Contact Information
Forescout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134 USA
https://www.Forescout.com/support/
Toll-Free (US): 1.866.377.8771
Tel (Intl): 1.408.213.3191
Support: 1.708.237.6591

About the Documentation
- Refer to the Resources page on the Forescout website for additional technical documentation: https://www.Forescout.com/company/resources/
- Have feedback or questions? Write to us at documentation@Forescout.com

Legal Notice
© 2019 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at https://www.Forescout.com/company/legal/intellectual-property-patents-trademarks, Other brands, products, or service names may be trademarks or service marks of their respective owners.
# Table of Contents

## Preface
- About the CounterACT Solution ........................................... 6
- About This Guide ............................................................... 6
- CounterACT Package Contents ........................................... 7
  - Virtual Devices .............................................................. 7
- Additional CounterACT Documentation ............................... 8
  - Documentation Downloads ............................................ 8
  - Documentation Portal .................................................. 9
- Forescout Help Tools .......................................................... 9

## Chapter 1: System Components and Requirements .................. 10
- CounterACT Components .................................................. 11
  - CounterACT Appliance .................................................. 11
  - CounterACT Enterprise Manager .................................... 12
  - Recovery Enterprise Manager ....................................... 12
  - CounterACT Console .................................................... 13
- Password Encryption Algorithm .......................................... 13
- Remote System Management Integration ............................... 13
- High Availability Tools ..................................................... 14
- Power Outage Handling .................................................... 14
- System Requirements ....................................................... 14
  - CounterACT Console Hardware Requirements ............... 15
  - Network Access Requirements ...................................... 15
  - Network Deployment Requirements ............................... 18
  - Appliance Information Requirements ............................. 18
  - Enterprise Manager Information Requirements ............. 18
  - Network Connection Requirements ............................... 18
  - Bandwidth Requirements ............................................. 19
- IPv6 Support ........................................................................ 19
- FIPS Compliance ............................................................. 19
  - Enabling FIPS Mode ..................................................... 19
  - Verifying FIPS Compliance .......................................... 20
  - FIPS Compliance with SecureConnector ..................... 20

## Chapter 2: Network Setup ................................................... 21
- About the CounterACT Installation .................................... 22
- Related Documents .......................................................... 22
- Appliance Interface Connections ........................................ 23
  - Management Interface .................................................. 23
  - Configure VLANs on the Management Interface .......... 24
  - Monitor Interface ......................................................... 24
  - Response Interface ...................................................... 25
- Setting Up Switch Connections .......................................... 25
Table of Contents

Recommended Installation: Separate Management, Monitor and Response Ports ...................................................... 26
Combined Monitor and Response Port .................................................................................................................. 26
Combined Management and Response Port (Single VLAN Only) ................................................................. 28
Combined Management, Response and Monitor Port (Single VLAN Only) .................................................... 28
Switch Setting Guidelines ................................................................................................................................. 28
Creating an Out-of-Band IP Management Interface.......................................................................................... 29

Chapter 3: Appliance Setup and Configuration, and Post-Installation Procedures .............................................. 32
Setting Up an Appliance ........................................................................................................................................ 33
Serial Port Setup .................................................................................................................................................. 33
Configuring an Appliance .................................................................................................................................... 34
Post-Installation Procedures ............................................................................................................................... 39
Connect an Appliance to the Network ................................................................................................................ 39
Integrate with Remote System Management .................................................................................................... 40
Verify the Management Interface Connection ................................................................................................. 46
Verify Switch/Appliance Connectivity ............................................................................................................... 47
Perform a Ping Test ............................................................................................................................................... 48
Generate a Configuration Summary for an Appliance .......................................................................................... 48
Configure Password Protection for the Boot Loader .......................................................................................... 49
Additional Installation Tools ................................................................................................................................ 49
Configuring the Interface Speed/Duplex .............................................................................................................. 50
Restoring Appliance System Settings ................................................................................................................ 50

Chapter 4: Enterprise Manager Setup and Configuration, and Post-Installation Procedures .............................. 53
About the Installation .............................................................................................................................................. 54
Setting Up the Enterprise Manager .................................................................................................................... 54
Configuring the Enterprise Manager ................................................................................................................... 54
Post-Installation Procedures ............................................................................................................................... 59
Connect the Enterprise Manager to the Network ............................................................................................... 59
Integrate the Enterprise Manager with Remote System Management ............................................................. 59
Restoring Enterprise Manager System Settings ............................................................................................... 59
Restoring as a High Availability Device ............................................................................................................ 61

Chapter 5: Upgrading CounterACT Devices ...................................................................................................... 62
Upgrading to a New Version ............................................................................................................................... 63
Upgrading with the DVD ..................................................................................................................................... 63
Upgrading via a USB Memory Device ................................................................................................................ 63
Upgrading from the Console ............................................................................................................................... 64
Gradual Upgrade .................................................................................................................................................. 64

Chapter 6: Installing the CounterACT Console .................................................................................................. 66
About the CounterACT Console Installation ..................................................................................................... 67
Information Required for the Installation ........................................................................................................... 67
Install from the CounterACT Support Page ....................................................................................................... 68
Install from the Installation DVD ....................................................................................................................... 71
Install from a Browser at Your Appliance ........................................................................................................... 71
## Table of Contents

- Logging In ........................................................................................................... 71
- Installing the Cumulative Update Pack ............................................................... 72
- Running the Initial Setup Wizard on the Console ............................................... 75
- Uninstalling Previous Versions ............................................................................ 76

### Chapter 7: CounterACT Virtual Systems ......................................................... 77

- About CounterACT Virtual Systems .................................................................. 78
  - Hybrid Deployments ......................................................................................... 78
- What to Do .......................................................................................................... 78
- Virtual System Requirements .............................................................................. 79
  - Hardware Minimum Requirements ................................................................... 79
  - Network Connection Requirements for CounterACT Virtual Devices ............... 80
- Virtual Environment Setup - Define Real NICs .................................................. 80
- VMware Virtual Systems .................................................................................... 81
  - VMware Requirements and Support ............................................................... 81
  - Create and Configure Virtual Switches ......................................................... 82
  - CounterACT Virtual Device Deployment in VMware ...................................... 85
  - Post-Deployment Verification and VMware Configuration ............................. 88
- Hyper-V Virtual Systems .................................................................................... 89
  - Hyper-V Requirements and Support .............................................................. 90
  - Deploy CounterACT Virtual Devices in Hyper-V ........................................... 90
  - Configuring Hyper-V to Work with CounterACT Devices .............................. 99
  - Automating CounterACT Deployment in Hyper-V Environments .................. 101
- CounterACT Virtual Device Configuration ......................................................... 108
  - Configure the Virtual Enterprise Manager and Appliances .......................... 108
  - Verify Switch-Appliance Connectivity ........................................................... 109
  - Install the Console ......................................................................................... 109
  - Perform the Initial Console Setup ................................................................... 110
  - Install a Virtual License ................................................................................ 112
  - Duplicating Virtual Devices ......................................................................... 115
  - Moving Virtual Devices .............................................................................. 116

### Appendix A: Site Preparation Form ................................................................. 117

### Appendix B: Upgrading To CounterACT 7.0.0 on Hardware Revision 2x ... 119

### Appendix C: Updating Firmware on Hardware Revision 2x .......................... 121
Preface

This preface includes:

- About the CounterACT Solution
- About This Guide
- CounterACT Package Contents

About the CounterACT Solution

CounterACT delivers complete endpoint security and lets you effortlessly apply your business security policies to the IT infrastructure, accurately and automatically. CounterACT effectively:

- Ensures Network Access Control (NAC) compliance
- Combats worms, self-propagating malware and hackers
- Automatically protects network vulnerabilities
- Creates a virtual firewall that protects or opens specific network zones
- Allows security teams, IT departments and the Help Desk to leverage extensive network information via CounterACT’s web-based Assets Portal

The CounterACT Console User Manual provides more information about these capabilities.

About This Guide

This guide details the CounterACT software installation and configuration procedures and related information for the following components:

- Appliance hardware components
- Enterprise Manager hardware component
- Appliance and Enterprise Manager virtual components
- CounterACT Console management application

Information about setting up Switch connections is also included.

The Installation Guide contains the following chapters:

| Chapter 1: System Components and Requirements | CounterACT system requirements, including hardware and networking requirements |
| Chapter 2: Network Setup | Information about hardware setup options |
| Chapter 3: Appliance Setup and Configuration, and Post-Installation Procedures | How to install and upgrade CounterACT Appliances |
CounterACT Package Contents

Your CounterACT package includes the following components:

- The CounterACT Appliance/Enterprise Manager
- CounterACT Quick Installation Guide
- A CounterACT DVD containing the Console software, the CounterACT Console User Manual, and this guide
- Warranty document
- Mounting brackets
- Power cord
- DB9 Console connecting cable (for serial connections only)
- Getting Started document (CT-xxxx Appliances based on hardware revision 5x)

See CounterACT Components for an overview of each component.

If you are working with a High Availability system, you should have received a separate package with another Appliance or Enterprise Manager. Refer to the Resiliency Solutions How-to Guide for more information.

Virtual Devices

If you are installing CounterACT virtual devices, you should receive instead:

- A link to a CounterACT virtual package image
• An email from Forescout with one demo license file per virtual device to be installed and links to the CounterACT Quick Installation Guide and the complete CounterACT Installation Guide

This system includes CounterACT virtual Appliances, the CounterACT virtual Enterprise Manager and the Console. These components operate identically to physical components, with the exception of licenses.

See Chapter 7: CounterACT Virtual Systems for details about installing virtual systems and about virtual system licenses.

**Additional CounterACT Documentation**

For information about other Forescout features and modules, refer to the following resources:

- Documentation Downloads
- Documentation Portal
- Forescout Help Tools

**Documentation Downloads**

Access documentation downloads from the Forescout Resources Page, or one of two Forescout portals, depending on which licensing mode your deployment is using.

- **Per-Appliance Licensing Mode** – Product Updates Portal
- **Flexx Licensing Mode** – Customer Portal

⚠️ Software downloads are also available from these portals.

**To identify your licensing mode:**

- From the Console, select Help > About Forescout.

**Forescout Resources Page**

The Forescout Resources Page provides links to the full range of technical documentation.

**To access the Forescout Resources Page:**


**Product Updates Portal**

The Product Updates Portal provides links to Forescout version releases, Base and Content Modules, and eyeExtend products, as well as related documentation. The portal also provides a variety of additional documentation.

**To access the Product Updates Portal:**

- Go to https://updates.forescout.com/support/index.php?url=counteract and select the version you want to discover.
Customer Portal
The Downloads page on the Forescout Customer Portal provides links to purchased Forescout version releases, Base and Content Modules, and eyeExtend products, as well as related documentation. Software and related documentation only appear on the Downloads page if you have a license entitlement for the software.

To access documentation on the Forescout Customer Portal:
- Go to https://Forescout.force.com/support/ and select Downloads.

Documentation Portal
The Forescout Documentation Portal is a searchable, web-based library containing information about Forescout tools, features, functionality, and integrations.

- If your deployment is using Flexx Licensing Mode, you may not have received credentials to access this portal.

To access the Documentation Portal:
- Go to https://updates.forescout.com/support/files/counteract/docs_portal/ and use your customer support credentials to log in.

Forescout Help Tools
Access information directly from the Console.

Console Help Buttons
Use context-sensitive Help buttons to access information about tasks and topics quickly.

Forescout Administration Guide
- Select Forescout Help from the Help menu.

Plugin Help Files
- After installing the plugin, select Tools > Options > Modules, select the plugin, and then select Help.

Online Documentation
- Select Online Documentation from the Help menu to access either the Forescout Resources Page (Flexx licensing) or the Documentation Portal (Per-Appliance licensing).
Chapter 1: System Components and Requirements

- CounterACT Components
- Password Encryption Algorithm
- Remote System Management Integration
- High Availability Tools
- Power Outage Handling
- System Requirements
- IPv6 Support
- FIPS Compliance
CounterACT Components

CounterACT components include:

- CounterACT Appliance
- CounterACT Enterprise Manager
- Recovery Enterprise Manager
- CounterACT Console

CounterACT Device

Virtual systems are also available. See Chapter 7: CounterACT Virtual Systems for more information.

Refer to the CounterACT Enterprise Manager Appliance Communication Technical Note for information regarding Enterprise Manager/Appliance communication.

CounterACT Appliance

The CounterACT Appliance is a dedicated device that monitors traffic going through your organization’s network. It protects the network against malicious activity, performs extensive NAC protection, lets you create network security zones and handles vulnerabilities.

Multiple Appliance Deployments

Multiple CounterACT Appliances can be deployed to ensure maximum protection of your organization. Each CounterACT Appliance is installed in order to see vital network traffic.

To handle malware and hackers, the Appliance must be installed:

- At the connection point between a protected network area and the rest of the network. This enables protection of a specific network range against infection attempts initiated from the rest of the network and network protection against infection attempts generated from a specific network area (e.g. a contractors segment, which might be potentially more dangerous).
- Behind a VPN concentrator, where encrypted VPN channels are decrypted and malicious traffic can enter your network.
Chapter 1: System Components and Requirements

- Behind remote access servers, where remote access users are entering your network.

**To apply an admission control policy, the Appliance must be installed:**
- Within broadcast domains, preferably mirroring tagged ports.

**To work with the Virtual Firewall, the Appliance must be installed:**
- Between segments/VLANs.

![Typical Appliance Setup](image)

### CounterACT Enterprise Manager

The CounterACT Enterprise Manager is an aggregation device that communicates with multiple CounterACT Appliances distributed across an enterprise. It manages the CounterACT activity and policies, and collects information about malicious activity that is detected at each Appliance, including infection attempts, and identification, notification, restriction and remediation actions taken by CounterACT. This information is available for display and reporting at the CounterACT Console.

#### Enterprise Manager Support for Appliances

A single Enterprise Manager can support up to 200 Appliances.

### Recovery Enterprise Manager

The CounterACT Recovery Enterprise Manager is used as a recovery device for an Enterprise Manager that is no longer functioning due to, for example, a natural disaster or crisis. This device provides complete and continued management of network Appliances from a remote site. The Recovery Enterprise Manager is installed at the remote Data Center using the same installation procedure as the Enterprise Manager and is later added at the Console as you would any other CounterACT component. Refer to the [Resiliency Solutions How-to Guide](#) for more information.
CounterACT Console

The Console is the CounterACT management application used for viewing and managing important information about NAC policies, malicious intrusions, vulnerable network hosts and more. The Console lets you define the conditions under which hosts are identified and handled by CounterACT. The Console also provides a number of tools:

- Policy tools that allow you to define a virtual firewall policy, a policy for handling NAC, security and compliance issues, and a policy for handling malicious sources.
- Sophisticated reporting tools that let you generate an extensive range of reports about malicious source activity, NAC activity and vulnerability scanning, as well as CounterACT’s response to these activities.
- Control tools that allow you to start and stop Appliances and Enterprise Managers and update the configuration defined during installation (for example, the network range that CounterACT is protecting or the time zone setting). Other control tools allow you to communicate with your Network Management application and to work with third-party plugin applications.

Refer to the CounterACT Console User Manual for more information.

Password Encryption Algorithm

Users may be required to insert credentials when working with CounterACT components, for example, domain credentials or community strings. These credentials are encrypted using the AES-256 algorithm.

Remote System Management Integration

Integrated remote server modules give you location-independent and OS-independent remote access over the LAN or Internet to CounterACT devices. Use the module for remote KVM access and power on/off/reset, and to perform troubleshooting and maintenance tasks.

See the following sections for information about setting up these modules:

- Hardware revision 2x devices support Intel Remote Management Module 3 (RMM3). See Integrating Appliances Based on Hardware Revision 2x with RMM3.
- Hardware revision 3x/4x/5x devices support Integrated Dell Remote Access Controller (iDRAC). See Integrating Appliances Based on Hardware Revision 3x/4x/5x with iDRAC.

This integration is not applicable to virtual systems.
High Availability Tools

A CounterACT High Availability system is implemented by configuring two Appliances or two Enterprise Managers in a pair. Redundancy is achieved by one of the devices serving as the Active node (managing the activities required for effective NAC) while the second node waits in Standby mode to take over in case of Active node failure. Refer to the Resiliency Solutions How-to Guide for more information.

Power Outage Handling

By default, when there is a power outage, the Appliance and Enterprise Manager are set to the Stay Off mode. You can change this default to the Power On mode so that the machine powers on automatically after a power outage recovery.

To change the power outage recovery setting:

1. Reboot the CounterACT device.
2. While the machine is powering on, select F2. The BIOS Setup Utility screen opens.
3. Select the Server tab.
4. Use the arrow keys to select the Default>Stays Off option.
5. Press Enter and then the Down arrow to select Power On.

System Requirements

Verify that the following requirements are met before you begin installation and that you have completed a Site Preparation Form (see Appendix A: Site Preparation Form).

- CounterACT Console Hardware Requirements
- Network Access Requirements
- Network Deployment Requirements
- Appliance Information Requirements
- Enterprise Manager Information Requirements
- Network Connection Requirements
- Bandwidth Requirements

Some requirements may vary for virtual systems. See Virtual System Requirements for details.
CounterACT Console Hardware Requirements

You must supply a machine to host the CounterACT Console application software. Minimum hardware requirements are:

- Non-dedicated machine, running:
  - Windows XP/Vista/7/8/8.1/10
  - Windows Server 2003 or Server 2008
  - Linux
- Pentium 3, 1GHz
- 2GB memory
- 1GB disk space

Network Access Requirements

Deploying CounterACT requires TCP/IP communication. This section details CounterACT connectivity requirements. Check your security policy (Router ACLs etc.), and modify it, if required, to allow for this communication.

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 run the CounterACT Console. The connectivity listed in the following table is required.

<table>
<thead>
<tr>
<th>Port</th>
<th>Service</th>
<th>To or From CounterACT</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>22/TCP</td>
<td>SSH</td>
<td>From</td>
<td>Allows remote inspection of OS X and Linux endpoints. Allows CounterACT to communicate with network switches and routers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To</td>
<td>Allows access to the CounterACT command line interface.</td>
</tr>
<tr>
<td>2222/TCP</td>
<td>SSH</td>
<td>To</td>
<td>(High Availability) Allows access to the physical CounterACT devices that are part of the High Availability pair. Use 22/TCP to access the shared (virtual) IP address of the pair.</td>
</tr>
<tr>
<td>25/TCP</td>
<td>SMTP</td>
<td>From</td>
<td>Allows CounterACT access to the enterprise mail relay.</td>
</tr>
<tr>
<td>53/UDP</td>
<td>DNS</td>
<td>From</td>
<td>Allows CounterACT to resolve internal IP addresses.</td>
</tr>
<tr>
<td>80/TCP</td>
<td>HTTP</td>
<td>To</td>
<td>Allows HTTP redirection.</td>
</tr>
<tr>
<td>123/UDP</td>
<td>NTP</td>
<td>From</td>
<td>Allows CounterACT access to a local time server or ntp.Forescout.net By default CounterACT accesses ntp.Forescout.net</td>
</tr>
<tr>
<td>135/TCP</td>
<td>MS-WMI</td>
<td>From</td>
<td>Allows remote inspection of Windows endpoints.</td>
</tr>
<tr>
<td>Port</td>
<td>Service</td>
<td>To or From CounterACT</td>
<td>Function</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------------------</td>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>139/TCP</td>
<td>SMB, MS-RPC</td>
<td>From</td>
<td>Allows remote inspection of Windows endpoints (For endpoints running Windows 7 and earlier).</td>
</tr>
<tr>
<td>445/TCP</td>
<td></td>
<td></td>
<td>Allows remote inspection of Windows endpoints.</td>
</tr>
<tr>
<td>161/UDP</td>
<td>SNMP</td>
<td>From</td>
<td>Allows CounterACT to communicate with network switches and routers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For information about configuring SNMP, refer to the CounterACT Console User Manual.</td>
</tr>
<tr>
<td>162/UDP</td>
<td>SNMP</td>
<td>To</td>
<td>Allows CounterACT to receive SNMP traps from network switches and routers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For information about configuring SNMP, refer to the CounterACT Console User Manual.</td>
</tr>
<tr>
<td>389/TCP</td>
<td>LDAP</td>
<td>From</td>
<td>Allows CounterACT to communicate with Active Directory.</td>
</tr>
<tr>
<td>(636)</td>
<td></td>
<td></td>
<td>Allows communication with CounterACT web-based portals.</td>
</tr>
<tr>
<td>443/TCP</td>
<td>HTTPS</td>
<td>To</td>
<td>Allows HTTP redirection using TLS.</td>
</tr>
<tr>
<td>2200/TCP</td>
<td>SecureConnector for Macintosh/Linux Property Scanner</td>
<td>To</td>
<td>Allows SecureConnector to create a secure (encrypted SSH) connection to the Appliance from Linux machines. SecureConnector is a script-based agent that enables management of Linux endpoints while they are connected to the network.</td>
</tr>
<tr>
<td>10006/TCP</td>
<td>SecureConnector for Linux</td>
<td>To</td>
<td>Allows SecureConnector to create a secure connection, over TLS 1.2, to the Appliance from Linux machines.</td>
</tr>
</tbody>
</table>
## Chapter 1: System Components and Requirements

### Forescout Installation Guide

<table>
<thead>
<tr>
<th>Port</th>
<th>Service</th>
<th>To or From CounterACT</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>10003/TCP</td>
<td>SecureConnector for Windows</td>
<td>To</td>
<td>Allows SecureConnector to create a secure (encrypted TLS) connection to the Appliance from Windows machines. <em>SecureConnector</em> is an agent that enables management of Windows endpoints while they are connected to the network. Refer to the <em>CounterACT Console User Manual</em> for more information about SecureConnector. When SecureConnector connects to an Appliance or to the Enterprise Manager it is redirected to the Appliance to which its host is assigned. Ensure this port is open to all Appliances and to the Enterprise Manager to allow transparent mobility within the organization.</td>
</tr>
<tr>
<td>10005/TCP</td>
<td>SecureConnector for OS X</td>
<td>To</td>
<td>Allows SecureConnector to create a secure (encrypted TLS) connection to the Appliance from OS X machines. <em>SecureConnector</em> is an agent that enables management of OS X endpoints while they are connected to the network. Refer to the <em>CounterACT Console User Manual</em> for more information about SecureConnector. When SecureConnector connects to an Appliance or to the Enterprise Manager it is redirected to the Appliance to which its host is assigned. Ensure this port is open to all Appliances and to the Enterprise Manager to allow transparent mobility within the organization.</td>
</tr>
<tr>
<td>13000/TCP</td>
<td>CounterACT</td>
<td>From/To</td>
<td>For systems with only one Appliance – from the Console to the Appliance. For systems with more than one CounterACT Device – from the Console to the CounterACT Device and from one CounterACT Device to another. CounterACT Device communication includes communication with the Enterprise Manager and the Recovery Enterprise Manager, using TLS.</td>
</tr>
</tbody>
</table>
Network Deployment Requirements

Each Appliance must be set up at a location in which it sees vital network traffic and can protect devices connected to your switch.

CounterACT supports deployment options for:

- Monitoring multiple VLANs (tagged traffic) – recommended, since it provides the best overall coverage while monitoring only a single port
- Monitoring a tagged port (802.1Q tagged)
- Monitoring a single VLAN (untagged)
- Monitoring a single port (untagged)

Refer to the CounterACT Console User Manual for more information about these features.

Important notes:

- Carefully consider the traffic to monitor.
- It is recommended to monitor the authentication traffic between end users and authentication servers.
- To notify end users via their web browsers, you must monitor HTTP traffic between end users and the Internet/Intranet.

Appliance Information Requirements

The following information regarding each CounterACT Appliance is required:

- CounterACT Appliance IP address
- CounterACT Appliance host name
- Management interface through which Appliance and Console communicate
- Network mask
- Default gateway IP address
- List of the company’s DNS server addresses – to allow resolution of internal IP addresses to their DNS names

Enterprise Manager Information Requirements

The following information regarding the Enterprise Manager is required:

- CounterACT Enterprise Manager IP address
- CounterACT Enterprise Manager host name
- Enterprise Manager Administrator password
- Management interface
- Network mask
- Default gateway
- DNS domain name
• DNS server addresses

**Network Connection Requirements**

Network connections must allow full visibility to all response and monitor traffic. Virtual systems have additional requirements. See [Network Connection Requirements for CounterACT Virtual Devices](#) for details.

**Bandwidth Requirements**

Typical bandwidth usage in CounterACT systems is:

- Between Enterprise Manager and CounterACT Console: Up to 2.5 kbps per Console
- Between Enterprise Manager and Appliance: Up to 1 kbps per Appliance

Actual values will depend on CounterACT system setup, including the number of user-defined policies and their content, and the frequency of communication between CounterACT devices and endpoints.

**IPv6 Support**

You can use IPv6 addresses when installing CounterACT devices.

**FIPS Compliance**

CounterACT meets Federal Information Processing Standard (FIPS) 140-2 (level 2) requirements.

FIPS is disabled by default in your CounterACT system and should be enabled only when required by the US Federal government.

**Enabling FIPS Mode**

An fstool command lets you enable FIPS on CounterACT devices.

```
You must run the fstool command separately on each CounterACT device.
```

**To enable a CounterACT device to work with FIPS:**

1. Log in to the CounterACT device as root and run the following command:
   ```
   fstool fips
   ```
   This toggles the current FIPS status.

**Examples:**

When FIPS is not enabled, `fstool fips` enables FIPS:

```
You are about to enable FIPS 140-2 on this CounterACT machine. 
Note that CounterACT service will be restarted. 
Enable FIPS and restart CounterACT service? (yes/no) :
```
When FIPS is enabled, `fstool fips` disables FIPS:

<table>
<thead>
<tr>
<th>You are about to disable FIPS 140-2 on this CounterACT machine.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note that CounterACT service will be restarted.</td>
</tr>
<tr>
<td>Disable FIPS and restart CounterACT service? (yes/no) :</td>
</tr>
</tbody>
</table>

**Verifying FIPS Compliance**

To verify that your system is FIPS (Federal Information Processing Standard) compliant, log in to the CounterACT device and run the following command:

```bash
fstool version
```

```
---------------------------
<CounterACT_device_type> version information
---------------------------

<table>
<thead>
<tr>
<th>Version</th>
<th>7.0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Build number</td>
<td>&lt;build_number&gt;</td>
</tr>
<tr>
<td>Build date</td>
<td>&lt;date_time_stamp&gt;</td>
</tr>
<tr>
<td>HA supported</td>
<td>&lt;Yes</td>
</tr>
<tr>
<td>FIPS enabled</td>
<td>&lt;Yes</td>
</tr>
</tbody>
</table>
```

**FIPS Compliance with SecureConnector**

Additional configuration is required to enable SecureConnector to work in a FIPS environment.

**To remain FIPS compliant when working with SecureConnector:**

1. Select **Tools**->**Options**->**HPS Inspection Engine**->**SecureConnector** tab.
2. In the **TLS options** drop-down list, select **TLS version1 (FIPS)**.
Chapter 2: Network Setup

- About the CounterACT Installation
- Appliance Interface Connections
- Setting Up Switch Connections
- Creating an Out-of-Band IP Management Interface
About the CounterACT Installation

CounterACT is designed for installation in various network environments. The configurations shown here demonstrate some of the more typical options and introduce the terminology involved in the installation. Each Appliance requires three types of connections to the network.

If your management network must be separated from the rest of your network, you can create an Out-of-Band management IP interface. This allows the management-related traffic to be routed through a management interface. Other traffic, for example NAC policy remote registry queries and HTTP notifications, is routed through standard response interfaces. See Creating an Out-of-Band IP Management Interface for more information. If you are installing a CounterACT High Availability system, refer to the Resiliency Solutions How-to Guide for more information about the configuration and wiring.

Related Documents

Cisco Switches

For information about port mirroring on Cisco switches, refer to:

Rack Mounting Instructions

For information regarding rack-mounting instructions refer to:

- For Appliances based on hardware revision 2x:
  - CT-100 and CT-1000 Appliances:
  - CT-2000, CT-4000 and CT-10000 Appliances:

- For Appliances based on hardware revision 3x:
  - CT-100 and CT-1000 Appliances:
  - CT-2000, CT-4000 and CT-10000 Appliances

- For Appliances based on hardware revision 5x:
Appliance Interface Connections

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

- Management Interface
- Monitor Interface
- Response Interface

For specific information about setting up monitor and response interfaces to match these connections, refer to the Working with Appliance Channel Assignments section in the CounterACT Console User Manual. Select Help>CounterACT Help from the Console and search for the section.

Management Interface

The management interface allows you to manage CounterACT and perform queries and deep inspection of endpoints. The interface must be connected to a switch port with 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 port must have access to additional services. See Network Access Requirements for more information.

![Diagram of network setup](image)

**Management Interface Setup**

**Configure VLANs on the Management Interface**

This section describes how to configure VLANs on the management interface.

> This configuration is not supported for High Availability deployments.

**To configure the VLAN:**

1. Log in to the CounterACT Appliance as root and run the following command:
   
   `fstool netconfig`

   ```
   CounterACT Machine Network Configuration Options:
   1) Configure network interfaces
   2) Configure default gateway
   3) Configure static routing rules
   4) Restart network services
   5) Quit
   
   Choice (1-5) :
   ```

2. Type 1 to configure the interface as required. After creating the interface, the menu reopens. The following prompt appears.

3. A prompt appears allowing you to choose a physical interface on which to configure the new VLAN.

4. Select (A)Add and choose physical interface to configure the new VLAN on.

5. Specify the VLAN ID (tag) for the VLAN.

**Monitor Interface**

The monitor interface allows the Appliance to monitor and track network traffic. Any available interface can be used as the monitor interface.

Traffic is mirrored to a port on the switch and monitored by the Appliance. The use of 802.1Q VLAN tagging depends upon the number of VLANs being mirrored.
Chapter 2: Network Setup

- **Single VLAN**: When monitored traffic is generated from a single VLAN, the mirrored traffic does not need to be VLAN tagged.

- **Multiple VLANs**: If monitored traffic is from more than one VLAN, the mirrored traffic must be 802.1Q VLAN tagged. See IP Layer Response (for Layer-3-Only Core Switch Installation) for a workaround if this is not possible.

When two switches are connected as a redundant pair, the Appliance must monitor traffic from both switches. See Setting Up Switch Connections for related information.

No IP address is required on the monitor interface.

**Response Interface**

The Appliance responds to traffic using the response interface. Response traffic is used to protect against malicious activity and to perform policy actions. These actions may include, for example, redirecting web browsers or performing session blocking. The related switch port configuration depends upon the traffic being monitored.

Any available interface can be used as the response interface.

- **Single VLAN**: When monitored traffic is generated from a single VLAN, the response port must belong to the same VLAN. In this case, the Appliance requires a single IP address on that VLAN.

- **Multiple VLANs**: If monitored traffic is from more than one VLAN, the response port must also be configured with 802.1Q VLAN tagging for the same VLANs. The Appliance requires an IP address for each monitored VLAN.

**Setting Up Switch Connections**

The Appliance was designed to seamlessly integrate with 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.

Depending upon the configuration, you can combine ports to reduce the number of cables and ports needed for installation.
Recommended Installation: Separate Management, Monitor and Response Ports

The recommended installation uses three separate cables as detailed in Appliance Interface Connections.

![Separate Management, Monitor and Response Ports](image)

Combined Monitor and Response Port

If the switch can receive data packets into a mirrored port (for example, by using the `inpkts enable` keywords on a Cisco Catalyst switch), you can combine the monitor and response ports. This configuration is possible for single VLAN and multiple VLAN installations.

![Combined Monitor and Response Port](image)

**Passive Inline Tap**

Instead of connecting to the switch monitor port, the Appliance can use a passive inline tap.

A passive inline tap requires two monitor ports (one for upstream traffic and one for downstream traffic), except in the case of a recombination tap, which combines the
two duplex streams into a single port. Note that if the traffic on the tapped port is 802.1Q VLAN tagged, then the response port must also be 802.1Q VLAN tagged.

**Passive Inline Tap**

**Active (Injection-Capable) Inline Tap**

The Appliance can use an active inline tap. If the tap is injection capable, the Appliance combines the monitor and response ports so that there is no need to configure a separate response port on the switch. This option can be used regardless of the type of upstream or downstream switch configuration.

**IP Layer Response (for Layer-3-Only Core Switch Installation)**

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 only in situations where the Appliance monitors ports that are not part of any VLAN and so 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.
Chapter 2: Network Setup

Combined Management and Response Port (Single VLAN Only)

If the Appliance is protecting a single VLAN and the management IP is on the same VLAN, you can combine the management and response ports. This configuration is quite common for installation on an access layer switch.

This configuration is not possible on a multiple VLAN installation.

Combined Management, Response and Monitor Port (Single VLAN Only)

If the Appliance is protecting a single VLAN, the management IP is on the same VLAN and the switch is capable of response into the monitor port, then all the cables can be combined into a single port. This configuration is quite common for installation on an access layer switch.

This configuration is not possible on a multiple VLAN installation.

Switch Setting Guidelines

VLAN (802.1Q) Tags

- **Monitoring a Single VLAN**: If the monitored traffic is from a single VLAN, then traffic does not need 802.1Q VLAN tags.
Monitoring Multiple VLANs: If the monitored traffic is from two or more VLANs, then both the monitored and response ports must have 802.1Q VLAN tagging enabled. Monitoring multiple VLANs is recommended 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 port, then 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 the 802.1Q VLAN tags, you must use the IP layer response option.

Additional Guidelines

- In the following cases you should mirror just one interface (that does allow transmit/receive):
  - If the switch cannot mirror both transmitted and received traffic
  - If the switch cannot mirror all the switch traffic
  - If the switch cannot mirror all the traffic over a VLAN

- Verify that you do not overload the mirroring port.

- Some switches (e.g. Cisco 6509) may require that the current port configuration be completely deleted before entering a new configuration. Not deleting old port information often causes the switch to strip 802.1Q tags.

Creating an Out-of-Band IP Management Interface

If the management network must be separate from the rest of your network, create an Out-of-Band IP management interface. When you do this, management related traffic is routed through the management interface, while other traffic (for example, NAC policy remote registry queries and HTTP notifications) is routed through the Out-of-Band interface/s. In this case, each interface has its own IP address.

As well as creating an Out-of-Band IP management interface, you may need to configure a gateway and routing rules.
To create and configure the interface:

1. Log in to the CounterACT Appliance as root and run the following command:
   
   `fstool netconfig`

   CounterACT Machine Network Configuration Options:
   
   1) Configure network interfaces
   2) Configure default gateway
   3) Configure static routing rules
   4) Restart network services
   5) Quit

   Choice (1-5) :

2. Type 1 to configure the interface as required. After creating the interface, the menu reopens.

3. Type either 2 to Configure default gateway or 3 to Configure static routing rules.

   The current Machine Static Routing Table Configuration opens. You will be prompted if no routing has been defined.

   Example configuration:

<table>
<thead>
<tr>
<th>Destination Net IP address</th>
<th>Gateway IP address</th>
<th>Genmask IP address</th>
<th>Iface</th>
</tr>
</thead>
<tbody>
<tr>
<td>13.0.0.0</td>
<td>10.0.4.108</td>
<td>255.0.0.0</td>
<td>eth0</td>
</tr>
<tr>
<td>12.0.0.0</td>
<td>10.0.4.108</td>
<td>255.0.0.0</td>
<td>eth0</td>
</tr>
<tr>
<td>11.0.0.0</td>
<td>10.0.4.109</td>
<td>255.0.0.0</td>
<td>eth0</td>
</tr>
</tbody>
</table>

   (E)dit, (A)dd, (D)elete, (S)ave, (B)ack :

4. Type A and then press Enter to select an interface in which to add a route.

   A menu opens with the interface you selected and its configuration parameters. For example:

<table>
<thead>
<tr>
<th>1) eth0</th>
<th>Address: 10.0.4.197</th>
<th>Netmask: 255.255.255.0</th>
</tr>
</thead>
</table>

   Choice (1-1) :

5. Press Enter to configure the routing.

6. Type S and press Enter to save the configuration.

Additional Example

In this example, the CounterACT device has one in-band interface on the Intranet, and one Out-of-Band interface on the management segment. The mail server also has interfaces on both the Intranet and the management segment. In this example, mail from the CounterACT device needs to be routed through the management segment to the mail server and then sent to the Intranet.
To configure mail routing:

1. Log in to the CounterACT Appliance as root and run the following command:
   ```
   fstool netconfig
   ```

   CounterACT Machine Network Configuration Options:
   1) Configure network interfaces
   2) Configure default gateway
   3) Configure static routing rules
   4) Restart network services
   5) Quit

   Choice (1-5) :

2. Type 3 and then type A to add an interface.

3. When prompted, select the interface to the management segment.

4. Set the **Destination Net IP Address** to the IP address of the mail server.

5. Set the **Destination Genmask** to 255.255.255.255.

6. Set the **Gateway IP Address** to the default gateway of the management interface.
Chapter 3: Appliance Setup and Configuration, and Post-Installation Procedures

- Setting Up an Appliance
- Configuring an Appliance
- Post-Installation Procedures
- Additional Installation Tools
Setting Up an Appliance

This section describes how to set up your Appliance.

1. Remove the Appliance and the power cord from the shipping container.
2. Install the Appliance in the relevant rack location. See Rack Mounting Instructions.
3. Connect the power cord to the power connector on the front or rear panel of the Appliance.
4. Connect the other end of the power cord to a grounded AC outlet.
5. Connect a keyboard, mouse and monitor to the Appliance or set up the Appliance for serial port connection. For information about performing this setup, see Serial Port Setup.

The CT-R Appliance does not have a serial port; you must perform the configuration locally.

6. Power on the Appliance.
7. Configure the Appliance. For information about performing this configuration, see Configuring an Appliance.
8. Connect the Appliance to the network. For information about performing this connection, see Connect an Appliance to the Network.

Serial Port Setup

This section is relevant when setting up both Appliances and the Enterprise Manager.

If it is inconvenient to configure the CounterACT device locally, you can configure the device remotely via a serial port connection.

Verify that you have the following:

- A computer that will act as the client to control the installation process
  - Verify that all output is redirected and displayed on the terminal client.
- A serial cable (supplied with the CounterACT device)
- A terminal client, such as Hyper Terminal (Windows) or minicom (Linux)

To set up a serial port connection:

1. Connect the CounterACT device and the computer. Connect the serial cross cable to the CounterACT device.
2. Configure the terminal client according to the following parameters:
   - Baud: 19200
   - Parity: None
   - Data Bit: 8
   - Stop Bits: 1
− Flow Control: None (*minicom* enables flow control by default—edit its configuration to disable this)
− Emulation: ANSI (at least for *minicom*)

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 that you may not see the command as you type it.

− Type the following for CT-100: `console=ttys0,19200`
− Type the following for CT-1000 or CT-2000: `console=ttys1,19200`

3. Continue the setup procedure.
− CounterACT Appliance: Continue with the next section, Configuring an Appliance.
− Enterprise Manager: Continue with Configuring the Enterprise Manager.

## Configuring an Appliance

This section describes how to configure your Appliance. Most configuration definitions set here can later be changed through the CounterACT Console. Refer to the *CounterACT Console User Manual* for more information.

Some variations may apply to virtual systems. See [Chapter 7: CounterACT Virtual Systems](#) for details.

1. Power on the Appliance. If you have a Forescout 51xx Appliance, the following menu appears:

```plaintext
CounterACT <version>-<build> options:
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) : 
```

If you have a CT-xxxx CounterACT device, you will see either CounterACT 7.0.0 or CounterACT 8.0.0 listed as the version at the top of the menu.

− If you see CounterACT 7.0.0, you can either upgrade to or perform a fresh installation of version 8.0.0. After upgrade or installation to version 8.0.0, you will see the menu listed above.
− If you see CounterACT 8.0.0, the menu offers an option to install CounterACT 7.0.0 or CounterACT 8.0.0, as shown below. If you select
CounterACT 7.0.0, you will not be able to reinstall CounterACT 8.0.0 through the Configuration menu.

CounterACT <version>-<build> options:
1) Install CounterACT 7.0.0-<build>
2) Configure CounterACT 8.0.0-<build>
3) Restore saved CounterACT configuration
4) Identify and renumber network interfaces
5) Configure keyboard layout
6) Turn machine off
7) Reboot the machine

Choice (1-7) :

2. To identify the ports on the rear panel of the Appliance, type 3 and press Enter.

Text is displayed indicating which interface has been detected. The associated port LED blinks on the rear panel.

3. Label the port on the panel so that it is easily identifiable and press Enter.

More text is displayed indicating the next detected interface. The associated port LED now blinks.

4. Label this port as well and press Enter. This process continues until all active interfaces are detected and you have labeled the associated port for each active interface.

5. Once all interfaces have been detected, press Enter.

CounterACT <version>-<build> options:
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) :

6. Type 1 and press Enter.

Select High Availability Mode:
1) Standard Installation
2) High Availability – Primary Node
3) High Availability – Secondary Node

Note: If you are adding a node to an existing primary/secondary active node, select option 3.

Choice (1-3) [1] :
7. Press Enter.

`>>>>>> CounterACT Initial Setup <<<<<<<`

You are about to setup CounterACT. During the initial setup process you will be prompted for basic parameters used to connect this machine to the network. When this phase is complete, you will be instructed to complete the setup from the CounterACT Console.

Continue ? (yes/no) [yes] :

8. Press Enter.

`>>>>>> Select CounterACT Installation Type <<<<<<<`

1) CounterACT Appliance
2) CounterACT Enterprise Manager

Choice (1-2) :

9. Type 1 and press Enter. The setup is initialized. This may take a few moments.

`>>>>>> Enter Machine Description <<<<<<<`

Enter a short description of this machine (e.g. New York office).

Description :

10. Type a description and press Enter.

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

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

Administrator password :

11. Type the string that is to be your password (the string is not echoed to the screen) and press Enter. You are asked to confirm the password.

Administrator password (confirm) :

12. Retype the password (the string is not echoed to the screen) and press Enter.

`>>>>>> Set Host Name <<<<<<<`

It is recommended to choose a unique host name.

Host name :

13. Type a host name and press Enter. The host name can be used when logging into the Console. In addition, it is displayed on the Console to help you identify the CounterACT Appliance that you are viewing. The hostname should not exceed 13 characters.
The **Management interface** prompt is displayed (subsequent prompts are displayed after you enter a value for the preceding prompt):

```
>>>>>> Configure Network Settings <<<<<<
Management interface (one of: <interface_list>) :
Management IP address :
Network mask [255.255.255.0] :
Default gateway :
Domain name :
DNS server addresses :
Management IPv6 address or ’none’ :
```

- 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 addresses as well 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.

14. **Type a value at the Management interface prompt and press Enter.**
15. **Type a value at each subsequent prompt and press Enter.** After pressing Enter at the last prompt, the setup summary is displayed.

```
>>>>>> Setup Summary <<<<<<
Role:                 Appliance
Host name:            <user_entered_value>
Description:          <user_entered_value>
Management Interface: < user_entered_value >,
eth<n>,                Interface:
Netmask:              <user_entered_value>
Default gateway:      <user_entered_value>
DNS server:           <user_entered_value>
Domain name:          <user_entered_value>
(T)est,(R)econfigure,(D)one :
```

16. **To test the configuration, type T and press Enter.** The test verifies the following:
   - Storage I/O performance (Virtual systems only)
   - Connected interfaces
   - Connectivity of the default gateway
   - DNS resolution
   
   Results indicate if any test failed so that you can reconfigure if necessary.
If there are no failures, the following is displayed:

```
Checking eth0...OK. (100Mb/s Full duplex)
Checking default gateway...OK.
Checking DNS resolution...OK.
```

Press ENTER to review configuration summary.

17. **Press Enter.** The setup summary is displayed again.

18. **To complete the installation,** type **D** and press **Enter.**

```
Finalizing CounterACT setup, this will take a few minutes
```

After setup is complete, the following is displayed:

```
Starting CounterACT service -
```

After the service starts, the following is displayed:

```
>>>>>> CounterACT Initial Setup is Complete <<<<<<
CounterACT Console will guide you through the rest of the Appliance setup.
Use the following URL to install the CounterACT Console:
  http://<management_interface_IP>/install
```

Press ENTER to clear the screen.

19. **Press Enter.**

You can now start to work using the demo license, which is valid for 30 days. During this period, you should receive a permanent license from Forescout and place it in an accessible folder on your disk or network. Install the license from this location before the 30-day demo license expires. (If necessary, you can request an extension to the demo license.)

You will be alerted that your license is about to expire in a number of ways:

- Through periodic email reminders.
- Through the Status and License columns in the CounterACT Devices pane (accessible through the **Options** icon from the Console), which indicates how many days remain until the license expires.
- Through the Status pane in the CounterACT Devices pane, which also shows the time until the license expires.
- Through an icon and tooltip on the Console, Status bar.

If you are working with a CounterACT virtual system, the demo license is not installed automatically at this stage. See [CounterACT Virtual Device Deployment in VMware](http://www.Forescout.com/kb) for details.

For details about requesting a permanent license, refer to any of the following:

- *CounterACT Console User Manual* located on the CounterACT DVD in the `/docs` folder
- Console Online Help
Post-Installation Procedures

After installing an Appliance, perform the following tasks:

- Connect an Appliance to the Network
- Integrate with Remote System Management
- Verify the Management Interface Connection
- Verify Switch/Appliance Connectivity
- Perform a Ping Test
- Generate a Configuration Summary for an Appliance
- Configure Password Protection for the Boot Loader
- Install the CounterACT Console. See Chapter 6: Installing the CounterACT Console.
- Run the Initial Setup Wizard. Refer to the CounterACT Console User Manual.

Connect an Appliance to the Network

Connect the monitor and response interface cables to Ethernet ports on the rear panel of the Appliance and note the Appliance interfaces associated with the ports. You will need this information to define a channel when you run the Initial Setup Wizard from the CounterACT Console (see Running the Initial Setup Wizard on the Console). (During Appliance configuration, you discovered which interface each Ethernet port connects to and labeled the ports accordingly.)
Forescout has tested and approved the following Finisar SFPs for Appliances. You can replace the Forescout-supplied SFPs with one of these SFPs for deployment flexibility.

1Gb/s SFPs only work with 1Gb/s ports, and 10Gb/s SFPs only work with 10Gb/s ports.

<table>
<thead>
<tr>
<th>SFP Model</th>
<th>Details</th>
<th>Supported Appliances</th>
</tr>
</thead>
<tbody>
<tr>
<td>FCLF8521P2BTL</td>
<td>1Gb/s, 1000BASE-T</td>
<td>CT-xxxx</td>
</tr>
<tr>
<td>FTLF1318P3BTL</td>
<td>1Gb/s, 1000BASE-LX</td>
<td></td>
</tr>
<tr>
<td>FTLF8519P3BNL</td>
<td>1Gb/s, 1000BASE-SX</td>
<td></td>
</tr>
<tr>
<td>FTLX1471D3BCL</td>
<td>10Gb/s 10GBase-LR SFP+</td>
<td>CT-xxxx, based on hardware revision 4x or lower</td>
</tr>
<tr>
<td>FTLX8571D3BCL</td>
<td>10Gb/s 10GBase-SR SFP+</td>
<td></td>
</tr>
<tr>
<td>FTLX1471D3BCV</td>
<td>10G/1G Dual Rate</td>
<td>CT-xxxx, based on hardware revision 5x</td>
</tr>
<tr>
<td></td>
<td>(10GBase-LR and 1000BASE-LX)</td>
<td></td>
</tr>
<tr>
<td>FTLX8574D3BCV</td>
<td>10G/1G Dual Rate</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(10GBase-SR and 1000BASE-SX)</td>
<td></td>
</tr>
<tr>
<td>571540003 (AMPHENOL)</td>
<td>Direct Attach 10G</td>
<td></td>
</tr>
</tbody>
</table>

Integrate with Remote System Management

This integration is not applicable to virtual systems.

You can integrate with Remote System Management using RMM3 or iDRAC, depending on your Appliance model and hardware revision.

- Integrating Appliances Based on Hardware Revision 2x with RMM3
- Integrating Appliances Based on Hardware Revision 3x/4x/5x with iDRAC

Remote System Management features of CounterACT Appliances (RMM3 or iDRAC) are intended to be used on a separate management network. They are not designed or intended to be placed on or connected to a widely-accessible LAN or to the Internet. Doing so could expose the connected system to security and other risks. Along with locating the remote management ports on a separate management subnet, users should isolate the management subnet / VLAN, and limit access to the subnet / VLAN to authorized administrators.

Integrating Appliances Based on Hardware Revision 2x with RMM3

When the following Appliances are implemented on hardware revision 2x, they support the Intel Remote Management Module 3 (RMM3):

- CT-100
- CT-1000
The RMM3 module is an integrated server system solution that gives you location-independent and OS-independent remote access over the LAN or Internet to CounterACT devices. Use the module to carry out KVM access, for power on/off/reset and to perform troubleshooting and maintenance tasks.

Perform the following to work with the module:

- **Enable and Configure the RMM3**
- **Connect the Module to the Network**

**Enable and Configure the RMM3**

You must change BIOS settings on the Appliance to enable the RMM.

**To change BIOS settings on an Appliance:**

1. Boot the Appliance.
2. Select **F2** to enter the BIOS setup.
3. Navigate to the Server Management tab and select **BMC LAN Configuration**.
4. In the **Intel (R) RMM3 LAN configuration** section, define **IP source** and (optional) **BMC DHCP host name**.

5. Navigate to the **User configuration** section.

6. Enable at least one of the users in the list and set a password. (All users are disabled by default).

7. Save the BIOS settings and reboot.
Connect the Module to the Network

The RMM3 connects to an Ethernet network. It is customary to connect it to a management network. The following diagram illustrates the RMM3 port location on the rear panel of the CT-1000 Appliance.

For more information, refer to the Remote Management Module 3 User Guide:

Integrating Appliances Based on Hardware Revision 3x/4x/5x with iDRAC

The Integrated Dell Remote Access Controller (iDRAC) is an integrated server system module that gives you location-independent/OS-independent remote access over the LAN or Internet to CounterACT Appliances/Enterprise Managers. Use the module to support KVM access, power on/off/reset and to 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
- Log In 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 Appliance.
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 iDRAC. 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.

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:

![IDRAC port location](image)

Log In to iDRAC

To log in to iDRAC:

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

![iDRAC login](image)

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

3. Select Submit.

For more information, refer to the iDRAC User's Guide:


- It is very important to update the default credentials.

Verify the Management Interface Connection

Test the management interface connection to verify that the management interface is correctly configured.
To run the test:

1. Log in to the Appliance and run the following command:
   
   ```bash
   fstool linktest
   ```

<table>
<thead>
<tr>
<th>Management Interface status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pinging default gateway information</td>
</tr>
<tr>
<td>Ping statistics</td>
</tr>
<tr>
<td>Performing Name Resolution Test</td>
</tr>
<tr>
<td>Test summary</td>
</tr>
</tbody>
</table>

Verify Switch/Appliance Connectivity

Verify that the switch is properly connected to the Appliance.

To verify connectivity:

1. Log in to the Appliance and run the following command for each interface detected:
   
   ```bash
   fstool ifcount [-v] interfaceA [interfaceB] [interfaceC] [...]
   ```

   This tool works in two modes: per interface (default) or per VLAN (via the `-v` flag). The mode can be changed while the tool is running.

   The tool continuously displays network traffic on the specified interfaces. The display includes the total bits per second and the percentage of traffic for the specified interfaces.

2. Verify that:
   - The monitor interface primarily sees more than 90% mirrored traffic.
   - The response interface primarily sees broadcast traffic.
   - Both the monitor and response interfaces see the expected VLANs.

3. If you do not see any traffic, verify that the interface is up by running the following command:
   
   ```bash
   ifconfig <interface_name> up
   ```

   **Example 1:**

   To view traffic information for interfaces, run the following command:
   
   ```bash
   fstool ifcount eth0 eth1
   ```

<table>
<thead>
<tr>
<th>Interface</th>
<th>Total</th>
<th>Broadcast</th>
<th>Mirrored</th>
<th>To my MAC</th>
<th>From my MAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth0</td>
<td>3Kbps</td>
<td>42.3%</td>
<td>0.0%</td>
<td>14.1%</td>
<td>43.7%</td>
</tr>
<tr>
<td>eth1</td>
<td>475bps</td>
<td>0.0%</td>
<td>100.0%</td>
<td>0.0%</td>
<td>0.0%</td>
</tr>
</tbody>
</table>

   - **To my MAC**: The destination MAC address is the Appliance MAC address
   - **From my MAC**: Traffic sent by this Appliance (the source MAC address is the Appliance MAC address; the destination can be broadcast or unicast)
Example 2:

To view traffic information for VLANs, run the following command:

```
ftime ifcount -v eth3
```

<table>
<thead>
<tr>
<th>Interface/Vlan</th>
<th>Total</th>
<th>Broadcast</th>
<th>Mirrored</th>
<th>To my MAC</th>
<th>From my MAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth3.untagged</td>
<td>4Mbps</td>
<td>0.2%</td>
<td>99.8%</td>
<td>0.0%</td>
<td>0.0%</td>
</tr>
<tr>
<td>eth3.1</td>
<td>9Mbps</td>
<td>0.0%</td>
<td>100.0%</td>
<td>0.0%</td>
<td>0.0%</td>
</tr>
<tr>
<td>eth3.2</td>
<td>3Mbps</td>
<td>0.1%</td>
<td>99.9%</td>
<td>0.0%</td>
<td>0.0%</td>
</tr>
<tr>
<td>eth3.4</td>
<td>542bps</td>
<td>100.0%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
</tr>
<tr>
<td>eth3.20</td>
<td>1Kbps</td>
<td>100.0%</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
</tr>
</tbody>
</table>


- **To my MAC**: The destination MAC address is the Appliance MAC address
- **From my MAC**: Traffic sent by this Appliance (the source MAC address is the Appliance MAC address; the destination can be broadcast or unicast)

Perform a Ping Test

Run the following command from the Appliance to a network desktop to verify connectivity:

```
Ping <network_desktop_IP_address>
```

Generate a Configuration Summary for an Appliance

You can generate a configuration summary of Appliances in your enterprise including, for example, the Appliance version, channel, switch and additional networking information. This makes it easier to:

- Identify a missing configuration at a glance.
- Document an Appliance configuration so that a replacement system can be easily configured.

To generate a summary:

1. Log in to the Appliance and run the following command:

```
fstime netconfig_sum
```

The following screens opens:

```
Version information
Version
Build number
Internal Version
Build date
Host information
Hostname
Domain name
Dns
Network information
Gateway
eth0 Address: Netmask:
Channel Configuration Information
```

Forescout Installation Guide 48
Configure Password Protection for the Boot Loader

CounterACT devices use the GNU GRUB boot loader. To prevent malicious changes to boot settings, you can protect access to these settings by requiring a password.

- Once you define a boot loader password, you cannot disable password protection or define a null password.

To configure password protection for the boot loader:

1. Log in to the CounterACT device as root.
2. Submit the following command:
   ```
   fstool grub -setpassword
   ```
3. The following prompt appears:
   ```
   Enter grub password:
   ```
4. Enter the password. The following prompt appears:
   ```
   Re-type grub password:
   ```
5. Re-enter the password. The following prompt appears:
   ```
   Successfully updated grub password.
   ```

The system prompts for this password when users try to edit boot loader settings.

Additional Installation Tools

This section details additional tools that can be used for the installation.

- Configuring the Interface Speed/Duplex
- Restoring Appliance System Settings
Configuring the Interface Speed/Duplex

You can modify the default interface speed and duplex values.

1. Log in to the Appliance and run the following command:
   
   \[
   \text{fstool ethset}
   \]

   eth0 (e1000) Config: Auto Status: 1000Mb/s, Full
   eth1 (e1000) Config: Auto Status: 1000Mb/s, Full
   eth2 (e1000) Config: Auto Status: 1000Mb/s, Full
   eth3 (e1000) Config: Auto Status: 1000Mb/s, Full

   E(dit),B(link),S(how),Q(uit) :

   (This is an example; the actual display will depend on your setup.)

2. Type `b` and press Enter.

   Choose interface to blink (one of: eth0, eth1, eth2, eth3, all):

3. Type the name of an interface and press Enter.

   Blinking eth<n>. Press Enter to continue.

4. Press Enter.

   The list of interfaces is displayed again:

   eth0 (e1000) Config: Auto Status: 1000Mb/s, Full
   eth1 (e1000) Config: Auto Status: 1000Mb/s, Full
   eth2 (e1000) Config: Auto Status: 1000Mb/s, Full
   eth3 (e1000) Config: Auto Status: 1000Mb/s, Full

   E(dit),B(link),S(how),Q(uit) :

5. Type `e` and press Enter.

   Choose interface to configure (one of: eth0, eth1, eth2, eth3) :

6. Type the name of an interface and press Enter.

   Speed (one of : 10, 100, Auto) [Auto] :

7. Type a speed and press Enter.

   Applying new configuration.
   Saving new eth<n> configuration. This may take a few seconds.

8. When list of interfaces is displayed again, type `q` and press Enter.

Restoring Appliance System Settings

Backup and restore procedures allow you to save your system settings and later restore them to an Appliance. Use this feature in cases of Appliance hard drive failures or when data on an Appliance is lost for any other reason. Refer to the CounterACT Console User Manual for more information.
To restore system settings:

1. Power on the Appliance.

   CounterACT <version>-<build> options:
   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) :

2. Type 2 and press Enter.

   Restore options:
   1) Restore from USB storage device
   2) Restore from CD-ROM
   3) Get shell prompt
   4) Reset to factory setup
   5) Cancel

   Choice (1-5) :

3. Type the number of the relevant restore option and press Enter.

   The restore process will now search for backup files in the selected media. Note that backup file names must have a ".fsb" extension. Insert the media where the backup file reside and press ENTER to continue.

4. Insert the media where the backup file resides and press Enter.

   All FSB files found on the media are displayed.

   Searching for backup files in <selected_storage_type>...

   Choose backup file:
   1) <backup_file1_name>.fsb
   2) <backup_file2_name>.fsb
   3) Cancel

   Choice (1-3) :

5. Type the number of the relevant backup file and press Enter.

   Verifying <full_path_and_file_name>.fsb...
   -------------------------
   Backup Volume Information
   -------------------------
   Product     : CounterACT
   Host-name   : <host_name>
   Address     : <IP_address>
   Backup date : <date_and_time_stamp>

   Verifying Backup volume, please wait.

   Restore? (yes/no) :
6. Type **yes** and press **Enter**.

```
Setup the restored machine in High Availability mode? (yes/no) [no]
```

7. Press **Enter**:

```
******* CounterACT <version>-<build> Restore *******

>>> Installing Packages <<<
Checking stored Packages...... done.>>> Configuring the System <<<
>>> Installing Database <<<Creating database... done....
Restoring... done.
Installation log written to /tmp/CounterACT-install.log
The Operating System will now reboot in order to complete the CounterACT restore process.
```

When you backup and restore system settings using two different CounterACT devices, the interface numbering may change. To correlate the new interface numbering with the correct interfaces you must run `fstool ethtest` and reassign the interfaces accordingly.

**Restoring as a High Availability Device**

Note that you can select to restore system settings to a High Availability device, even if the backup was taken from a standard Appliance. If the backup was taken on a standard Appliance and you want to restore as High Availability, you are prompted for the required High Availability parameters. Refer to the section on High Availability Backup and Restore in the Resiliency Solutions How-to Guide for details about working with High Availability systems.
Chapter 4: Enterprise Manager Setup and Configuration, and Post-Installation Procedures

- About the Installation
- Setting Up the Enterprise Manager
- Configuring the Enterprise Manager
- Post-Installation Procedures
- Restoring Enterprise Manager System Settings
About the Installation

This chapter details the Enterprise Manager setup and configuration procedures. Many of the configuration definitions set here can later be updated through the CounterACT Console. Refer to the CounterACT Console User Manual for more information.

Some variations may apply to virtual systems. See About CounterACT Virtual Systems for details.

Setting Up the Enterprise Manager

This section describes how to set up your Enterprise Manager.

1. Remove the Enterprise Manager and the power cord from the shipping container.
2. Connect the power cord to the power connector on the rear panel of the Enterprise Manager.
3. Connect the other end of the power cord to a grounded AC outlet.
4. Connect a keyboard, mouse and monitor to the Enterprise Manager or set up the Enterprise Manager for serial port connection. See Serial Port Setup.
5. Power on the Enterprise Manager from the front panel.
6. If the Enterprise Manager is installed in the location at which it will operate, connect it to the network. For information about performing this connection, see Connect the Enterprise Manager to the Network. If the Enterprise Manager is not in its final location, you can perform the Enterprise Manager configuration now and connect it to the network later.

Configuring the Enterprise Manager

This section describes how to configure the Enterprise Manager.

1. Power on the Enterprise Manager. If you have a Forescout 51xx device, the following menu appears:

   CounterACT <version>-<build> options:
   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) :

   If you have a CT-xxxx CounterACT device, you will see either CounterACT 7.0.0 or CounterACT 8.0.0 listed as the version at the top of the menu.

   – If you see CounterACT 7.0.0, you can either upgrade to or perform a fresh installation of version 8.0.0. After upgrade or installation to version 8.0.0, you will see the menu listed above.
If you see CounterACT 8.0.0, the menu offers an option to install CounterACT 7.0.0 or CounterACT 8.0.0, as shown below. If you select CounterACT 7.0.0, you will not be able to reinstall CounterACT 8.0.0 through the Configuration menu.

CounterACT <version>-<build> options:
1) Install CounterACT 7.0.0-<build>
2) Configure CounterACT 8.0.0-<build>
3) Restore saved CounterACT configuration
4) Identify and renumber network interfaces
5) Configure keyboard layout
6) Turn machine off
7) Reboot the machine

Choice (1-7) :

2. To identify the ports on the rear panel of the Enterprise Manager, type 3 and press Enter.

Text is displayed indicating which interface has been detected. The associated port LED blinks on the rear panel.

3. Label the port on the panel so that it is easily identifiable and press Enter.

More text is displayed indicating the next detected interface. The associated port LED now blinks.

4. Label this port as well and press Enter. This process continues until all active interfaces are detected and you have labeled the associated port for each active interface.

5. Once all interfaces have been detected, press Enter.

CounterACT <version>-<build> options:
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) :

6. Type 1 and press Enter.

Select High Availability Mode:
1) Standard Installation
2) High Availability – Primary Node
3) High Availability – Secondary Node

Note: If you are adding a node to an existing primary/secondary active node, select option 3.

Choice (1-3) [1] :
7. Press Enter.

   >>>>>> CounterACT Initial Setup <<<<<<
   
   You are about to setup CounterACT. During the initial setup process you will be prompted for basic parameters used to connect this machine to the network. When this phase is complete, you will be instructed to complete the setup from the CounterACT Console.
   
   Continue ? (yes/no) [yes] :

8. Press Enter.

   >>>>>> Select CounterACT Installation Type <<<<<<
   
   1) CounterACT Appliance
   2) CounterACT Enterprise Manager
   
   Choice (1-2) :

9. Type 2 and press Enter. The setup is initialized. This may take a few moments.

   >>>>>> Enter Machine Description <<<<<<
   
   Enter a short description of this machine (e.g. New York office).
   
   Description [Enterprise Manager] :

10. Type a description and press Enter.

   >>>>>> Set Administrator Password <<<<<<
   
   This password will be used to log in as ‘root’ to the machine Operating System and as ‘admin’ to the CounterACT Console. The password must be between 6 and 15 characters long and must contain at least one non-alphabetic character.
   
   Administrator password :

11. Type the string that is to be your password (the string is not echoed to the screen) and press Enter. You are asked to confirm the password:

   Administrator password (confirm) :

12. Retype the password (the string is not echoed to the screen) and press Enter.

   >>>>>> Set Host Name <<<<<<
   
   It is recommended to choose a unique host name.
   
   Host name :

13. Type a host name and press Enter.

   The host name can be used when logging in to the Console. In addition, it is displayed on the Console to help you identify the CounterACT device that you are viewing. The hostname should not exceed 13 characters.
The **Management interface** prompt is displayed (subsequent prompts are displayed after you enter a value for the preceding prompt): 

```plaintext
>>>>>> Configure Network Settings <<<<<<<
Management interface (one of: <interface_list>) :
Management IP address :
Network mask [255.255.255.0] :
Default gateway :
Domain name :
DNS server addresses :
Management IPv6 address or ‘none’ :
```

- The number of management interfaces listed depends on the Enterprise Manager 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 addresses as well but you may need to include an external-resolving DNS server. As nearly all DNS queries performed by the Enterprise Manager will be for internal addresses, the external DNS server should be listed last.

14. Type a value at the **Management interface** prompt and press **Enter**.

15. Type a value at each subsequent prompt and press **Enter**.

After pressing **Enter** at the last prompt, the setup summary is displayed:

```plaintext
>>>>>> Setup Summary <<<<<<<
Role:                 Enterprise Manager
Host name:            <user_entered_value>
Description:          <user_entered_value>
Management Interface: < user_entered_value >, Interface:
eth<n>, Netmask:
DNS server:           <user_entered_value>
Domain name:          <user_entered_value>
(T)est,(R)econfigure,(D)one :
```

16. To test the configuration, type **T** and press **Enter**. The test verifies the following:

- Storage I/O performance (Virtual systems only)
- Connected interfaces
- Connectivity of the default gateway
- DNS resolution

Results indicate if any test failed so that you can reconfigure if necessary.
If there are no failures, the following is displayed:

```
Checking eth0...OK. (100Mb/s Full duplex)
Checking default gateway...OK.
Checking DNS resolution...OK.
```

Press ENTER to review configuration summary

17. Press **Enter**. The setup summary is displayed again.

18. To complete the installation, type **D** and press **Enter**.

```
Finalizing CounterACT setup, this will take a few minutes
```

After setup is complete, the following is displayed:

```
Starting CounterACT service -
```

After the service starts, the following is displayed:

```
>>>>>> CounterACT Initial Setup is Complete <<<<<<
CounterACT Console will guide you through the rest of the Enterprise Manager setup.
Use the following URL to install the CounterACT Console:
http://<management_interface_IP>/install
```

Press ENTER to clear the screen

19. Press **Enter**.

You can now start to work using the demo license, which is valid for 30 days. During this period, you should receive a permanent license from Forescout and place it in an accessible folder on your disk or network. Install the license from this location before the 30-day demo license expires. (If necessary, you can request an extension to the demo license.)

You will be alerted that your license is about to expire in a number of ways:

- Through periodic email reminders.
- Through the Status and License columns in the CounterACT Devices pane (accessible through the **Options** icon from the Console), which indicates how many days remain until the license expires.
- Through the Status pane in the CounterACT Devices pane, which also shows the time until the license expires.
- Through an icon and tooltip on the Console, Status bar.

If you are working with a CounterACT virtual system, the demo license is not installed automatically at this stage. See **CounterACT Virtual Device Deployment in VMware** for details.

For details about requesting a permanent license, refer to any of the following:

- **CounterACT Console User Manual** located on the CounterACT DVD in the `/docs` folder
- Console Online Help
Post-Installation Procedures

After installing the Enterprise Manager, perform the following tasks:

- Connect the Enterprise Manager to the Network
- Integrate the Enterprise Manager with Remote System Management

Connect the Enterprise Manager to the Network

During the Enterprise Manager configuration, you are asked to specify the network interface. Once this parameter is determined, connect the interface cable to the associated Ethernet port on the rear panel of the Enterprise Manager.

Integrate the Enterprise Manager with Remote System Management

CounterACT supports integration with both Integrated Dell Remote Access Controller (iDRAC) and Intel Remote Management Module 3 (RMM3). Both are integrated server system solutions that give you location-independent and OS-independent remote access over the LAN or Internet to CounterACT devices. Use the modules to carry out KVM access and power on/off/reset, and perform troubleshooting and maintenance tasks.

See Integrate with Remote System Management for more details.

This integration is not applicable to virtual systems.

Restoring Enterprise Manager System Settings

Backup and restore procedures allow you to save your system settings and later restore them to an Enterprise Manager. Use this feature in cases of Enterprise Manager hard drive failures or when data on an Enterprise Manager is lost for any other reason. Refer to the CounterACT Console User Manual for more information.

To restore system settings:

1. Power on the Enterprise Manager.

```
  CounterACT <version>-<build> options:
  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) : 
```
2. Type 2 and press **Enter**.

<table>
<thead>
<tr>
<th>Restore options:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Restore from USB storage device</td>
</tr>
<tr>
<td>2) Restore from CD-ROM</td>
</tr>
<tr>
<td>3) Get shell prompt</td>
</tr>
<tr>
<td>4) Reset to factory setup</td>
</tr>
<tr>
<td>5) Cancel</td>
</tr>
</tbody>
</table>

   Choice (1-5) : 

3. Type the number of the relevant restore option and press **Enter**.

   The restore process will now search for backup files in the selected media. Note that backup file names must have a ".fsb" extension. Insert the media where the backup file reside and press ENTER to continue.

4. Insert the media where the backup file resides and press **Enter**.

   All FSB files found on the media are displayed.

   - The backup file name can only contain alphanumeric characters. Special characters are not allowed.

<table>
<thead>
<tr>
<th>Searching for backup files in &lt;selected_storage_type&gt;...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choose backup file:</td>
</tr>
<tr>
<td>1) &lt;backup_file1_name&gt;.fsb</td>
</tr>
<tr>
<td>2) &lt;backup_file2_name&gt;.fsb</td>
</tr>
<tr>
<td>3) Cancel</td>
</tr>
</tbody>
</table>

   Choice (1-3) :

5. Type the number of the relevant backup file and press **Enter**.

<table>
<thead>
<tr>
<th>Backup Volume Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product : CounterACT</td>
</tr>
<tr>
<td>Host-name : &lt;host_name&gt;</td>
</tr>
<tr>
<td>Address : &lt;IP_address&gt;</td>
</tr>
<tr>
<td>Backup date : &lt;date_and_time_stamp&gt;</td>
</tr>
</tbody>
</table>

   Verifying Backup volume, please wait.

   Restore? (yes/no) : 

6. Type **yes** and press **Enter**.

   Setup the restored machine in High Availability mode? (yes/no) [no]
7. Press **Enter**.

```
******** CounterACT <version>-<build> Restore *******

>>> Installing Packages <<<
Checking stored Packages...... done.>>> Configuring the System <<<

>>> Installing Database <<<Creating database... done....
Restoring... done.
Installation log written to /tmp/CounterACT-install.log
The Operating System will now reboot in order to complete the CounterACT restore process.
```

When you backup and restore system settings using two different CounterACT devices, the interface numbering may change. To correlate the new interface numbering with the correct interfaces you must run `fstool ethtest` and reassign the interfaces accordingly.

**Restoring as a High Availability Device**

Note that you can select to restore system settings to a High Availability device, even if the backup was taken from a standard Enterprise Manager. If the backup was taken on a standard Enterprise Manager and you want to restore as High Availability, you are prompted for the required High Availability parameters. Refer to the section on High Availability Backup and Restore in the Resiliency Solutions How-to Guide for details about working with High Availability systems.
Chapter 5: Upgrading CounterACT Devices

- Upgrading to a New Version
- Gradual Upgrade
Upgrading to a New Version

The Installer program automatically identifies an earlier CounterACT version on your system. Upgrade options allow you to either maintain the configuration parameters from the previous version or define new parameters.

Review the CounterACT Release Notes for important information before performing an upgrade. The CounterACT Release Notes are located on your CounterACT DVD under the /docs folder and on the Forescout website.

The ISO file is too large for a CD and so is provided on DVD. For older CounterACT Appliances that cannot natively mount a DVD, Forescout provides an IMG file to install via a USB memory device.

The following upgrade options are supported:

- Upgrading with the DVD
- Upgrading via a USB Memory Device
- Upgrading from the Console

For High Availability upgrade information, refer to the section on upgrading High Availability systems in the Resiliency Solutions How-to Guide.

Upgrading with the DVD

You can perform the software upgrade using the DVD provided by CounterACT.

To upgrade the Appliance from the DVD:

1. Insert the CounterACT Installation DVD into its drive.
2. Log in to the Appliance as root and run the following commands:
   ```
   mount /mnt/cdrom
   cd /mnt/cdrom
   ./setup
   ```

   A prompt indicates that you are about to upgrade the software. The procedures are detailed in Configuring an Appliance. You can maintain previous values, which appear as the defaults, or define new values.

Upgrading via a USB Memory Device

You will need a USB memory device with at least 4GB of free memory.

To install the image on the USB memory device under Linux:

1. Download the image from the CounterACT Product Downloads page to a Linux machine.
2. Plug in the USB memory device and determine its identity.
3. Log in to the Appliance/Linux machine and run the following command:
   ```
   dd if=<image_location> of=/dev/sd<x> bs=10M
   ```
   Where sd<x> can be, for example, sdc, sdd or sde depending on the memory device.
Note that the command must be `/dev/sd<x>` and not `/dev/sd<x>1` (that is, use the whole device rather than a single partition on the device).

**To install the image on the USB memory device under Windows:**

1. Download the image from the Forescout website to a Windows machine.
2. Download (from https://launchpad.net/win32-image-writer) and install Image Writer for Windows on the Windows machine. Image Writer for Windows is available as a zip file; installation involves copying its content to a directory.
   
   A window opens that allows you to select the image and the USB drive.

To upgrade the CounterACT software from the USB memory device, you must configure the CounterACT device BIOS so that the device boots from the USB memory device.

**To change the BIOS settings on a CounterACT device:**

1. Boot the Appliance.
2. Select F2 to enter the BIOS setup.
3. Change the default boot device.
   
   The exact instructions are model and revision dependent.
4. Save the BIOS settings and reboot.
   
   A prompt indicates that you are about to upgrade the software. These procedures are detailed in Configuring an Appliance. You can maintain previous values, which appear as the defaults, or define new values.
5. Remember to reset the BIOS settings after you complete the installation.

**Upgrading from the Console**

You can perform the software upgrade from the Console. If you upgrade from the Console, you cannot change the installation parameters. For complete procedures, refer to the CounterACT Console User Manual.

**Gradual Upgrade**

You can gradually upgrade a CounterACT deployment. This may be required for large deployments where simultaneous upgrade is not desired, is not practical or is not allowed by the corporate IT policy. The gradual upgrade process also allows you to upgrade a single Plugin or Service Pack, test and review the upgrade to verify proper functionality, and then upgrade some or all of the remaining Plugins and Service Packs.

A temporary Enterprise Manager is used to facilitate the gradual upgrade. During the transition period, two Enterprise Managers are simultaneously active. The permanent Enterprise Manager manages the Appliances running the new version, while the temporary Enterprise Manager manages the Appliances running the old version.
For more information, refer to the CounterACT Deployment, Service Packs and Plugins Gradual Upgrade Guide.
Chapter 6: Installing the CounterACT Console

- About the CounterACT Console Installation
- Logging In
- Installing the Cumulative Update Pack
- Running the Initial Setup Wizard on the Console
- Uninstalling Previous Versions
About the CounterACT Console Installation

The CounterACT Initial Setup Wizard assists you in quickly installing the CounterACT Console software for both the Appliance and Enterprise Manager. When logging in, enter the CounterACT device login credentials that you defined during these installations. The login determines to which CounterACT device to log in, based on the credentials.

The following options are available for installing the Console:

- Install from the CounterACT Support Page
- Install from the Installation DVD
- Install from a Browser at Your Appliance

It is recommended to install the Console from the CounterACT Support Page to ensure that you receive the latest version of the Console.

Information Required for the Installation

Before installing the Console, gather the information listed below and enter it in the Value column for easy access.

<table>
<thead>
<tr>
<th>Information Required by Wizard</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTP server address used by your organization (optional)</td>
<td></td>
</tr>
<tr>
<td>Internal mail relay IP address to allow delivery of email alerts if SMTP traffic is not allowed from the Appliance (optional)</td>
<td></td>
</tr>
<tr>
<td>CounterACT administrator email address</td>
<td></td>
</tr>
<tr>
<td>Monitor and response interfaces</td>
<td></td>
</tr>
<tr>
<td>For segments/VLANs with no DHCP, the network segment/VLANs to which the response interface is directly connected and a permanent IP address to be used by CounterACT at each such VLAN</td>
<td></td>
</tr>
<tr>
<td>IP address range that this Appliance will monitor (all the internal addresses, including unused addresses)</td>
<td></td>
</tr>
<tr>
<td>LDAP user account information and the LDAP server IP address</td>
<td></td>
</tr>
<tr>
<td>Domain credentials, including the domain administrative account name and password</td>
<td></td>
</tr>
<tr>
<td>Authentication servers, so that CounterACT can analyze which network hosts have successfully been authenticated</td>
<td></td>
</tr>
<tr>
<td>Switch IP Address, Vendor and SNMP Parameters</td>
<td></td>
</tr>
</tbody>
</table>
Install from the CounterACT Support Page

To install from the CounterACT Support Page:


2. Select the CounterACT Console Setup file. The initial CounterACT installation screen opens.

3. Select the download link required. The download process initiates and the Choose Install Folder screen opens.
4. Accept the default location or define a new location to install the Console and then select **Next**. The Choose Shortcut Folder screen opens.

![Choose Shortcut Folder Screen](image1)

5. Select a location for product icons and then select **Next**. The Pre-Installation Summary screen opens.

![Pre-Installation Summary Screen](image2)
6. Review the settings and select **Install**. The Installing CounterACT screen opens and the Console installation begins.

![Installing CounterACT Screen](image1.png)

7. After installation is complete, the Install Complete screen opens.

![Install Complete Screen](image2.png)

8. Select **Done**.
Chapter 6: Installing the CounterACT Console

Install from the Installation DVD

To install the CounterACT Console from the DVD:
1. Insert the Installation DVD into the DVD drive of the PC that will run the Console software.
2. Locate and run ManagementSetup.htm.
3. Follow the on-screen instructions.

Install from a Browser at Your Appliance

This option is not available when upgrading.

To use the installation software built into your Appliance to install the CounterACT Console:
1. Open a browser window from the PC that will run the Console.
2. Run the following command from your browser address line:
   http://<IP_address>/install
   (Where IP_address is the IP address of the Appliance)
   The browser displays the CounterACT software installation window.
3. Follow the on-screen instructions.

Logging In

After completing the installation, you can log in to the CounterACT Console from the shortcut location you created during the installation.

1. Select the CounterACT icon from the shortcut that you created. The CounterACT Login dialog box opens.
2. In the **IP/Name** field, type the IP address or host name of a CounterACT device.

3. Choose a login method from the **Login Method** drop-down list. Refer to the *CounterACT Console User Manual* for more information about login methods.

4. In the **User Name** field, type your user name.

5. In the **Password** field, type your password.

6. Select **Login** to open the Console.

The system comes with the predefined *admin* user. The user password and CounterACT address are set during CounterACT installation. You can change the password using a command line utility or via the Console. Refer to the *CounterACT Console User Manual* for more information about this utility.

### Installing the Cumulative Update Pack

The Cumulative Update Pack provides a simplified and automated process for updating a CounterACT environment with the latest versions of the CounterACT service pack and plugins bundled with CounterACT, along with additional core plugins. You are prompted to install the pack during the initial launch of the CounterACT Console, before the Initial Setup Wizard is run. It is recommended, but not mandatory, to install this pack.

- **If you did not use the latest Console Setup file, available on the CounterACT Support Page, to install the Console, you might not be prompted to install the pack.**

After pack installation, the various installed components will appear in the **Options > Plugins** pane in the Console. The pack itself is dissolvable, and will not appear in this pane.

This pack contains the latest versions of the CounterACT service pack and plugins bundled with CounterACT. Some dependencies may exist between the service pack and various plugin versions. This pack automatically accounts for and resolves any such dependencies.

Refer to the *Cumulative Update Pack Configuration Guide* available on the *Product Downloads page* of the Customer Support portal for more information and a list of service pack and plugin versions included in the pack.
To install the pack:

1. When you log in to the Console for the first time, the Cumulative Update dialog box opens.

2. Select one of the following and then select OK:
   a. Download and install from Forescout web site.
      The pack will take up to several minutes to download. After the pack has finished downloading, the installation process will begin.
   b. Install from file.
      Use this option if you do not have Internet access from this desktop. Download the pack (via USB device, for example) and install it from a local file.

If you choose to download and install the pack from the CounterACT Support Page, the following download screen opens, indicating the amount of time until the download is complete.

- If you are installing from a local file, the wizard begins immediately with the installation process described in the next step.
3. After the download is complete, the installation automatically begins.

The dialog box shows a list of the plugins as they are being installed.

The installation process may take up to about 30 minutes to complete. When the post-installation process begins, the amount of time that has elapsed appears on the bottom of the dialog box.

After the installation is complete, the CounterACT service starts and the Console is updated. This may take a few minutes.

4. Select **Launch Console** to open the CounterACT Login dialog box.
Running the Initial Setup Wizard on the Console

After login, the Initial Setup Wizard opens. The Wizard guides you through essential configuration steps to ensure that CounterACT is up and running quickly and efficiently.

License installation can be performed from the Wizard when working with virtual systems. See [CounterACT Virtual Device Deployment in VMware](#).
Uninstalling Previous Versions

To uninstall a previous Console version:

1. Use the Windows Uninstall tool to perform the uninstall procedure.

2. Alternatively, select the **Uninstall CounterACT Console** icon from the Forescout program group on the Start menu.
Chapter 7: CounterACT Virtual Systems

- About CounterACT Virtual Systems
- What to Do
- Virtual System Requirements
- Virtual Environment Setup - Define Real NICs
- VMware Virtual Systems
- Hyper-V Virtual Systems
- CounterACT Virtual Device Configuration
- Duplicating Virtual Devices
- Moving Virtual Devices
About CounterACT Virtual Systems

CounterACT virtual devices can be installed and managed in virtual data centers and IT environments, and provide capabilities identical to Appliance and Enterprise Manager software installed on dedicated machines. Using CounterACT virtual devices lets you:

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

The license feature has been customized to meet the needs of users working in virtual environments. Specifically, these changes ensure that virtual users are working with authorized, protected licenses. See Install a Virtual License for details.

Beyond changes to handling licenses, all other CounterACT features and tools available when working with CounterACT hardware are available in the virtual version. Refer to the CounterACT Console User Manual or the Console Online Help for details.

Hybrid Deployments

Hybrid deployments are also supported. This means that a physical Enterprise Manager can manage both physical and virtual Appliances, and a virtual Enterprise Manager can manage both physical and virtual Appliances.

Note that an Internet connection is required for virtual systems, but is not required for physical systems.

What to Do

Perform the following in order to work with virtual devices:

1. Verify that you have met requirements. See Virtual System Requirements.
2. Set up the virtual environment to work with CounterACT. See Virtual Environment Setup - Define Real NICs.
3. Deploy the CounterACT virtual devices. See VMware Virtual Systems or Hyper-V Virtual Systems.
4. Configure the CounterACT virtual devices and set up the Console. See CounterACT Virtual Device Configuration.

You should have a solid understanding of virtual networking concepts and functionality when working with CounterACT virtual devices.
Virtual System Requirements

This section describes:

- Hardware Minimum Requirements
- Network Connection Requirements for CounterACT Virtual Devices

Additional requirements described for physical deployments also apply. See System Requirements.

Hardware Minimum Requirements

- The recommended maximum disk latency is 5ms.
- The recommended minimum disk bandwidth is 200MB/s for read and 50MB/s for write.
- No CPU overcommitment on virtual hosts which might lead to performance or CPU ready issues.
- The CPUs and memory must be dedicated/reserved to the CounterACT Virtual Appliance or the CounterACT Virtual Enterprise Manager.

CounterACT Virtual Appliance

<table>
<thead>
<tr>
<th>Model</th>
<th>Devices</th>
<th>CPUs</th>
<th>GHz/CPU</th>
<th>RAM</th>
<th>Disk</th>
</tr>
</thead>
<tbody>
<tr>
<td>VCT-R</td>
<td>100</td>
<td>2</td>
<td>1.5</td>
<td>4GB</td>
<td>80GB</td>
</tr>
<tr>
<td>VCT-100</td>
<td>500</td>
<td>4</td>
<td>2.0</td>
<td>4GB</td>
<td>80GB</td>
</tr>
<tr>
<td>VCT-1000</td>
<td>1000</td>
<td>4</td>
<td>2.0</td>
<td>8GB</td>
<td>80GB</td>
</tr>
<tr>
<td>VCT-2000</td>
<td>2500</td>
<td>6</td>
<td>2.0</td>
<td>8GB</td>
<td>80GB</td>
</tr>
<tr>
<td>VCT-4000</td>
<td>4000</td>
<td>8</td>
<td>2.0</td>
<td>10GB</td>
<td>80GB</td>
</tr>
<tr>
<td>VCT-10000</td>
<td>10000</td>
<td>8</td>
<td>2.0</td>
<td>16GB</td>
<td>80GB</td>
</tr>
</tbody>
</table>

- Devices include user endpoints (such as laptops, tablets and smartphones), network infrastructure devices (such as switches, routers and access points), non-user devices (such as printers, IP phones, security equipment, medical devices and manufacturing equipment) and virtual machines.

- If you are using VMware virtual machines and would like to use more than eight CPUs, the VCT-10000 Appliance must be deployed on vSphere 5.x and above with an Enterprise license or above.

CounterACT Virtual Enterprise Manager

<table>
<thead>
<tr>
<th>Model</th>
<th>Appliances</th>
<th>CPUs</th>
<th>GHz/CPU</th>
<th>RAM</th>
<th>Disk</th>
</tr>
</thead>
<tbody>
<tr>
<td>VCEM-05</td>
<td>5</td>
<td>4</td>
<td>2.0</td>
<td>8GB</td>
<td>80GB</td>
</tr>
<tr>
<td>VCEM-10</td>
<td>10</td>
<td>4</td>
<td>2.0</td>
<td>8GB</td>
<td>80GB</td>
</tr>
<tr>
<td>VCEM-25</td>
<td>25</td>
<td>6</td>
<td>2.0</td>
<td>8GB</td>
<td>80GB</td>
</tr>
<tr>
<td>VCEM-50</td>
<td>50</td>
<td>6</td>
<td>2.0</td>
<td>8GB</td>
<td>80GB</td>
</tr>
</tbody>
</table>
### Network Connection Requirements for CounterACT Virtual Devices

At least one CounterACT virtual device must have an Internet connection. This connection is used to authenticate the CounterACT licenses against the Forescout License server. Authentication is performed daily.

The CounterACT device connected to the Internet sends license authorization requests to the Forescout License server (https://license.Forescout.com) via port 443 (HTTPS, TLS-based). Verify that this port is open.

Licenses that cannot be authenticated for one month are revoked. In case of a problem, you will receive a daily warning email indicating that there is a communication error with the server.

### Virtual Environment Setup - Define Real NICs

Verify that the virtual server on which the virtual Appliance is installed is configured with three interface connections to the network switch. (Only two interface connections are required for Layer 3 deployment). Only a virtual Enterprise Manager requires the management interface connection.

#### 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 with access to all network endpoints.

#### Monitor Interface

This interface allows the Appliance to monitor and track network traffic. Traffic is mirrored to a port on the switch and monitored by the Appliance. Depending upon the number of VLANs being mirrored, the traffic may or may not be 802.1Q VLAN tagged. If more than one VLAN is mirrored, the traffic must be 802.1Q VLAN tagged, provided the IP layer is not used.

#### Response Interface

The Appliance responds to traffic using this interface. Response traffic is used to protect against malicious activity and to perform policy actions. These actions may include, for example, redirecting web browsers or performing session blocking. The related switch port configuration depends upon the traffic being monitored. The response interface is not required when the IP layer is used.

Refer to [Appliance Interface Connections](#) for more information about these interfaces.

<table>
<thead>
<tr>
<th>Model</th>
<th>Appliances</th>
<th>CPUs</th>
<th>GHz/CPU</th>
<th>RAM</th>
<th>Disk</th>
</tr>
</thead>
<tbody>
<tr>
<td>VCEM-100</td>
<td>100</td>
<td>8</td>
<td>2.0</td>
<td>10GB</td>
<td>80GB</td>
</tr>
<tr>
<td>VCEM-150</td>
<td>150</td>
<td>8</td>
<td>2.0</td>
<td>16GB</td>
<td>80GB</td>
</tr>
<tr>
<td>VCEM-200</td>
<td>200</td>
<td>8</td>
<td>2.0</td>
<td>16GB</td>
<td>80GB</td>
</tr>
</tbody>
</table>
VMware Virtual Systems
This section describes how to work with VMware virtual systems.

- VMware Requirements and Support
- Create and Configure Virtual Switches
- CounterACT Virtual Device Deployment in VMware
- Post-Deployment Verification and VMware Configuration

VMware Requirements and Support
This section describes requirements and supported VMware versions.

Supported VMware Versions
The CounterACT virtual system is supported when running on the following VMware versions:

- VMware ESXi v6.0
- VMware ESXi v5.5
- VMware ESXi v5.1
- VMware ESX and ESXi v4.1 updates 1 through 3
- VMware ESX and ESXi v4.0 updates 1 through 4
- VMware ESX and ESXi v3.5 update 5

The guest OS is defined as Other Linux-2.6 32bit kernel.

VMware Tools Support
The VMware Tools Plugin automates installation of the VMware Tools utility package on CounterACT devices. This package provides various enhancements to guest virtual machines. You can access the plugin from the CounterACT Console.

To access the plugin:
1. Log in to the Console and select the Options icon from the Console toolbar.
2. Select the Plugins folder, and then select Install.
3. Navigate to the location where you saved the plugin installation file and install the plugin.
4. The plugin updates VMware drivers. Reboot to complete driver update. No configuration is required. The plugin runs automatically after installation.

vMotion Support
CounterACT virtual devices partially support VMware High Availability and load balancing. Failover due to failure of the physical server and migration due to load balancing is supported; automatic detection of a failure of the virtual Appliance operating system is not supported. For failover and virtual Appliance migration to work properly, all VM hosts participating in failover or load balancing must have visibility to the mirrored traffic and should be configured accordingly.
Create and Configure Virtual Switches

After you have verified that the VMware server on which the CounterACT virtual device is installed is configured with the required number of interface connections to the network switch, as described in the preceding section, you can create and configure virtual switches.

There are other ways to deploy a CounterACT virtual device: this document describes one alternative. (For example, you do not need a virtual switch for each port as vSwitches are generally trunk ports. The management interface and the response interface could be on one virtual switch with two logical interfaces configured on the vSwitch.)

Creating Virtual Switches

Select a host on which to install the virtual Appliance, and create virtual switches (vSwitches) for the management, monitor and response NICs on the host.

To create a virtual switch:

1. Log in to your VMware vSphere Console.
2. Select Home>Inventory>Hosts and Clusters.
3. Select the host (physical device) on which to install the CounterACT virtual device.
4. Select the Configuration tab.
5. In the Hardware pane, select Networking.

6. To create a virtual switch, select the Add Networking link. The Connection Type page of the Add Network Wizard opens.
7. Select Virtual Machine and then select Next. The Network Access page of the Add Network Wizard opens.
8. Select **Create a virtual switch**, select the available **vmnic** interface and then select **Next**.

The Connection Settings page of the Add Network Wizard opens.

9. Type a suitable name in the **Network Label** field and then select **Next**.

   - For a vSwitch handling mirrored / SPAN traffic (that is, the monitor interface), it is suggested to use **SPAN Port**. Leave the **VLAN ID** field empty as you want to SPAN all traffic and not VLAN tag any of it.

The Summary page of the Add Network Wizard opens.

10. Select **Finish**.

The vSwitch is created.

The wizard closes and returns to the Configuration tab of the Inventory window. The new switch is added in the window.

### Configuring Virtual Switches

After creating virtual switches for the monitor, management and response interfaces, you must configure them:
To configure a virtual switch:

1. Select the **Properties** link for the virtual switch.

![Switch Properties – Ports Tab](image)

2. In the Ports tab, select the appropriate Port Group and then select **Edit**. The General tab of the `<Network_Label>` Port Properties dialog box opens.

3. Define the **VLAN ID**, if necessary.
   - For the monitor and response interfaces, define the **VLAN ID** as **All**.

4. Select the Security tab and configure policy exceptions.

![Port Properties – Security Tab](image)

   - For the monitor and response interfaces, select and **Accept** all three options (**Promiscuous Mode**, **MAC Address Changes** and **Forged Transmits**).
   - For the monitor interface for mirrored / SPAN traffic, select and **Accept** the **Promiscuous Mode** option.
5. Select **OK** to return to the vSwitch Properties dialog box.
6. Select **Close**.

**CounterACT Virtual Device Deployment in VMware**

To work with your CounterACT virtual system, you must extract the image files from the CounterACT virtual system package that you received. You can use the image to deploy several devices and then apply a unique license to each device. See [Install a Virtual License](#) for details.

**Extract Deployment Files from the CounterACT Virtual System Package**

Your CounterACT virtual system package is a zip file that contains all the files required to deploy a CounterACT virtual devices. The file includes:

- An OVF template
- A file containing the virtual machine

You should extract the contents of the zip file and note the location of the extracted content.

* Due to the size of the OVF file, it is recommended to use a download manager.

**Deploy CounterACT Virtual Devices**

Perform the following once for each CounterACT virtual device that you plan to deploy.

**To deploy a CounterACT virtual device:**

1. Access the vSphere Console.
2. Select **File>Deploy from file (OVF template).**

   The Deploy OVF Template wizard opens at the Source page.

![Deploy OVF Template Wizard – Source Page](image)
3. Select the location where you extracted the contents of the CounterACT virtual system package and then select **Next**. The OVF Template Details page opens.

![Deploy OVF Template Wizard – OVF Template Details Page](image1)

4. Select **Next**. The Name and Location page opens.

![Deploy OVF Template Wizard – Name and Location Page](image2)
5. Specify a name and then select **Next**. The Datastore page opens.

![Deploy OVF Template Wizard – Datastore Page](image1)

6. Define the location where you want to store the virtual machine file (you need at least 80 GB free space) and then select **Next**. The Network Mapping page opens.

![Deploy OVF Template Wizard – Network Mapping Page](image2)
7. Map the physical and virtual interfaces and then select **Next**. The Ready to Complete page opens.

![Deploy OVF Template Wizard – Ready to Complete Page](image)

8. Select **Finish** to deploy the CounterACT virtual device.

**Post-Deployment Verification and VMware Configuration**

You should verify virtual host properties after deployment.

1. In the VMware vSphere Console, select the CounterACT virtual machine.

![Machine Selection](image)
2. Select **Edit virtual machine settings**. The **Virtual Machine Properties** dialog box opens.

![Virtual Machine Properties Dialog Box](image)

3. For each interface verify that:
   - The **Adapter Type** is defined as **E1000**.
   - The **Network label** is configured with the correct virtual switch.

The following table shows the mapping between the interfaces.

<table>
<thead>
<tr>
<th>VM Interface</th>
<th>CounterACT Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Adapter 1</td>
<td>eth0 (Management)</td>
</tr>
<tr>
<td>Network Adapter 2</td>
<td>eth1 (Monitor)</td>
</tr>
<tr>
<td>Network Adapter 3</td>
<td>eth2 (Response)</td>
</tr>
</tbody>
</table>

You may delete Network Adapter 3 if you are configuring your CounterACT in a Layer 3 configuration.

After verifying that each interface is configured correctly, you can configure the CounterACT virtual devices.

### Hyper-V Virtual Systems

This section describes how to work with Hyper-V virtual systems.

- [Hyper-V Requirements and Support](#)
- [Deploy CounterACT Virtual Devices in Hyper-V](#)
- [Configuring Hyper-V to Work with CounterACT Devices](#)
- [Automating CounterACT Deployment in Hyper-V Environments](#)
Hyper-V Requirements and Support
The CounterACT virtual system is supported when running on Microsoft Hyper-V.

Supported Hyper-V Versions
The CounterACT virtual system is supported when running on the following Hyper-V versions:

- Hyper-V Server 2012
- Hyper-V Server 2012 R2

There is no support for Hyper-V Generation 2 virtual machines.

Hyper-V Requirements

- CounterACT 7.0.0 ISO Update 2.2.0 or above.
  It is recommended not to mount the CounterACT ISO over an out-of-band management tool such as Integrated Lights-Out (iLO).
- Install Windows Server with the Hyper-V role.
- Run Windows Update after the Hyper-V role is created.
- If you are using Hyper-V Server 2012, install the following Microsoft hotfix ("Packet sniffing tool does not sniff all network traffic through port mirroring on a virtual machine that is hosted by a Windows Server 2012 Hyper-V server"):
  http://support.microsoft.com/kb/2885541
- Configure the outgoing interface as IP Layer in CounterACT.

  This option cannot respond to ARP requests, which limits the ability of the Appliance to detect scans inside the broadcast domain of the monitored subnet.

  See the section about working with channel assignments in the CounterACT Console User Manual.

- If the switch’s monitor ports monitor more than one VLAN, define the monitor ports as trunk ports and verify that all VLANs are allowed to send and receive traffic. To monitor untagged traffic, you must define the VLAN range starting from VLAN ID ‘0’.
- Verify that NIC drivers are updated with the latest version.

Deploy CounterACT Virtual Devices in Hyper-V
Perform the following for each CounterACT virtual device that you plan to deploy.

- Configuring Virtual Switches
- Create a Hyper-V Virtual Machine
- Modify Virtual Processor Settings
- Configuring Network Adapters
Configuring Virtual Switches
Create and configure two virtual switches, parallel to the Management and Monitor interfaces.

To create virtual switches:
1. Select **Virtual Switch Manager** from the Hyper-V Manager Actions pane.

2. Select **New virtual network switch** and select the type of virtual switch you want to create (External, Internal or Private).
3. Select **Create Virtual Switch**.

4. Name the switch and configure any relevant settings in the Virtual Switch Manager window.

   ![Virtual Switch Manager](image)

   **Virtual Switch Manager – Switch Configuration**

5. Select the virtual switch from the list of Virtual Switches in the Virtual Switch Manager.
6. Select **Extensions** and then select **Microsoft NDIS Capture**.

7. Select **OK**.

**Create a Hyper-V Virtual Machine**

New virtual machines are created with only one interface (Management). Additional interfaces are added later.

**To create a Hyper-V Virtual Machine:**

1. Select **New > Virtual Machine** from the Hyper-V Manager Actions pane, and then select **Next**.
2. Choose a name and location for the virtual machine and select **Next**.

3. Select **Generation 1** and select **Next**.  
   *This step is only relevant for Hyper-V Server 2012 R2.*

4. Specify the amount of memory to allocate to the virtual machine and select **Next**. See [Hardware Minimum Requirements](#) for more information.
5. Select the Management network adaptor configured in Configuring Virtual Switches and select Next. You can also configure this at a later time. Legacy Network Adapters should not be used.

New Virtual Machine – Configure Networking

6. Create a virtual hard disk, specifying the name, location and size and select Next. See Hardware Minimum Requirements for more information.

Connect Virtual Hard Disk
7. Install an operating system if you have access to the setup media or install it later, and select **Next**.

![New Virtual Machine – Installation Options](image)

**New Virtual Machine – Installation Options**

8. Review the virtual machine settings and select **Finish**.

![New Virtual Machine – Summary](image)

**New Virtual Machine – Summary**

**Modify Virtual Processor Settings**

After successfully adding a new virtual machine, you can adjust the number of virtual processors.

**To modify the number of virtual processors (CPU):**

1. Right-click the virtual machine and select **Settings**.

2. Select **Hardware > Processor** and adjust the number of virtual processors. See **Hardware Minimum Requirements** for more information.
**Configuring Network Adapters**

New virtual machines are created with one only interface (Management). Add a second network adapter for the Monitor interface.

The following table shows the mapping between the interfaces.

<table>
<thead>
<tr>
<th>VM Interface</th>
<th>CounterACT Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Adapter 1</td>
<td>eth0 (Management)</td>
</tr>
<tr>
<td>Network Adapter 2</td>
<td>eth1 (Monitor)</td>
</tr>
</tbody>
</table>

If you are using more than one VLAN, configure the port mirroring settings of the Management and Monitor interfaces. Legacy Network Adapters should not be used.

**To configure Network Adapters:**

1. Select **Add Hardware** from the Virtual Machine Settings window.
2. Select **Network Adapter** and then select **Add**.

![Virtual Machine Settings – Add Hardware](image)
3. Select the newly created Network Adapter from the Virtual Machine Settings designated as the Monitor Interface.

- If you are using a single VLAN, you can select *Enable virtual LAN identification.*
4. Select Advanced Features, and set the Mirroring mode to Destination.

To monitor internal traffic between guest virtual machines, set the Mirroring mode on each guest virtual machine to Source.

Configuring Hyper-V to Work with CounterACT Devices

By default, Hyper-V 2012 and 2012 R2 virtual ports do not operate in Promiscuous mode. This prevents port mirroring from external switch ports to the virtual NIC, which limits the ability of CounterACT to respond to network traffic. Manually configure Hyper-V to operate in Promiscuous mode for CounterACT to fully monitor and respond to this traffic.

Configuring vSwitch to Operate in Promiscuous Mode

The Get-VMSystemSwitchExtensionPortFeature cmdlet is used to get port-level features supported by virtual switch extensions on one or more Hyper-V guest virtual machines. Run this cmdlet to monitor traffic on switches. The returned feature object contains default values for the feature. The object can then be used to apply the configuration on specific ports using the Add-VmSwitchExtensionPortFeature command.
To enable vSwitch to operate in Promiscuous mode:

1. If this is your first time configuring promiscuous mode on this switch, perform the following:
   a. Run the following PowerShell cmdlet:
      ```powershell
      $a = Get-VMSwitchExtensionPortFeature -FeatureId 776e0ba7-94a1-41c8-8f28-951f524251b5
      ```
   b. After you receive a response, run the following PowerShell cmdlet to allow monitoring traffic:
      ```powershell
      $a.SettingData.MonitorMode = 2
      ```
   c. Run the following PowerShell cmdlet:
      ```powershell
      Add-VMSwitchExtensionPortFeature -ExternalPort –SwitchName <virtual_switch_name> -VMSwitchExtensionFeature $a
      ```
      If you receive an error after running this cmdlet, proceed with the next step.

2. If this is not your first time configuring promiscuous mode on this switch, perform the following:
   a. Run the following PowerShell cmdlet:
      ```powershell
      $a = Get-VMSwitchExtensionPortFeature -ExternalPort –SwitchName <virtual_switch_name> -FeatureId 776e0ba7-94a1-41c8-8f28-951f524251b5
      ```
   b. After you receive a response, run the following PowerShell cmdlet to allow monitoring traffic:
      ```powershell
      $a.SettingData.MonitorMode = 2
      ```
   c. Run the following PowerShell cmdlet:
      ```powershell
      Set-VMSwitchExtensionPortFeature -ExternalPort –SwitchName <virtual_switch_name> -VMSwitchExtensionFeature $a
      ```

To disable vSwitch from operating in Promiscuous mode:

1. Run the following PowerShell cmdlet:
   ```powershell
   $a = Get-VMSwitchExtensionPortFeature -ExternalPort –SwitchName <virtual_switch_name> -FeatureId 776e0ba7-94a1-41c8-8f28-951f524251b5
   ```

2. After you receive a response, run the following PowerShell cmdlets to disable monitoring traffic:
   ```powershell
   $a.SettingData.MonitorMode = 0
   ```

Configuring VLAN Filter Settings

The set-VMNetworkAdapterVlan cmdlet is used to configure VLAN filter settings for traffic through a virtual network adapter. You can use the cmdlet to receive 802.1q encapsulated traffic on either a single interface or multiple interfaces. If you are using both a monitor and a response interface, this cmdlet needs to be applied on both interfaces.
The channels defined in the CounterACT Console for the Monitor interface must be set to monitor *All Traffic* or *All Tagged Traffic*. Refer to the section about working with Appliance channel assignments in the *CounterACT Console User Manual* for more information.

**To configure VLAN filter settings:**

1. Run the following PowerShell cmdlet:

   ```powershell
   set-VMNetworkAdapterVlan -VMName <virtual_machine_name> [-VMNetworkAdapterName <adapter_name>] -Trunk -AllowedVlanIdList <802.1q_encapsulation_vlans> -NativeVlanId <802.1q_encapsulation_vlan_for_untagged_traffic> [-Confirm]
   ```

   Where `802.1q_encapsulation_vlans` is a range of VLANs allowed on the network adapter. Although the allowable range is 0-4094, using the maximum value as the upper limit may not work. If you want to use an open-ended range, use, for example, 0-4000.

   Where, `802.1q_encapsulation_vlan_for_untagged_traffic` is the untagged VLAN on an 802.1q trunked switch port, within the range of the `AllowedVlanIdList` parameter.

   If, after running the PowerShell cmdlet, you receive an error that the operation failed and is not supported, temporarily disassociate the virtual switch from the virtual machine by selecting *Not connected* in the virtual switch interface settings.

   Run the PowerShell cmdlet again and then reconfigure the virtual switch.

2. Run the following PowerShell cmdlet to view the configured settings:

   ```powershell
   Get-VMNetworkAdapterVlan -VMName <virtual_machine_name> [-VMNetworkAdapterName <adapter_name>]
   ```

**Automating CounterACT Deployment in Hyper-V Environments**

This section provides information regarding how to automate CounterACT deployment in Hyper-V environments. The automation process involves preparing a newly installed version of CounterACT for template creation, creating a template using the Hyper-V Manager and then deploying the template using Hyper-V and an fstool command line.
CounterACT Console settings that are stored on the Enterprise Manager, such as Switch assignment details, will be lost during the template creation process and will not be exported to the deployed machine. Therefore, avoid configuring CounterACT Console settings before running the template. Some configurations, such as Channel settings, are stored on the Appliance, and will remain after the template creation process.

This feature was released with Hotfix 1.6.3.

**Create a CounterACT Single/High Availability Template**

**To create a template:**

1. Perform standard installation of the High Availability or Single Appliance on Hyper-V, including running the Initial Setup Wizard. The parameters that are set during this phase will serve as placeholders for the real ones.

2. Install Hotfix version 1.6.3 or above for the Appliance from the CounterACT Console.

3. Run the following command:
   
   ```bash
   fstool conf --template
   ```
   
   This command prepares CounterACT and its virtual hard disk for template creation.

   In a High Availability environment, run this command:
   
   ```bash
   from fsroot.
   ```
   
   − for the Active node only. It is recommended that the Active node be the Primary node.

   If a Standby node existed in the original High Availability pair, you should power it off before powering off the Active node. Otherwise, the Standby node will failover and become the active node at the end of the template creation process. Refer to the section on Failover in the Resiliency Solutions How-to Guide for more information.

   **After successfully running the fstool command, it is recommended to delete the Standby node by removing the virtual hard disk or the entire virtual machine in order to prevent security vulnerabilities.**

4. Create a Hyper-V template from a virtual hard disk using Hyper-V Manager.

   The template should use the following elements:
   
   − The HDD that was built in the previous step.
   
   − The memory and network adaptors of the original machine.
   
   − The Operating System should be Linux, CentOS 6, 32 bit.

   Note that you may need to repeat the steps above, creating up to 3 sets of templates:
   
   - Non-High Availability Appliance
   
   - High Availability Primary Appliance
   
   - High Availability Secondary Appliance
Optionally you can create Enterprise Manager templates.

When a deployed High Availability Standby node machine is created, the Active node should be running to allow the Standby node to synchronize with it.

If you build a High Availability pair for template purposes only, you only need to build the Primary node, since both the Active node and the Standby node templates are taken from the Primary node.

**Deploy an Appliance from a Template**

**To deploy an Appliance from a template:**

1. Create a new host from template using Hyper-V Manager according to its workflow.
2. The tool has an option to run scripts on the guest OS. This is where the new fs_tool conf command line would be called with a set of parameters that will be provided, according to the deployment environment. Following boot, the Appliance will run the script, re-generate an identity and will apply the various parameters that would be provided. The `fs_tool conf --wait` command should be run at least 14 times to guarantee that the first command has enough time to be properly completed. See [FS_tool Samples for Automated Deployments](#) for details.

**Configure Operating System – fs_tool conf command**

**General Deployment Notes**

- Deployment may take up to 60 minutes (depending on the network).
- Each Appliance will reboot several times during deployment.
- Deployed Appliances are stopped at the end of the process by default. See 'Start the virtual machine after deploying it' checkbox.
Chapter 7: CounterACT Virtual Systems

- After deploying the template, connect the Appliance to the Enterprise Manager, verify/set Appliance configuration and install licenses on Appliances. The licensing installation workflow is identical to the standard procedure for virtual Appliances. See Install a Virtual License for details.

Setup Notes

When creating/deploying the template:

- Deploy using Static IP.
- Add all interfaces.
- Associate with appropriate switches.
- Set monitoring as the target.
- For High Availability systems use the following interfaces: Management, Monitoring and two inter-cluster/pair Sync interfaces.

Configuration Recommendations

When configuring network adaptors in the Virtual Machine Wizard:

- Connect the interface to a network. Select the Connectivity Connected to a VM network option and select a network name. Select separate network names for each interface.
- Use Static IP Connectivity. Select the Connectivity Static IP (from a Static IP Pool) option. Deployment may fail if you select Dynamic IP.
Save and Reuse the Original Script

Add a Virtual Hard Disk to the Library

- Select **Library>Add Physical Resource**.
- Use VM settings to verify that you selected the correct VHD.
Hostname Limitations
The specified computer name cannot be larger than 15 bytes.

Troubleshooting Logs
If the deployment fails you can review SCVMM Linux agent deployment logs at the following locations:

- /var/log/scvmm.log
- /var/log/fsconf.log

FStool Samples for Automated Deployments
This section displays samples of the fstool conf command for standalone and High Availability setups.

The `fstool conf --wait` command listed in the examples below should be run at least 14 times to guarantee that the first command has enough time to terminate properly.

Single Setup

```
--management-eth management_interface
--management-addr management_address
--management-gw default_gateway_address
--hostname hostname
--management-netmask management_netmask (optional)
--domain domain (optional)
--dns dns_server_address (optional)
```

Single Sample

```
fstool conf --management-eth eth0
--management-addr 10.0.0.100
--management-gw 10.0.0.1
--hostname ct-appl
--management-netmask 24
--domain mydomain.com
--dns 10.0.0.1
fstool conf --wait 250
(x14)
```

Primary High Availability Setup

```
--management-eth management_interface
--management-addr management_address
--management-gw default_gateway_address
--hostname hostname
--ha-primary-addr primary_private_address
--management-netmask management_netmask (optional)
```
--domain                domain                    (optional)
--dns                   dns_server_address        (optional)
--ha-secondary-addr     secondary_private_address (optional)
--ha-sync-subnet        sync_subnet               (optional)
--ha-sync-netmask       sync_netmask              (optional)
--ha-sync-eth-primary   sync_interface_primary    (optional)
--ha-sync-eth-secondary sync_interface_secondary (optional)
--ha-sync-subnet        sync_subnet               (optional)

Primary High Availability Sample
fstool conf --management-eth eth0
  --management-addr 10.0.0.100
  --management-gw 10.0.0.1
  --hostname ct-appl
  --management-netmask 24
  --domain mydomain.com
  --dns 10.0.0.1
  --ha-primary-addr 10.0.0.101
  --ha-secondary-addr 10.0.0.102
  --ha-sync-eth-primary eth3
  --ha-sync-eth-secondary eth2
  --ha-sync-subnet 172.17.2
fstool conf --wait 250
(x14)

Secondary High Availability Setup
    --ha-secondary
  --ha-sync-eth-primary sync_interface_primary
  --ha-sync-subnet sync_subnet

Secondary High Availability Sample
fstool conf --ha-secondary
  --ha-sync-eth-primary eth3
  --ha-sync-subnet 172.17.2
fstool conf --wait 250
(x14)
CounterACT Virtual Device Configuration

Configuration involves the following steps:

1. Configure the Virtual Enterprise Manager and Appliances
2. Verify Switch-Appliance Connectivity
3. Install the Console
4. Perform the Initial Console Setup
5. Install a Virtual License

Configure the Virtual Enterprise Manager and Appliances

The following information is required to configure the Enterprise Manager and the Appliances in your virtual environment.

- CounterACT device host name
- CounterACT admin password
- Management interface
- Appliance IP address
- Network mask
- Default gateway IP address
- DNS domain name
- DNS server addresses

To configure the CounterACT device:

1. Start the CounterACT virtual device.
2. Open SSH to the machine.

CounterACT <version>-<build> options:

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) :

Follow the on-screen instructions. Refer to Configuring an Appliance and Configuring the Enterprise Manager for details.
Cloned CounterACT Devices
If you cloned a CounterACT device (rather than deploying the OVF file on each virtual device), the network interfaces on the cloned device will be numbered unpredictably; if the original device has n interfaces numbered from 0 to n-1, the numbering of the interfaces on the cloned device will begin at n. CounterACT detects this during the configuration and offers to renumber the interfaces:

<table>
<thead>
<tr>
<th>A reboot is required to renumber network interfaces.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Renumber? (yes/no) :</td>
</tr>
</tbody>
</table>

Verify Switch-Appliance Connectivity
Verify that the virtual switch is properly connected to the Appliance.

To verify connectivity:
1. At the Appliance, run the following command for each interface detected:
   ```bash
   fstool ifcount eth0 eth1
   ```
   Verify that you see a large percentage (>90%) of mirrored traffic on the eth1 interface.

Install the Console
Use the installation software built into your CounterACT device to install the CounterACT Console.

- Acquire and save the demo license files on the machine that will run the Console.

To install the Console:
1. Open a browser window from the machine at which the Console will run.
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 an installed virtual Appliance)
   The browser displays the Console installation window.
3. Follow the on-screen instructions.
   For more information, refer to Chapter 6: Installing the CounterACT Console.
Chapter 7: CounterACT Virtual Systems

Perform the Initial Console Setup

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

![Initial Setup Wizard – Welcome Page](image)

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

**Before You Begin**

Before working with the Wizard:

- Prepare the location of the demo license files received from your CounterACT representative.
- Fill in the table that appears in Information Required for the Installation.
Installing a Demo License

In the License page, select a virtual demo license that you received from Forescout. See Install a Virtual License for details.

To install a demo license:

1. In the License page, select Choose file.

The Choose the license file dialog box opens.

2. When working with the initial demo license, you can select any license file for any device, provided that a specific license file is installed on one device only. (If you use the same license file for more than one device, the license may be revoked. Moreover, you will be unable to add an Appliance to the Enterprise Manager if an Appliance with the same license is already connected.) You can rename the file if required. Extended demo virtual licenses and permanent virtual licenses are tailored for specific devices.
Navigate to the license and select **OK**. The Install License from File dialog box opens.

**Install License from File Dialog Box**

4. Select the device and select **Install**. A dialog box opens with information about the installation start and end date, and other license details.

**License Details**

5. Select **OK** and complete the Wizard.

**Install a Virtual License**

The license feature is designed to meet the needs of users working in Virtual IT environments, including environments that require a proxy server. This feature ensures that virtual users are working with authorized, secure and protected licenses.

**Demo Virtual License**

After installing a virtual Appliance, you must install the demo license you received from your CounterACT representative by email. The license can be installed during the initial Console setup (see **Perform the Initial Console Setup**) and is valid for 30 days from the time it was generated by the CounterACT representative. When installing, you will be presented with the license's expiration date.
You must request and install a permanent license via the Console before this period expires. (Tools>Options>Appliances>License>Generate Request). You can also request an extension to the demo license from this location.

License Details

Permanent Virtual License

Before your demo license expires, you must install a permanent license. This license has an installation begin and end date. You must install the permanent license within these dates, which will be sent to you when the license is issued. For details about requesting a permanent license, refer to any of the following:

- CounterACT Console User Manual located on the CounterACT DVD in the /docs folder
- Console Online Help
- Forescout Documentation Portal (http://www.Forescout.com/kb)

*On physical systems, the permanent license has no installation begin and end date.*

Virtual License Authorization

The demo and permanent license are authorized daily by the Forescout License server.

Communication with Forescout's License server is performed by one CounterACT device, which must have access to the Internet. This is required so that one device can perform the authentication for all the devices. The first device that has connectivity is used for the communication. If there are no communication problems, the first device on the list will usually be used for performing the communication with Forescout License server for all devices in the network. You should expect daily traffic from that device equivalent to the number of VM devices installed. See Connecting to the Forescout License Server for details about connecting.

Licenses that cannot be authorized for a month will be revoked. When this happens, significant CounterACT functionality will stop. You will be contacted via e-mail regarding the expiration date and violations. In addition, license alerts, violations, status and troubleshooting information can be accessed from the Console, Details pane.
On physical systems this authorization process does not take place.

If policies are stopped as a result of an expired license or license violations, or the license is revoked, and an authorized license is subsequently installed, the policies are not automatically restarted. You must restart policies from the Console. For information about how to do this refer to the chapter about managing Appliances, Enterprise Managers and Consoles, in the CounterACT Console User Manual.

License Capacity per CounterACT Virtual System Image

You can install several licenses for each CounterACT virtual system image. For example, if you want to work with one Enterprise Manager and nine Appliances, you will receive an image file for the Enterprise Manager and one image file for the Appliances, but 10 separate licenses.

Connecting to the Forescout License Server

Connection to the Forescout License server is performed via a CounterACT device connected to the Internet. By default, CounterACT assumes that all devices are connected.

License authorization requests are sent to the Forescout License (at https://license.Forescout.com) server via port 443 (HTTP-Secure –TLS based).

At least one CounterACT device must have an Internet connection, but you may select more than one to ensure a continued connection. Several devices may be required, if, for example, one device is temporarily down, or if you are not sure which device has an Internet connection. You can define a proxy for these connections.

To specify a device to connect to the Forescout License server:

1. Select the Options icon from the Console toolbar and then select License Server.

   ![License Server Options](image)

2. Select Specific CounterACT Devices.
3. Select **Add**.

The Add a device dialog box opens.

4. Select a device from the **Available Devices** drop-down list.

5. Organizations working without an Internet connection can use a proxy to ensure communication with the Forescout License server. Select **Use Proxy** and define the proxy.

6. To test the connection to the selected CounterACT device, select **Test**.

7. Select **OK**.

8. Repeat steps 3 to 7 as required.

### Duplicating Virtual Devices

You can duplicate a virtual device that does not have a CounterACT virtual license installed. However, it is not advisable to duplicate a virtual device that has a virtual license installed. If you duplicate a virtual device, you must install a unique license on each of the devices, otherwise the Forescout License server may reject all licenses on the involved devices, including the original one. You will be notified when this happens via email and from the Console.

**To reset a rejected license on the original device:**

1. Notify Forescout license support so that they can reset the license status from the server. This device will retain the original license and continue using it.

**To remove a rejected license from a duplicated device:**

1. Log in to the device and run the following commands.
   - Stop the device: `fstool service stop`
   - Remove the existing license: `fstool clear_license`
   - Start the device: `fstool service start`

2. Install a new virtual license on the device.
Moving Virtual Devices

You can ‘move’ a CounterACT virtual device by using the CounterACT backup and restore features.

**To move a licensed CounterACT device:**

1. Back up the CounterACT virtual device:
   a. Select **Options > CounterACT Devices**.
   b. Select a device.
   c. Select **Backup**.

2. Copy the backup file to the new virtual server.

3. Deploy the original OVF file.

4. Restore from the backup file.
# Appendix A: Site Preparation Form

This appendix lists the CounterACT site parameter requirements. Verify that you have the information required and that your site is set up appropriately. Enter your information in the **Value** column.

<table>
<thead>
<tr>
<th>Subject</th>
<th>Item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Communication Information</strong></td>
<td>CounterACT IP address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subnet mask</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Default gateway</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mail-relay server address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS server host name and address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Email addresses used for sending alerts regarding worm attack attempts</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VLAN ID on which the Appliance, router and Console are located (only required if these components must be located on a VLAN and are connected to a tagged port)</td>
<td></td>
</tr>
<tr>
<td><strong>Internal Network</strong></td>
<td>Address ranges of protected network (It is recommended to use your enterprise’s entire internal IP address range)</td>
<td></td>
</tr>
<tr>
<td><strong>Management</strong></td>
<td>Operating system on PC running CounterACT Console or CounterACT Enterprise Manager</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Allowed addresses for CounterACT Console or CounterACT Enterprise Manager connectivity</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Addresses of hosts allowed to control CounterACT through SSH</td>
<td></td>
</tr>
</tbody>
</table>
### Subject: Communication Equipment

<table>
<thead>
<tr>
<th>Item</th>
<th>Possible Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communication equipment to which the CounterACT is connected</td>
<td>Switch with mirroring port – supports traffic response</td>
</tr>
<tr>
<td></td>
<td>Switch with mirroring port – does not support traffic</td>
</tr>
<tr>
<td></td>
<td>response</td>
</tr>
<tr>
<td></td>
<td>Vendor and model:</td>
</tr>
</tbody>
</table>

### Subject: Logistics

<table>
<thead>
<tr>
<th>Item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available space:</td>
<td>19” Rack</td>
</tr>
<tr>
<td>How near/far is rack/shelf space from a network connection and</td>
<td>Shelf space</td>
</tr>
<tr>
<td>power connection (specify cable requirements)</td>
<td>Available space</td>
</tr>
<tr>
<td></td>
<td>Socket and cable availability</td>
</tr>
<tr>
<td></td>
<td>Standard power socket + cable</td>
</tr>
<tr>
<td></td>
<td>Network socket + cable</td>
</tr>
</tbody>
</table>

### Subject: Managed Switch SNMP Information

<table>
<thead>
<tr>
<th>Item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch IP Address and Brand</td>
<td></td>
</tr>
<tr>
<td>Identify the IP address and brand of the switches to monitor.</td>
<td></td>
</tr>
<tr>
<td>SNMP Community String Version and Type</td>
<td></td>
</tr>
<tr>
<td>Discuss Read-only and Read/Write abilities.</td>
<td></td>
</tr>
<tr>
<td>Copper or Fiber Connectivity</td>
<td>(10/100/1000Base-T copper (RJ-45) or 1000/10000Base-SX fiber (LC) can be used)</td>
</tr>
</tbody>
</table>

### Subject: Contact Details

<table>
<thead>
<tr>
<th>Item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td></td>
</tr>
<tr>
<td>Phone number</td>
<td></td>
</tr>
<tr>
<td>Email address</td>
<td></td>
</tr>
</tbody>
</table>
Appendix B: Upgrading To CounterACT 7.0.0 on Hardware Revision 2x

This appendix describes how to install CounterACT version 7.0.0 software on CounterACT Hardware Revision 2x devices. These instructions apply to devices deployed as CounterACT Appliances and Enterprise Managers.

You can perform this installation from either a DVD, or a USB flash memory device. Detailed instructions are provided for DVD installation only.

If the Appliance is a CT10000, perform the Extra Step for CT10000 Appliances. Perform this step whether you install from DVD or USB.

To install from a DVD:

1. Download the latest CounterACT 7.0.0 ISO image from the Customer Support Portal, Product Downloads page. You will need your organization’s user name and password to access the portal.
2. Burn the image onto a DVD.
3. Remove the device and the power cord from the shipping container.
4. Connect the power cord to the power connector on the device rear panel. Connect the other end of the power cord to a grounded AC outlet.
5. Connect a keyboard, mouse and monitor to the device. (You can also set up the device for serial port connection: 19,200, 8, none, hardware. For detailed instructions, see Serial Port Setup.)
6. Insert the CounterACT installation DVD you just created into the DVD drive on the CounterACT device.
7. Power on and boot the device, and make sure it boots from the DVD media.
8. Follow the on-screen instructions to allow for a full installation of the new version. This process typically takes 15-20 minutes.

Extra Step for CT10000 Appliances

If the Appliance is a CT10000, perform the following after installing version 7.0.0 software.

- First install CounterACT 7.0.0, or operational problems will occur.

1. Restart the Appliance.
2. Press F2 to get into BIOS setup.
3. On the main BIOS Setup screen, press the right arrow key to select Advanced.
4. On the Advanced Setup screen, select Processor Configuration and press ENTER.
5. On the Processor Configuration screen, scroll down with the down arrow until you find the option **Core Multi-Processing**.

6. From its drop-down menu, select the option **ALL**.

   - Do not change any other settings.

7. Press **F10** to save settings and exit. Confirm (**YES**).
Appendix C: Updating Firmware on Hardware Revision 2x

Several known CVEs relate to potential vulnerabilities that may be flagged against the RMM3 component of hardware revisions 20, 21 and 22.

To resolve these potential vulnerabilities, you can update the firmware on your CounterACT Appliance to BMC Firmware revision 0.64.

**To update your firmware:**

1. Verify that the Appliance you are about to update has a hardware revision of 20, 21 or 22.
   
   To find out the revision number of the Appliance, look at the model name on the Forescout label. The number is in the form of `CTxxxx-rr`, where “rr” is the revision number, for example, `CT2000-21`. **Do not proceed if the revision number is not 20, 21 or 22.**

2. Unzip the contents of the update package and copy all files to the root directory of an empty, clean USB flash drive. The zip file can be downloaded from the following location:
   

3. Insert the USB flash drive into any available USB port on the Appliance that you are updating.

4. Power on the Appliance.

5. Boot the Appliance to the UEFI shell by pressing the <F6> key for the Boot Menu during POST.

6. The system will automatically load the UEFI shell and begin the update process. This will take a few minutes.

   **WARNING: Do not interrupt, reboot or remove power from your Appliance during the update process. Doing so may render your Appliance inoperable.**

7. Reboot the Appliance after the update process has completed successfully.

**Verifying Firmware Updates**

**To verify the updates:**

1. During POST, press the <F2> key when prompted to access the BIOS Setup Utility.

2. Move the cursor to the SERVER MANAGEMENT menu.

3. Move the cursor down to the SYSTEM INFORMATION option and select `Enter`.

4. Verify that the BMC Firmware revision is 0.64.

   The system software update is complete.
Disabling IPMI over LAN

To disable IPMI over LAN:

1. Connect to your RMM.
3. Uncheck "IPMI over LAN" and select Save.