL CABLE

Configure the terminal client according to the following parameters:

- Baud: 19200
- Parity: None
- Data Bit: 8
- Stop Bits: 1
- Flow Control: None
- Emulation: ANSI

You may have to type the following command at the boot prompt in order to see the output on the computer connected through the serial cable. **Note:** You may not see the text as you type this.

1. Type this for the CTR if it has a 40GB hard drive:
   `1 ks=file:/40 console=ttyS0,19200 console=tty1`
2. Type this for the **CT-100**: `1 console=ttyS0,19200`
3. Type this for the **CT-1000/2000**: `1 console=ttyS1,19200`

G. HOW TO INSTALL A PRIVATE VLAN MANAGEMENT INTERFACE

If you have switch management or devices on a private VLAN, you can add an additional management interface to communicate with these devices. This information is discussed in more detail under **Appendix 6: HTTP Redirect**, in the CounterACT Console User Manual.

Use the `fstool redaddr` command if you need to change which IP Address is used to HTTP redirect from the pool of addresses assigned to CounterACT's ports. Assign addresses to CounterACT's ports using `fstool netconfig`.

H. HOW TO CONTROL COUNTERACT RESPONSES

There are several ways you can change how CounterACT responds to a range of addresses.

You can ignore a host completely in CounterACT by: [1] Adding the host to the Addresses to Ignore group (for policies) and [2] Excluding the host from the Active Response range (for malicious behavior marks) OR adding the host to Legitimate Probes.

1. **Internal Network**: Options | Internal Network. The Internal Network defines the scope of devices affected by policies. Hosts outside of this range will not be affected by policies.

2. **Addresses to Ignore**: Groups | select Addresses to Ignore and then select Edit. Individual addresses or ranges added here will be ignored for all Network Integrity Policies.
3. **Active Response Range (Protected Network)**: Options | IPS Policy | Advanced | Active Response Range. CounterACT's IPS responds to hosts only if they are detected as having attacked hosts in this range. Excluding a range of addresses from the Active Response Range prevents CounterACT from creating virtual hosts in the excluded range.
4. **Discovery Options**: Options | Discovery and adjust the discovery options as necessary. Note the checkbox to **Resolve properties displayed in the Console Information Panel** which controls whether CounterACT queries and gathers information on hosts as you view them in the information panel. For example, adding a new column may trigger this behavior.
5. **NBT Scan Plugin**: Options | Plugins | NBT Scanner. This plugin enables CounterACT to perform NBT lookups on hosts. Stopping this plugin disables this behavior.
6. **Policy Exceptions**: View the Advanced tab under the Network Integrity Policies you've created and select Exceptions. Here you can create exceptions based upon IP ranges and previously created segments among other options.
7. **Legitimate Scans**: Options | IPS Policy | Legitimate Scan and add or remove entries to prevent CounterACT from delivering marks to legitimate scanning devices.

I. NOTES ON OPEN PORTS REQUIRED

Internal Network Connectivity

Port	Service	Comments
22/TCP	*SSH*	Allows clients to access the CounterACT command line interface (CLI)
25/TCP	*SMTP*	Allows CounterACT access to the enterprise mail relay
80/TCP	*HTTP*	Allows clients to access the CounterACT web console
443/TCP	*HTTPS*	Allows clients to access the CounterACT web console using SSL
13000/TCP	*CounterACT*	Allows GUI console and Enterprise Manager to access CounterACT
53/UDP	*DNS*	Allows CounterACT access to resolve internal IP addresses
123/UDP	*NTP*	Allows CounterACT access to a time server.
161/UDP	*SNMP*	Allows CounterACT access to communicate with network devices.
162/UDP	*SNMP*	Allows CounterACT to receive SNMP traps from network devices.

External Network Connectivity

Port	Service	Comments
22/TCP	*SCP*	snapshot.forescout.com [212.179.35.137]
80/TCP	*HTTP*	updates.forescout.com [72.32.185.155]
443/TCP	*HTTPS*	updates.forescout.com [72.32.185.155]
30022/TCP	*Remote*	svc23.forescout.com [194.90.25.86]

30023/TCP	*Support*	
123/UDP	*NTP*	ntp.forescout.com [72.32.185.155]

I. OPTIONS FOR HANDLING USERS ON A NON-MANAGED SWITCH OR HUB

- Immediately perform an HTTP Hijack to inform the user that what they are doing is against policy, informing users that you are aware of the activity immediately. Most users will readily comply.
- Use the Virtual Firewall which prevents the host from making connections using resets to collapse the TCP connections
- Disable or reset the default VLAN port assignment for that port
- Alert administrators and event managers
- Add the device to a group and/or list in the console that allows you to track the activity of the end point
- Track any one of 39 properties for changes (e.g. DNS Name Change, Domain Member Change, Nmap-OS Class Change, Shared Directory Change, NetBIOS Hostname Change)
- If the device is manageable, then perform any scripting, remediation, or other manageable action on the endpoint
- And always – we monitor the end point for malicious activity, scanning, and worm propagation

APPENDIX F: POST EVALUATION – BACKING UP DATA

After an evaluation the customer may want to back up their data, policies, and settings for installation onto their production unit. Source events and your site structure (real and virtual hosts) are not saved. See the Console User's Manual if you need to backup source events. It's recommended that you backup each of the items below:

DATA	HOW
Backup All System Settings	The backup feature saves all CounterACT configuration settings, as well as many settings defined via the Console, for example. • CounterACT IP address • Root and Admin passwords • Channel, e-mail, and Protected/Source network parameters • Basic and advanced policy definitions • Legitimate probe definitions • Report schedules In the main console window, **navigate to CounterACT Options | Appliance | select an appliance | Backup.** Choose a place to save your backup file.
Network Integrity Policies	Right-click the policy and select **Export policy**. Backup all policies by backing up the system settings. Settings are exported as an XML file.
Network Segments	Right-click **All IPs** under **Network Segments** and select **Export**. Settings are exported as an XML file.
Legitimate Probe Rules	Navigate to **Policy | Malicious Source Settings | Legitimate Probes**. Select **Export**. Settings are exported as an XML file.
Virtual Firewall Rules	Navigate to **Policy | Virtual Firewall**. Select **Export**. Settings are exported as an CSV file.

RESTORING DATA

The option to restore from backup is available during the new installation **after the appliance reboots**. Make sure to **select option 2) Restore saved CounterACT-x.x.x configuration**. Next, select your preferred restore option and CounterACT will automatically attempt to find the restore file. *Note that you must restore to the same version of CounterACT that you backed up.*

Additionally, use the command line `fstool restore` to restore from a file locally at the appliance.

```
fstool restore [-f] [-e directory] backup-file.
```

APPENDIX G: SUPPORT INFORMATION

SUPPORT GENERAL INFORMATION:

1. Contact the regional Sales Engineer for support during evaluations.
2. Try searching the Console User's Manual on the installation CD: *CounterACT-x.x.x-Console-User-Manual.pdf*

Online Information	Web Portal: Support: Searchable Docs: Policy Templates:	http://www.forescout.com http://www.forescout.com/support/ http://www.forescout.com/support/files/counteract/docs_portal http://www.forescout.com/online/policy_templates/1/
Support	Online: Email: Phone:	http://www.forescout.com/support/ support@forescout.com Office: 866-377-8773
Licensing	Email:	license@forescout.com
Equipment Return	Shipping Address:	**ForeScout Technologies** *Attn: Christina Pessefall* 602-416-2121 1955 East Sky Harbor Circle No Phoenix, AZ 85034