



ForeScout CounterACT[®]

Installation Guide

Version 8.0

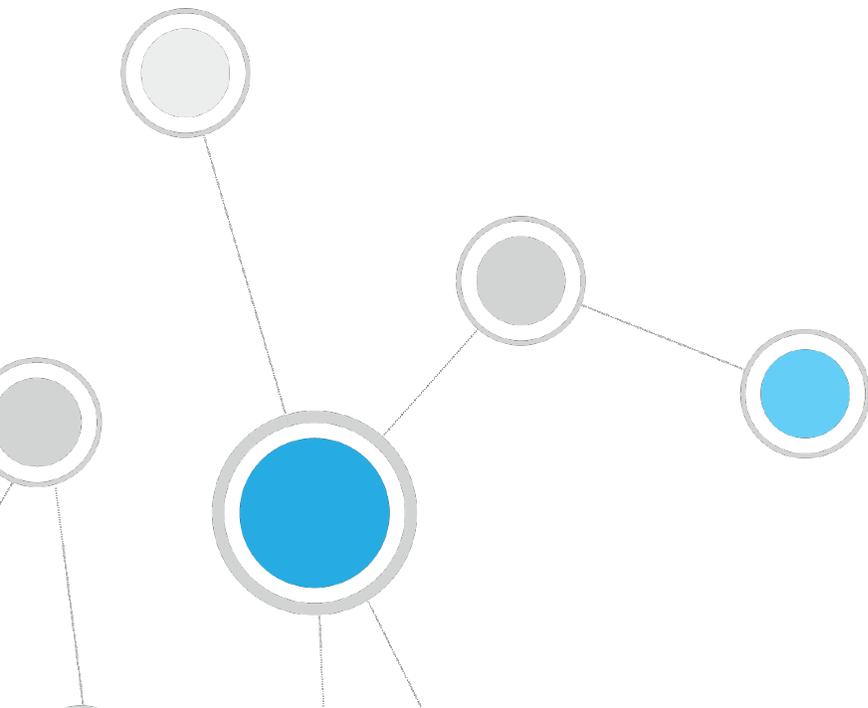


Table of Contents

Preface	5
About the CounterACT Solution	5
About This Guide	5
CounterACT Package Contents	6
Virtual Devices	6
Additional CounterACT Documentation	7
Documentation Downloads	7
Documentation Portal	8
CounterACT Help Tools.....	8
Chapter 1: System Components and Requirements	10
CounterACT Components.....	11
CounterACT Appliance.....	11
CounterACT Enterprise Manager	12
Recovery Enterprise Manager.....	12
CounterACT Console	12
Password Encryption Algorithm	13
Remote System Management Integration	13
High Availability Tools.....	13
Power Outage Handling.....	13
System Requirements.....	14
Supported Physical CounterACT Devices.....	14
CounterACT Console Hardware Requirements	15
Network Access Requirements	15
Network Deployment Requirements	18
Appliance Information Requirements.....	18
Enterprise Manager Information Requirements.....	19
Network Connection Requirements	19
Bandwidth Requirements.....	19
IPv6 Support	19
FIPS Compliance	19
Enabling FIPS Mode	19
Verifying FIPS Compliance.....	20
FIPS Compliance with SecureConnector.....	20
Licensing Mode	20
Chapter 2: Network Setup	22
About the CounterACT Installation.....	23
Related Documents	23
Appliance Interface Connections.....	24
Management Interface	24
Configure VLANs on the Management Interface.....	25
Monitor Interface.....	25
Response Interface.....	26

Setting up Switch Connections	26
Recommended Installation: Separate Management, Monitor and Response Ports	26
Combined Monitor and Response Port	27
Combined Management and Response Port (Single VLAN Only)	28
Combined Management, Response and Monitor Port (Single VLAN Only)	29
Switch Setting Guidelines	29
Creating an Out-of-Band IP Management Interface.....	30
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	44
Perform a Ping Test	45
Generate a Configuration Summary for an Appliance	45
Configure Password Protection for the Boot Loader	46
Configure ICMP Settings.....	46
Additional Installation Tools	46
Configuring the Interface Speed/Duplex	46
Restoring Appliance System Settings	47
Chapter 4: Enterprise Manager Setup and Configuration, and Post-Installation Procedures	50
About the Installation	51
Setting up the Enterprise Manager	51
Configuring the Enterprise Manager	51
Post-Installation Procedures	56
Connect the Enterprise Manager to the Network.....	56
Integrate the Enterprise Manager with Remote System Management	56
Restoring Enterprise Manager System Settings	57
Restoring as a High Availability Device.....	58
Chapter 5: Upgrading CounterACT Devices.....	60
Upgrading to a New Version	61
Upgrading High Availability Devices	62
Upgrading to a New Version and Migrating to Centralized Licensing Mode (v8.0)	62
Gradual Upgrade	63
Chapter 6: Reimaging CounterACT Devices	65
Reimaging CounterACT Devices.....	66
Prepare an Installation DVD.....	66
Prepare a Bootable USB Memory Device.....	66
Reimage the CounterACT Device	67

Chapter 7: Installing the CounterACT Console.....	68
About the CounterACT Console Installation.....	69
Information Required for the Installation.....	69
Install from ForeScout Portals.....	70
Install from a Browser on Your Appliance	72
Logging In.....	72
Running the Initial Setup Wizard on the Console	74
Uninstalling Previous Versions.....	74
Chapter 8: CounterACT Virtual Systems	75
About CounterACT Virtual Systems.....	76
Hybrid Deployments	76
What to Do.....	76
Virtual System Requirements.....	77
Hardware Minimum Requirements	77
Network Connection Requirements for CounterACT Virtual Devices	77
Virtual Environment Setup - Define Real NICs	77
VMware Virtual Systems.....	78
VMware Requirements and Support	78
Create and Configure Virtual Switches	79
CounterACT Virtual Device Deployment in VMware	82
Post-Deployment Verification and VMware Configuration	86
Hyper-V Virtual Systems	87
Hyper-V Requirements and Support.....	87
Deploy CounterACT Virtual Devices in Hyper-V.....	88
Configuring Hyper-V to Work with CounterACT Devices.....	96
Automating CounterACT Deployment in Hyper-V Environments.....	98
KVM Virtual Systems	105
KVM Requirements	105
Deploy CounterACT on a KVM virtual system	105
CounterACT Virtual Device Configuration.....	106
Configure the Virtual Enterprise Manager and Appliances	106
Verify Switch-Appliance Connectivity	107
Install the Console.....	107
Perform the Initial Console Setup	108
Install a Virtual License (Per-Appliance Licensing Mode Only).....	110
Duplicating Virtual Devices	113
Moving Virtual Devices.....	114
Appendix A: Site Preparation Form	115

Preface

This preface includes:

- [About the CounterACT Solution](#)
- [About This Guide](#)
- [CounterACT Package Contents](#)
- [Additional CounterACT Documentation](#)

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 Administration Guide* 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

Chapter 4: Enterprise Manager Setup and Configuration, and Post-Installation Procedures	How to install and upgrade the CounterACT Enterprise Manager
Chapter 5: Upgrading CounterACT Devices	How to upgrade the software on installed CounterACT devices
Chapter 6: Reimaging CounterACT Devices	How to reinstall CounterACT on a device using a prepared DVD or USB memory device.
Chapter 7: Installing the CounterACT Console	How to install the CounterACT Console
Chapter 8: CounterACT Virtual Systems	How to install and configure CounterACT virtual systems
Appendix A: Site Preparation Form	A CounterACT site preparation form with required site parameters

CounterACT Package Contents

Your CounterACT package includes the following components:

- The CounterACT Appliance/Enterprise Manager
- Front Bezel
- Rail Kits (Mounting brackets)
- Power cord(s)
- DB9 Console connecting cable (for serial connections only)
- Enterprise Products Safety, Environmental, and Regulatory Information
- Getting Started document (ForeScout 51xx Appliances only)

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 User Guide* for more information. See [Additional CounterACT Documentation](#) for information on how to access the guide.

Virtual Devices

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

- A link to a CounterACT virtual package image
- One of the following, depending on the [Licensing Mode](#) your deployment is using:
 - **Centralized Licensing Mode.** An email from ForeScout with purchase entitlement details, including your Deployment ID and links to the ForeScout Customer Portal containing software entitlements and downloads.

- **Per-Appliance Licensing Mode.** 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*.

See [Licensing Mode](#) for more information on licensing modes and to find out which mode you are using. Refer to the *CounterACT Administration Guide* for more information about licensing management and licensing modes. See [Additional CounterACT Documentation](#) for information on how to access the guide.

This system includes CounterACT virtual Appliances, the CounterACT virtual Enterprise Manager and the Console. These components function identically to physical components, with the exception of licenses, which function differently when operating in Per-Appliance Licensing Mode. Licensing functionality of physical and virtual systems is identical when operating in Centralized Licensing Mode.

See [Chapter 8: CounterACT Virtual Systems](#) for details about installing virtual systems and about virtual system licenses.

Additional CounterACT Documentation

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

- [Documentation Downloads](#)
- [Documentation Portal](#)
- [CounterACT Help Tools](#)

Documentation Downloads

Documentation downloads can be accessed from one of two ForeScout portals, depending on which licensing mode your deployment is using.

- **Per-Appliance Licensing Mode** - [Product Updates Portal](#)
- **Centralized Licensing Mode** - [Customer Portal](#)

 *Software downloads are also available from these portals.*

To learn which licensing mode your deployment is using, see [Identifying Your Licensing Mode in the Console](#).

Product Updates Portal

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

To access the Product Updates Portal:

1. Go to <https://updates.forescout.com/support/index.php?url=counteract>.
2. Select the CounterACT version you want to discover.

Customer Portal

The Downloads page on the ForeScout Customer Portal provides links to purchased CounterACT version releases, Base and Content Modules, and Extended Modules, as well as related documentation. Software and related documentation will only appear on the Downloads page if you have a license entitlement for the software. The Documentation page on the portal provides a variety of additional documentation.

To access documentation on the ForeScout Customer Portal:

1. Go to <https://forescout.force.com/support/>.
2. Select **Downloads** or **Documentation**.

Documentation Portal

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

 *If your deployment is using Centralized Licensing Mode, you may not have credentials to access this portal.*

To access the Documentation Portal:

1. Go to www.forescout.com/docportal.
2. Use your customer support credentials to log in.
3. Select the CounterACT version you want to discover.

CounterACT Help Tools

Access information directly from the CounterACT Console.

Console Help Buttons

Use context sensitive *Help* buttons to quickly access information about the tasks and topics you are working with.

CounterACT Administration Guide

Select **CounterACT Help** from the **Help** menu.

Plugin Help Files

1. After the plugin is installed, select **Options** from the **Tools** menu and then select **Modules**.
2. Select the plugin and then select **Help**.

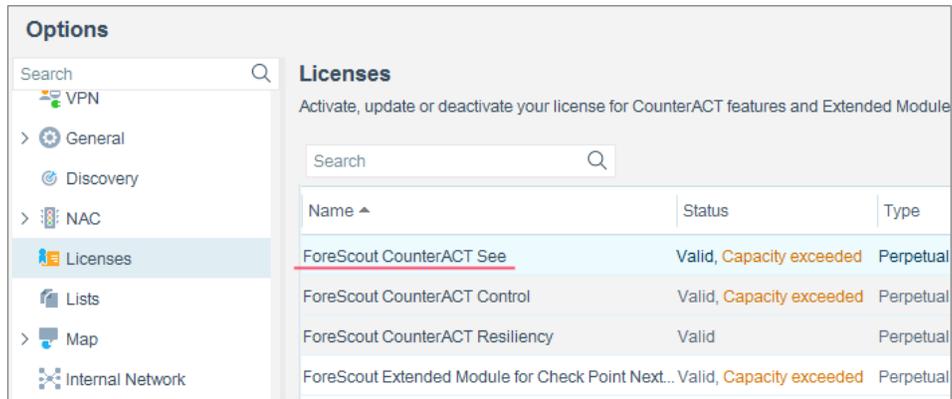
Documentation Portal

Select **Documentation Portal** from the **Help** menu.

Identifying Your Licensing Mode in the Console

If your Enterprise Manager has a *ForeScout CounterACT See* license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select **Options > Licenses** to see whether you have a *ForeScout CounterACT See* license listed in the table.



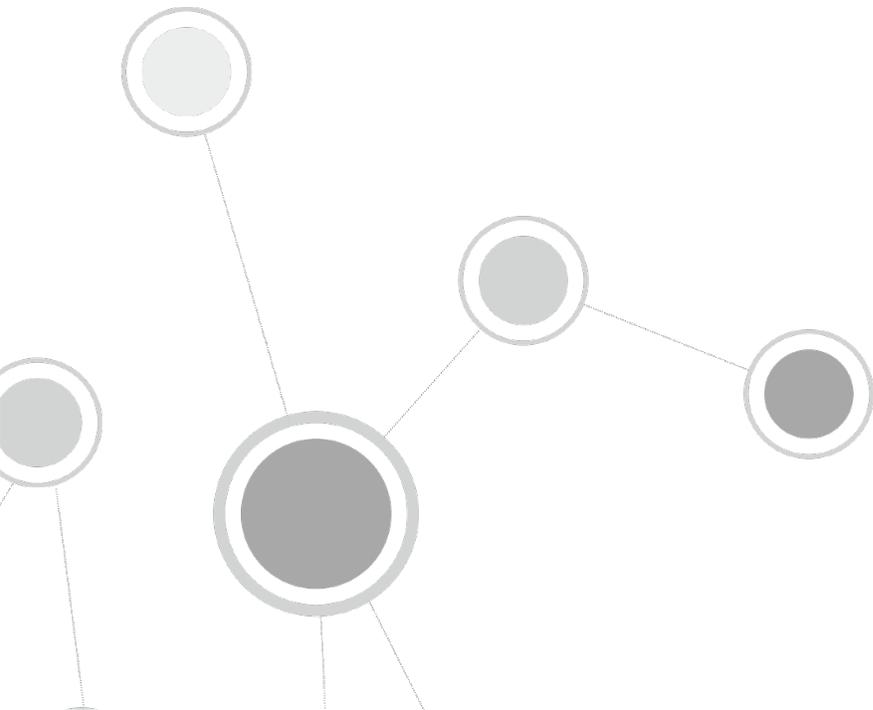
The screenshot shows the 'Options' menu on the left with 'Licenses' selected. The main area displays the 'Licenses' section with a search bar and a table of license information.

Name ▲	Status	Type
<u>ForeScout CounterACT See</u>	Valid, Capacity exceeded	Perpetual
ForeScout CounterACT Control	Valid, Capacity exceeded	Perpetual
ForeScout CounterACT Resiliency	Valid	Perpetual
ForeScout Extended Module for Check Point Next...	Valid, Capacity exceeded	Perpetual

Contact your ForeScout representative if you have any questions about identifying your licensing mode.

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
- Licensing Mode



CounterACT Components

CounterACT components include:

- [CounterACT Appliance](#)
- [CounterACT Enterprise Manager](#)
- [Recovery Enterprise Manager](#)
- [CounterACT Console](#)



CounterACT Device

Virtual systems are also available. See [Chapter 8: CounterACT Virtual Systems](#) for more information.

Refer to the *CounterACT Enterprise Manager Appliance Communication Technical Note* for information regarding Enterprise Manager/Appliance communication. See [Additional CounterACT Documentation](#) for information on how to access the guide.

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:

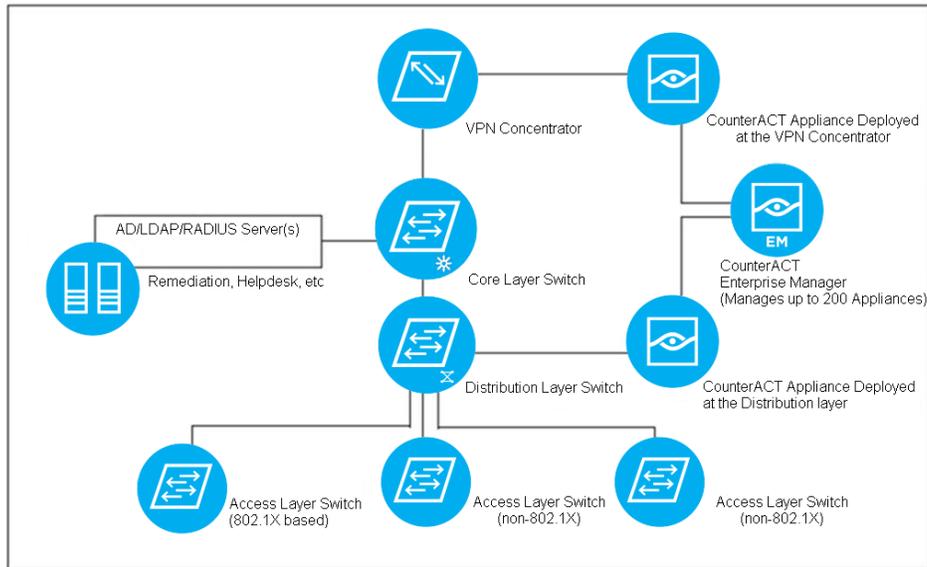
- At the connection point between a protected network area and the rest of the network. This enables protection of a specific network range against infection attempts initiated from the rest of the network and network protection against infection attempts generated from a specific network area (e.g. 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.
- 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

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.

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 User Guide* for more information. See [Additional CounterACT Documentation](#) for information on how to access the guide.

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 Administration Guide* for more information. See [Additional CounterACT Documentation](#) for information on how to access the guide.

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.

CT-xxxx Appliances based on Hardware revision 3x/4x and ForeScout 51xx Appliances support Integrated Dell Remote Access Controller (iDRAC). See [Integrating CT-xxxx Appliances Based on Hardware Revision 3x/4x and ForeScout 51xx Appliances with iDRAC](#) for information about setting up this module.

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 User Guide* for more information. See [Additional CounterACT Documentation](#) for information on how to access the guide.

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](#)).

- [Supported Physical CounterACT Devices](#)
- [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.

Supported Physical CounterACT Devices

This version of CounterACT can be installed on all hardware revisions of CounterACT physical Appliances and Enterprise Managers **except for the following**:

Model	Revisions Not Supported
CTR	CTR-11, CTR-12, CTR-13
CT100	CT100-20, CT100F-20 CT100-21, CT100F-21 CT100-22, CT100F-22
CT1000	CT1000-20, CT1000F-20, CT1000F2-20 CT1000-21, CT1000F-21, CT1000F2-21 CT1000-22, CT1000F-22, CT1000F2-22
CT-2000	CT2000-20, CT2000F-20, CT2000F2-20
CEM-25	CT2000-21, CT2000F-21, CT2000F2-21
CEM-50	CT2000-22, CT2000F-22, CT2000F2-22

Model	Revisions Not Supported
CT-4000 CEM-100	CT4000-20, CT4000F-20, CT4000F2-20, CT4000F10G-20 CT4000-21, CT4000F-21, CT4000F2-21, CT4000F10G-21 CT4000-22, CT4000F-22, CT4000F2-22, CT4000F10G-22
CT-10000 CEM-150 CEM-200	CT10000-20, CT10000F-20, CT10000F2-20 CT10000-21, CT10000F-21, CT10000F2-21, CT10000F10G-21 CT10000-22, CT10000F-22, CT10000F2-22, CT10000F10G-22
CEM-05 CEM-10	CT1000MS-20, CT1000MS-21 CT1000MS-22

 *CT-xxxx CounterACT devices based on hardware revision -10 or lower also do not support CounterACT version 8.0.*

To determine the revision of a specific Enterprise Manager, do one of the following:

- Run the *fstool model* command on the Enterprise Manager.
- See the product label on the machine.

To determine the revision of a specific Appliance, do one of the following:

- Run the *fstool model* command on the Appliance.
- Run the *fstool tech-support oneachmodel* command on the Enterprise Manager. Running this command requires the **Technical Support Plugin 1.1.2**.
- See the product label on the machine.

Contact your ForeScout sales representative for alternative solutions if any of your Appliances are on this list of revisions not supported.

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 7/8/8.1/10
 - Windows Server 2008/2008 R2/2012/2012 R2/2016
 - Linux RHEL/CentOS 7
- 2GB RAM
- 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.

Port	Service	To or From CounterACT	Function
22/TCP	SSH	From	Allows remote inspection of OS X and Linux endpoints. Allows CounterACT to communicate with network switches and routers.
		To	Allows access to the CounterACT command line interface.
2222/TCP	SSH	To	(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.
25/TCP	SMTP	From	Allows CounterACT access to the enterprise mail relay.
53/UDP	DNS	From	Allows CounterACT to resolve internal IP addresses.
80/TCP	HTTP	To	Allows HTTP redirection.
123/UDP	NTP	From	Allows CounterACT access to a local time server or ntp.forescout.net. By default CounterACT accesses ntp.foreScout.net
135/TCP	MS-WMI	From	Allows remote inspection of Windows endpoints.
139/TCP	SMB, MS-RPC	From	Allows remote inspection of Windows endpoints (For endpoints running Windows 7 and earlier).
445/TCP			Allows remote inspection of Windows endpoints.
161/UDP	SNMP	From	Allows CounterACT to communicate with network switches and routers. For information about configuring SNMP, refer to the <i>CounterACT Administration Guide</i> .
162/UDP	SNMP	To	Allows CounterACT to receive SNMP traps from network switches and routers. For information about configuring SNMP, refer to the <i>CounterACT Administration Guide</i> .

Port	Service	To or From CounterACT	Function
389/TCP (636)	LDAP	From	Allows CounterACT to communicate with Active Directory. Allows communication with CounterACT web-based portals.
443/TCP	HTTPS	To	Allows HTTP redirection using TLS.
2200/TCP	SecureConnector for Linux	To	Allows SecureConnector to create a secure (encrypted SSH) connection to the Appliance from Linux machines. <i>SecureConnector</i> is a script based agent that enables management of Linux endpoints while they are connected to the network.
10003/TCP	SecureConnector for Windows	To	Allows SecureConnector to create a secure (encrypted TLS) connection to the Appliance from Windows machines. <i>SecureConnector</i> is an agent that enables management of Windows endpoints while they are connected to the network. Refer to the <i>CounterACT Administration Guide</i> 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.
10005/TCP	SecureConnector for OS X	To	Allows SecureConnector to create a secure (encrypted TLS) connection to the Appliance from OS X machines. <i>SecureConnector</i> is an agent that enables management of OS X endpoints while they are connected to the network. Refer to the <i>CounterACT Administration Guide</i> 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.

Port	Service	To or From CounterACT	Function
13000/TCP	CounterACT	From/To	<p>For environments with only one Appliance – from the Console to the Appliance.</p> <p>For environments 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.</p>

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 Administration Guide* for more information about these features. See [Additional CounterACT Documentation](#) for information on how to access the guide.

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

Refer to the [ForeScout Licensing and Sizing Guide](#) for information on bandwidth requirements.

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 CLI 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:

```
You are about to disable FIPS 140-2 on this CounterACT machine.  
Note that CounterACT service will be restarted.  
Disable FIPS and restart CounterACT service? (yes/no) :
```

Verifying FIPS Compliance

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

`fstool version`

```
-----  
<CounterACT_device_type> version information  
-----  
  
Version           : 8.0.0  
Build number      : <build_number>  
Build date        : <date_time_stamp>  
HA supported      : <Yes|No>  
FIPS enabled      : <Yes|No>
```

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)**.

Licensing Mode

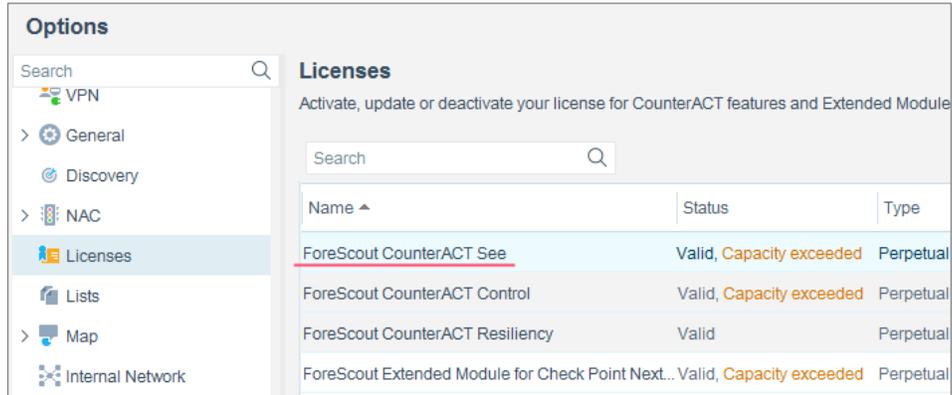
This version of CounterACT supports two different licensing modes. Each CounterACT deployment operates in one of the two modes. You may have multiple deployments that use different licensing modes. License requirements differ according to licensing mode.

Refer to the *CounterACT Administration Guide* for more information about licensing management and licensing modes. See [Additional CounterACT Documentation](#) for information on how to access the guide.

Identifying Your Licensing Mode in the Console

If your Enterprise Manager has a *ForeScout CounterACT See* license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select **Options > Licenses** to see whether you have a *ForeScout CounterACT See* license listed in the table.



Contact your ForeScout representative if you have any questions about identifying your licensing mode.

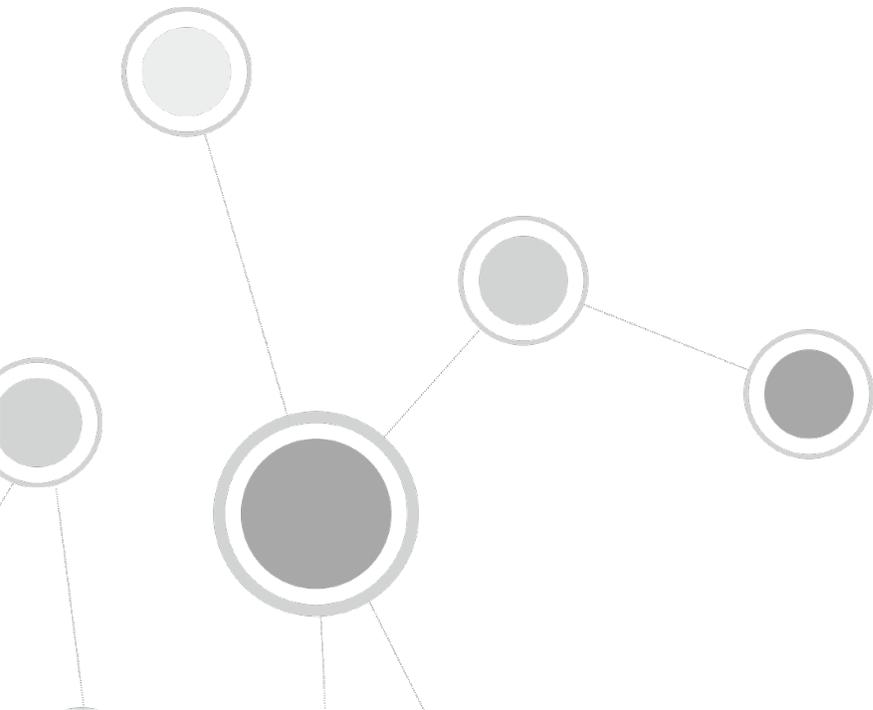
Chapter 2: Network Setup

[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 User Guide* for more information about the configuration and wiring. See [Additional CounterACT Documentation](#) for information on how to access the guide.

Related Documents

Cisco Switches

For information about port mirroring on Cisco switches, refer to the *Configuring the Cisco Switched Port Analyzer (SPAN)* document, which can be accessed from one of two ForeScout portals, depending on which licensing mode your deployment is using.

- **Per-Appliance Licensing Mode**
<https://updates.forescout.com/support/files/docs/Configuring-Cisco-SPAN.pdf>
- **Centralized Licensing Mode**
[Customer Portal](#), Documentation Page (Hardware Setup)

Rack Mounting Instructions

For information regarding rack-mounting instructions refer to:

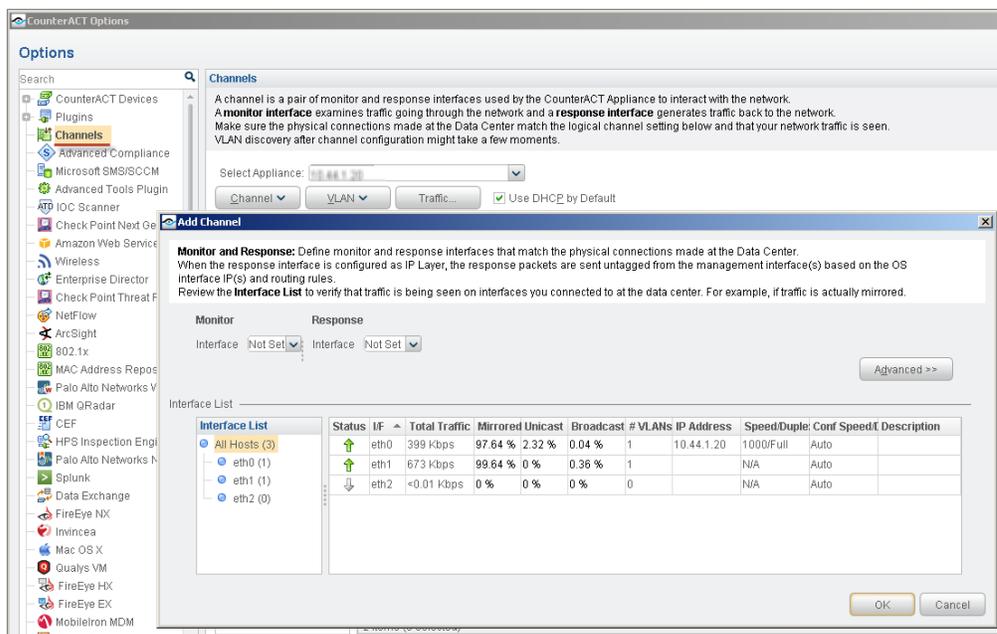
- 📄 *If your deployment uses Centralized Licensing Mode, the documents below can be accessed from the Documentation Page (Hardware Setup) of the [Customer Portal](#).*
- For CT-xxxx Appliances based on hardware revision 3x/4x
 - CT-100 and CT-1000 Appliances:
<https://updates.forescout.com/downloads/support/CT-AS-Rail-Kit-100-1000-rev3x.pdf>
 - CT-2000, CT-4000 and CT-10000 Appliances
<https://updates.forescout.com/downloads/support/CT-AS-Rail-Kit-2000-4000-10000-rev3x.pdf>
- For ForeScout 51xx Appliances (5120, 5140 and 5160):
<https://updates.forescout.com/downloads/support/51xx-Rail-Kit-5120-5140-5160.pdf>

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 Administration Guide*. See [Additional CounterACT Documentation](#) for information on how to access the guide.

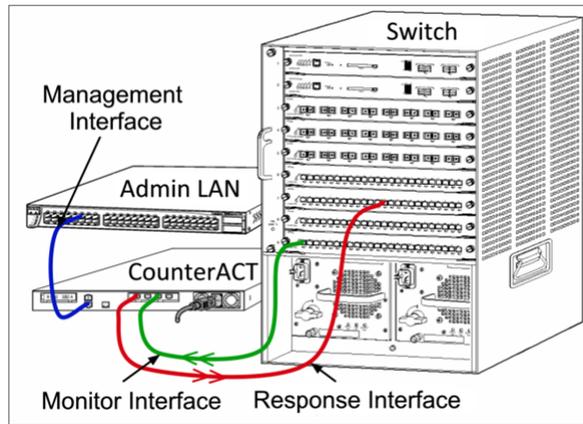


Management Interface

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 network services.

See [Network Access Requirements](#) for more information.



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 CLI 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.

- **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.

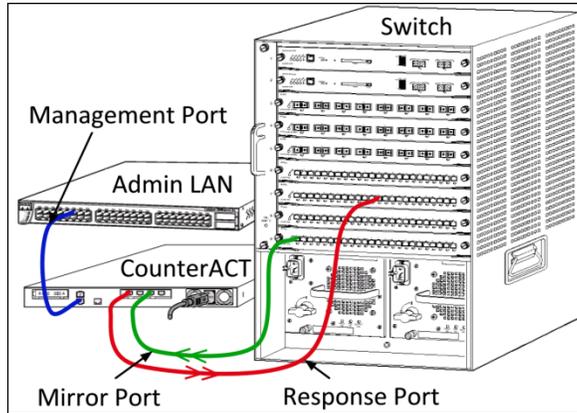
Setting up Switch Connections

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

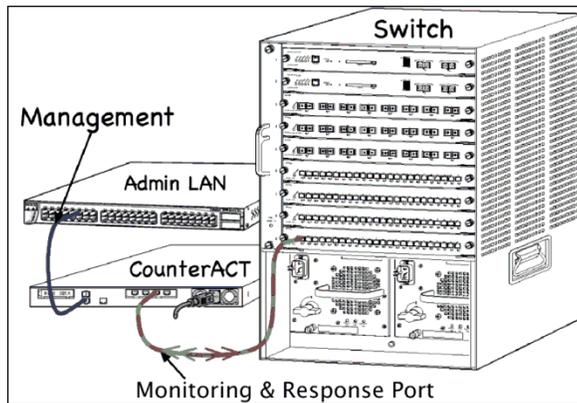
The recommended installation uses three separate cables as detailed in [Appliance Interface Connections](#).



Separate Management, Monitor and Response Ports

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.

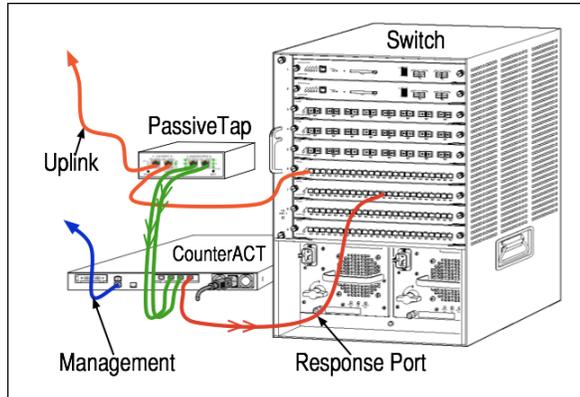


Combined Monitor and Response Port

Passive Inline Tap

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

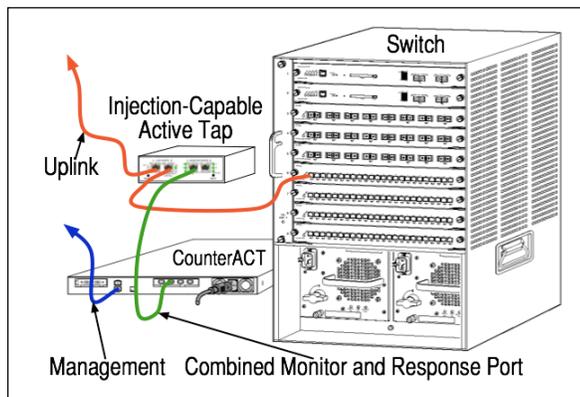
A passive inline tap requires two monitor ports (one for upstream traffic and one for downstream traffic), except in the case of a *recombination* tap, which combines the two duplex streams into a single port. Note that if the traffic on the tapped port is 802.1Q VLAN tagged, then the response port must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



Active Inline Tap

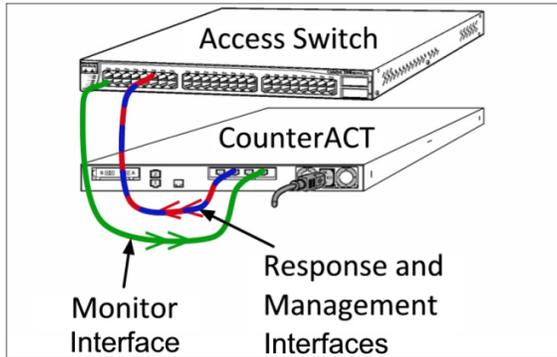
IP Layer Response (for Layer-3-Only Core Switch Installation)

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.

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.

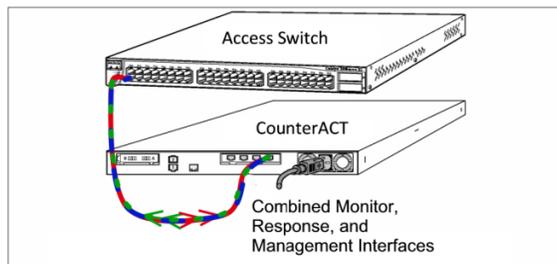


Combined Management and Response Port (Single VLAN Only)

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.



Combined Management, Response and Monitor Port (Single VLAN)

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 CLI 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:

```

Destination Net IP address : 13.0.0.0
Destination Genmask IP address : 255.0.0.0
Gateway IP address [0.0.0.0] : 10.0.4.108

-----
CounterACT Machine Static Routing Table Configuration
-----

Destination      Gateway          Genmask          Iface
13.0.0.0         10.0.4.108      255.0.0.0       eth0
12.0.0.0         10.0.4.108      255.0.0.0       eth0
11.0.0.0         10.0.4.109      255.0.0.0       eth0

(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:

```

1) eth0   Address: 10.0.4.197   Netmask: 255.255.255.0

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 CLI 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.

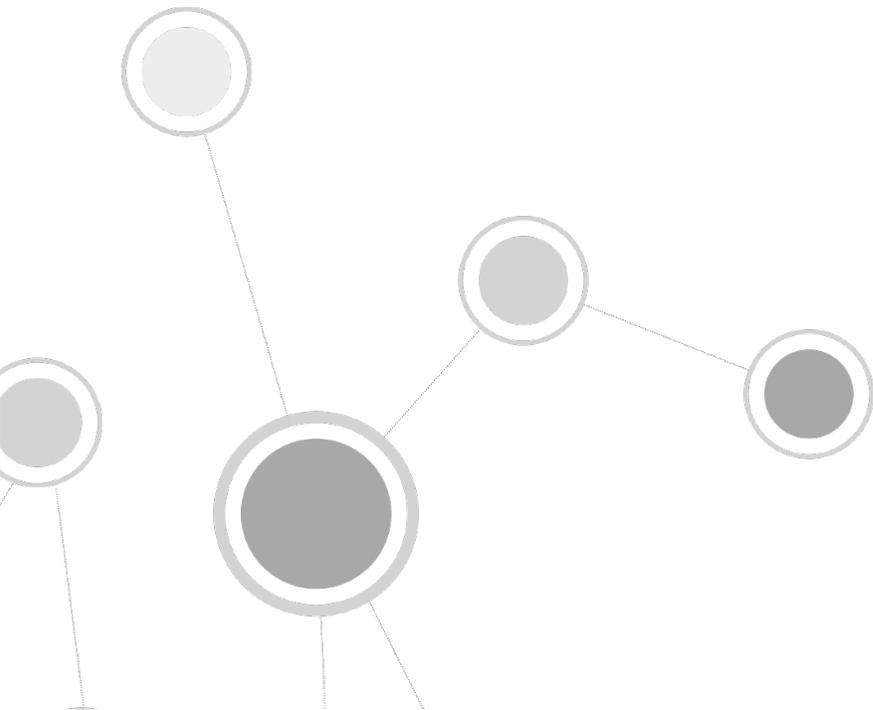
Chapter 3: Appliance Setup and Configuration, and Post-Installation Procedures

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 device and the ForeScout 5110 device do 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 Administration Guide* for more information. See [Additional CounterACT Documentation](#) for information on how to access the guide.

If the installation is interrupted or if you selected the wrong CounterACT version, you will need to reimage the Appliance with the relevant version of the ISO file. See [Chapter 6: Reimaging CounterACT Devices](#) for more information.

Some variations may apply to virtual systems. See [Chapter 8: CounterACT Virtual Systems](#) for details.

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

```
CounterACT 8.0.0-<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) :1
```

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. See the *CounterACT Installation Guide version 7.0.0* for details on configuring CounterACT 7.0.0.

```
CounterACT 8.0.0-<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, select **Identify and renumber network interfaces** 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) Add node to existing Active Node (Primary or Secondary)

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.

```
>>>>> Select Licensing Mode <<<<<<

1) Per Appliance Licensing Mode
2) Centralized Licensing Mode

Choice (1-2) [1]:
```

10. Select the licensing mode that your deployment uses. The licensing mode is determined during purchase. **Do not type a value until you have verified what licensing mode your deployment uses.** Contact your ForeScout representative to verify your licensing mode or if you entered the wrong mode.

Type **1** for the Per-Appliance Licensing Mode or **2** for the Centralized Licensing Mode and press **Enter**.

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

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

Description :
```

11. 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 should
contain at least one non-alphabetic character.

Administrator password :
```

12. 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) :
```

- 13.** 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 :
```

- 14.** 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 IP address :
Network mask [255.255.255.0] :
Default gateway :
Domain name :
DNS server addresses :
Management IPv6 address or 'auto' 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.

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

- 16.** 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 >,
Interface: eth<n>,
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 :
```

17. 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
```

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

19. 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
```

20. Press **Enter**.

After configuration, ensure that your CounterACT device has a valid license. The default licensing state of your CounterACT device depends on which licensing mode your deployment is using.

- If you are using **Per-Appliance Licensing Mode**, 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.)

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.

You will be alerted that your demo license is about to expire in a number of ways. Refer to the *CounterACT Administration Guide* for more information about demo license alerts. See [Additional CounterACT Documentation](#) for information on how to access the guide.

- If you are using **Centralized Licensing Mode**, the *Entitlement administrator* should receive an email when the license entitlement is created and available in the ForeScout Customer Portal (Each customer is assigned at least one *Entitlement administrator* who has permissions to download license files, software and documentation in the Portal for all customer deployments.). Once available, the *CounterACT administrator* of the deployment can activate the license in the CounterACT Console. Until the license is activated, CounterACT features will not function properly. For example, policies will not be evaluated and actions will not be performed. *No demo license is automatically installed during system installation.*

See [Licensing Mode](#) for more information on licensing modes and to find out which mode you are using. Refer to the *CounterACT Administration Guide* for more information about license management. See [Additional CounterACT Documentation](#) for information on how to access the guide.

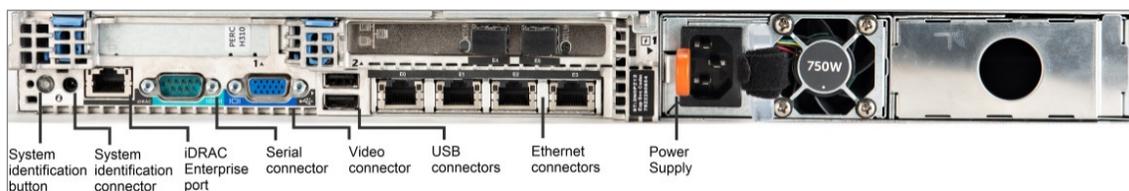
Post-Installation Procedures

After installing an Appliance, perform the following tasks:

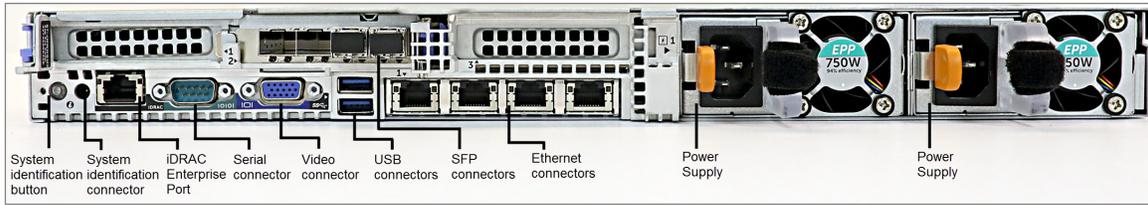
- [Connect an Appliance to the Network](#)
- [Integrate with Remote System Management](#)
- [Verify the Management Interface Connection](#)
- [Perform a Ping Test](#)
- [Generate a Configuration Summary for an Appliance](#)
- [Configure Password Protection for the Boot Loader](#)
- Install the CounterACT Console. See [Chapter 7: Installing the CounterACT Console](#).
- Run the Initial Setup Wizard. Refer to the *CounterACT Administration Guide*. See [Additional CounterACT Documentation](#) for information on how to access the guide.

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.)



Sample Appliance Rear Panel –CT-xxxx Appliance



Sample Appliance Rear Panel – ForeScout 51xx Appliance

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.*

SFP Model	Details	Supported Appliances
FCLF8521P2BTL	1Gb/s, 1000BASE-T	<ul style="list-style-type: none"> CT-xxxx ForeScout 5120/5140/5160
FTLF1318P3BTL	1Gb/s, 1000BASE-LX	<ul style="list-style-type: none"> CT-xxxx ForeScout 5120/5140/5160
FTRJ1319P1BTL		
FTLF8519P3BNL	1Gb/s, 1000BASE-SX	<ul style="list-style-type: none"> CT-xxxx ForeScout 5120/5140/5160
FTLF8519P2BCL		
FTLX1471D3BCL	10Gb/s 10GBase-LR SFP+	CT-xxxx
FTLX8571D3BCL / FTLX8574D3BCL	10Gb/s 10GBase-SR SFP+	CT-xxxx
FTLX1471D3BCV	10G/1G Dual Rate (10GBASE-LR and 1000BASE-LX)	ForeScout 5120/5140/5160
FTLX8574D3BCV	10G/1G Dual Rate (10GBASE-SR and 1000BASE-SX)	ForeScout 5120/5140/5160
571540003 (AMPHENOL)	Direct Attach 10G	ForeScout 5120/5140/5160

Integrate with Remote System Management

You can integrate with Remote System Management using iDRAC. This integration is not applicable to virtual systems.

- 📄 *Remote System Management features of CounterACT Appliances (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 CT-xxxx Appliances Based on Hardware Revision 3x/4x and ForeScout 51xx Appliances 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:

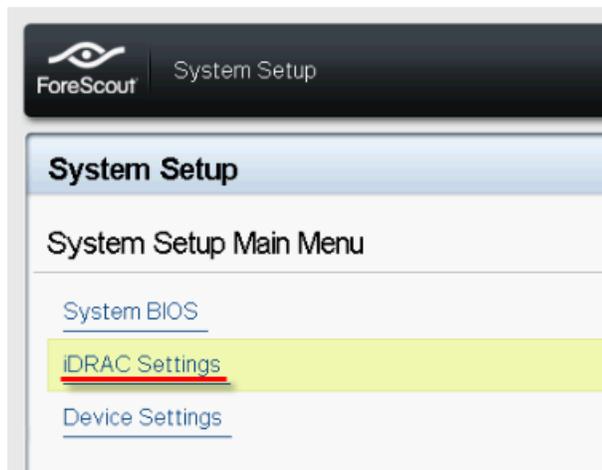
- [Enable and Configure the iDRAC Module](#)
- [Connect the Module to the Network](#)
- [Log In to iDRAC](#)

Enable and Configure the iDRAC Module

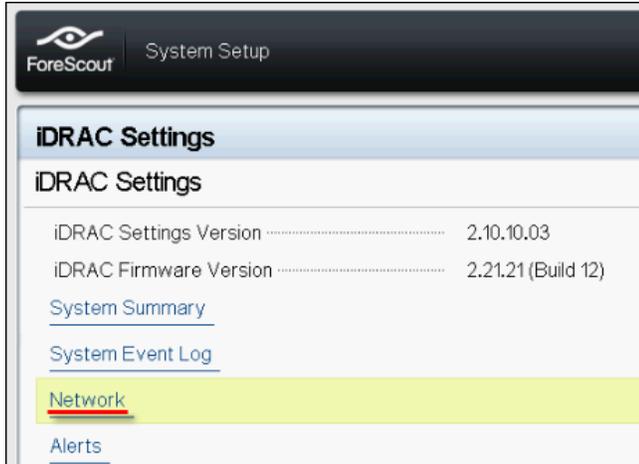
Change the iDRAC settings to enable remote access on the CounterACT device. This section describes basic integration settings required for working with CounterACT.

To configure iDRAC:

1. Turn on the managed Appliance.
2. Select F2 during the boot process.
3. In the System Setup Main Menu page, select **iDRAC Settings**.

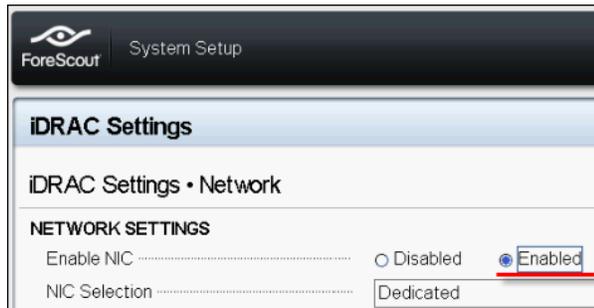


4. In the iDRAC Settings page, select **Network**.



5. Configure the following Network settings:

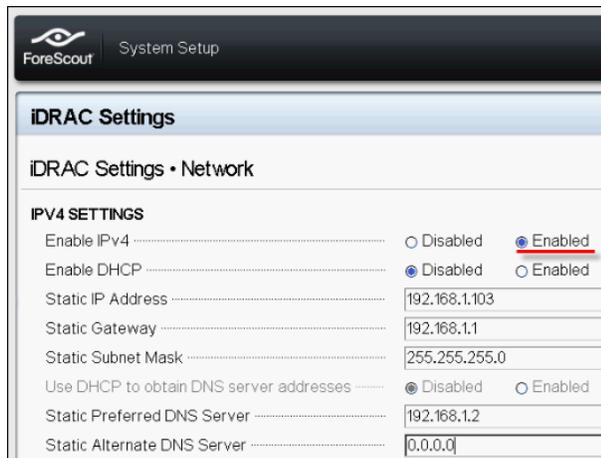
- **Network Settings.** Verify that the **Enable NIC** field is set to **Enabled**.



- **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.

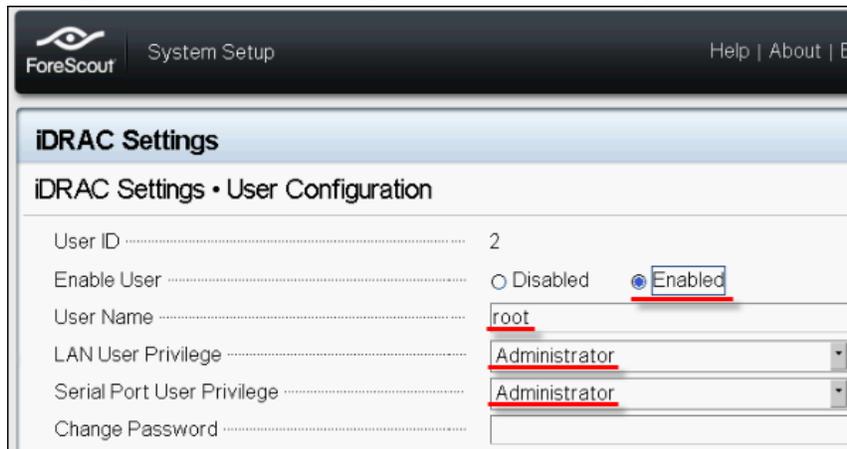


6. Select **Back**.

7. Select **User Configuration**.
8. Configure the following User Configuration fields for the root user:
 - **Enable User.** Verify that this field is set to Enabled.

 *The user name configured here is not the same as the CounterACT 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 configured 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

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

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*. You can access this guide in one of the following locations, depending on the licensing mode your deployment is using:

- Per-Appliance Licensing Mode - https://updates.forescout.com/downloads/support/iDRAC_user_guide.pdf
- Centralized Licensing Mode – [Customer Portal](#), Documentation Page.

See [Additional CounterACT Documentation](#) (*Identifying Your Licensing Mode in the Console*) to learn which licensing mode your deployment is using.

- 📄 *It is very important to update the default root password, if you have not done so already.*

Verify the Management Interface Connection

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

```
fstool linktest
```

The following information is displayed:

```
Management Interface status
Pinging default gateway information
```

```
Ping statistics
Performing Name Resolution Test
Test summary
```

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 CLI and run the following command:

```
fstool config_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

In: ethX <tagged|untagged>      Out: ethX <tagged|untagged>

CounterACT Configuration

SMTP Privacy
Mail relay
Operator mail
Protected net
Management Clients
SSH Clients
```

2. Save the information required.

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 CLI.
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.

Configure ICMP Settings

ICMP traffic on external interfaces is enabled by default in your CounterACT system.

To disable ICMP:

1. Log in to the Appliance CLI and run the following command:
`fstool set_property fs.fw.icmp.expired.time 0`
2. Restart the Appliance services by running the following command:
`fstool service restart`

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:
`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 Administration Guide* for more information. See [Additional CounterACT Documentation](#) for information on how to access the guide.

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 back up 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 User Guide* for details about working with High Availability systems. See [Additional CounterACT Documentation](#) for information on how to access the guide.

Chapter 4: Enterprise Manager Setup and Configuration, and Post-Installation Procedures

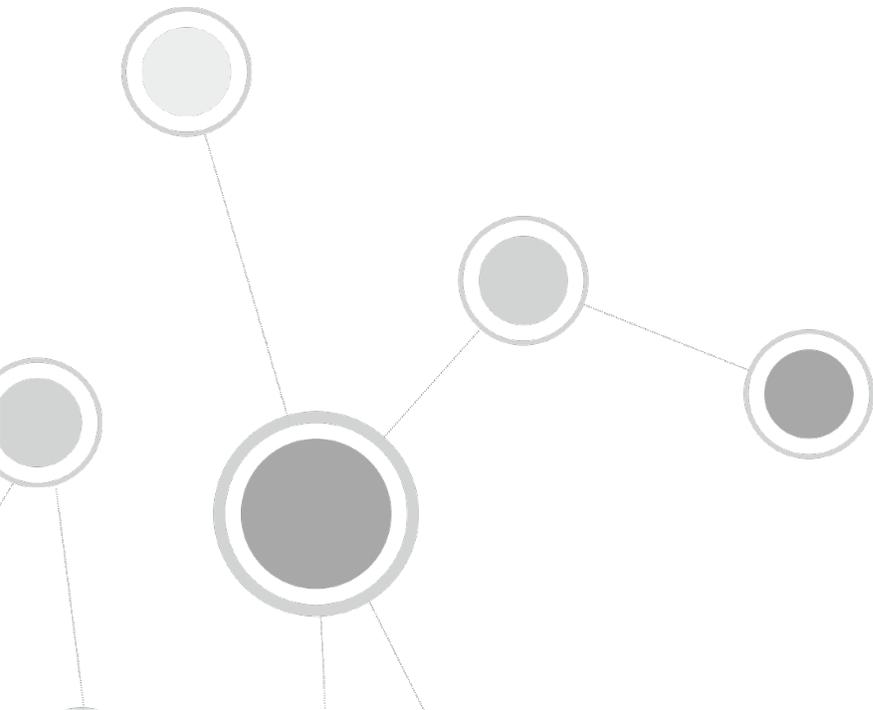
About the Installation

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 Administration Guide* for more information. See [Additional CounterACT Documentation](#) for information on how to access the guide.

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.

If the installation is interrupted or if you selected the wrong CounterACT version, you will need to reimage the Appliance with the relevant version of the ISO file. See [Chapter 6: Reimaging CounterACT Devices](#) for more information.

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

```
CounterACT 8.0.0-<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) :1
```

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. Refer to the *CounterACT Installation Guide* for details. 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. See the *CounterACT Installation Guide version 7.0.0* for details on configuring CounterACT 7.0.0.

```
CounterACT 8.0.0-<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) Add node to existing Active Node (Primary or Secondary)
```

```
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.

```
>>>>> Select Licensing Mode <<<<<<

1) Per Appliance Licensing Mode
2) Centralized Licensing Mode

Choice (1-2) [1]:
```

10. Select the licensing mode that your deployment uses. The licensing mode is determined during purchase. ***Do not type a value until you have verified what licensing mode your deployment uses.*** Contact your ForeScout representative to verify your licensing mode or if you entered the wrong mode.

Type **1** for the Per-Appliance Licensing Mode or **2** for the Centralized Licensing Mode and press **Enter**.

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

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

Description [Enterprise Manager] :
```

11. 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 should
contain at least one non-alphabetic character.

Administrator password :
```

12. 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) :
```

13. 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 :
```

14. 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):

```
>>>>> Configure Network Settings <<<<<<<

Management IP address :
Network mask [255.255.255.0] :
Default gateway :
Domain name :
DNS server addresses :
Management IPv6 address or 'auto' 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.

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

16. 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:                Enterprise Manager
Host name:           <user_entered_value>
Description:         <user_entered_value>
Management Interface: < user_entered_value >,
Interface: eth<n>,
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 :

```

17. 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

```

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

19. 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

```

20. Press **Enter**.

After configuration, ensure that your CounterACT device has a valid license. The default licensing state of your CounterACT device depends on which licensing mode your deployment is using.

- If your CounterACT deployment is operating in **Per-Appliance Licensing Mode**, 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.).

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.

You will be alerted that your demo license is about to expire in a number of ways. Refer to the *CounterACT Administration Guide* for more information about demo license alerts. See [Additional CounterACT Documentation](#) for information on how to access the guide.

- If your CounterACT deployment is operating in **Centralized Licensing Mode**, the *Entitlement administrator* should receive an email when the license entitlement is created and available in the ForeScout Customer Portal. Once available, the *CounterACT administrator* of the deployment can activate the license in the CounterACT Console. Until the license is activated, CounterACT features will not function properly. For example, policies will not be evaluated and actions will not be performed. *No demo license is automatically installed during system installation.*

See [Licensing Mode](#) for more information on licensing modes and to find out which mode you are using. Refer to the *CounterACT Administration Guide* for more information about license management. See [Additional CounterACT Documentation](#) for information on how to access the guide.

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 Integrated Dell Remote Access Controller (iDRAC), 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 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 Administration Guide* for more information. See [Additional CounterACT Documentation](#) for information on how to access the guide.

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**.

```
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.

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

```
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**.

```
-----
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 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

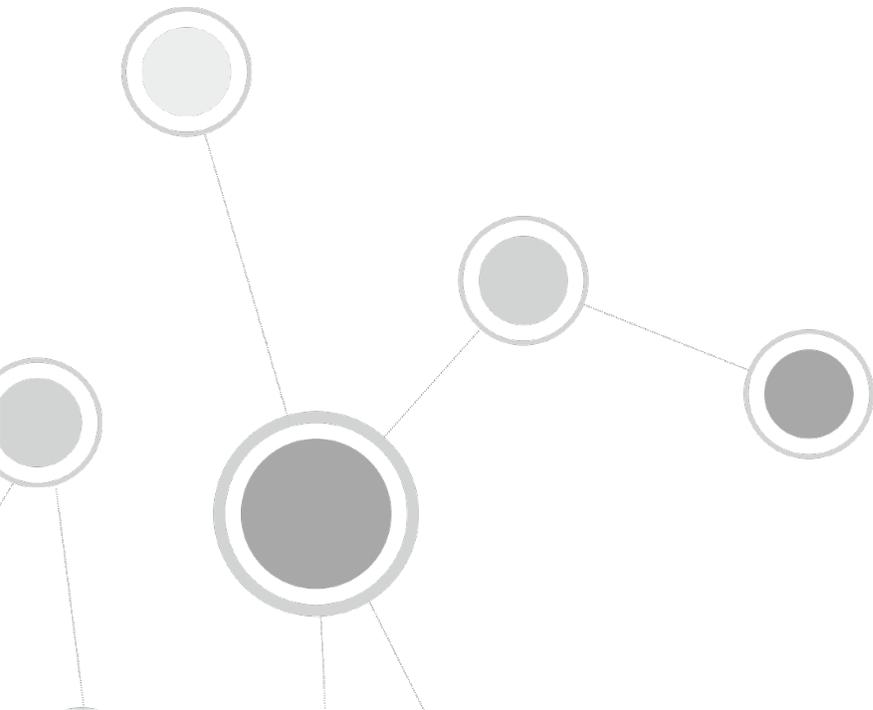
on High Availability Backup and Restore in the *Resiliency Solutions User Guide* for details about working with High Availability systems. See [Additional CounterACT Documentation](#) for information on how to access the guide.

Chapter 5: Upgrading CounterACT Devices

Upgrading to a New Version

Upgrading to a New Version and Migrating to Centralized Licensing Mode (v8.0)

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. See [Additional CounterACT Documentation](#) for information on how to access the release notes.

To upgrade to a new CounterACT version:

1. Before upgrading Appliances, you should upgrade your Enterprise Manager.
2. Download or obtain the upgrade file and save it to a location on your computer.
3. Select **Options** from the **Tools** menu.
CounterACT devices or Appliances are shown with their current version.
4. Select an Enterprise Manager or Appliances and select **Upgrade**. Do not select Enterprise Managers together with Appliances, because you cannot upgrade both Appliances and Enterprise Managers at the same time. The file selection dialog box opens.
5. Locate the upgrade file that you saved on your computer and select **OK**. After a check of the digital signature of the upgrade file is performed, the CounterACT Upgrade screen opens.
6. Select the **I accept the Terms and Conditions** checkbox. It is recommended to read the Release Notes.
7. Select **Verify**. A pre-upgrade check is performed to verify that the environmental and software requirements have been met. When the verification finishes, the Pre-Upgrade Verification summary screen opens.
 - 📄 *When upgrading an Appliance connected to an Enterprise Manager that was upgraded to the current CounterACT version, the pre-upgrade check is not performed, and the **Upgrade** button is immediately available in the CounterACT Upgrade screen.*
8. Select **Upgrade** when you are sure you want to proceed with the upgrade. Once you confirm, the upgrade process proceeds to completion and cannot be interrupted or cancelled.

High Availability Devices – Upgrade for High Availability devices can take a long time (up to a number of hours). If the upgrade of the second node and the synchronization are not shown in the log, you can verify status via icons on the Console status bar:

	Indicates the status of the High Availability Appliances connected to the Enterprise Manager.
	Indicates the status of the Enterprise Manager High Availability pair.
	Indicates that High Availability is down on the Appliance.



Indicates that High Availability is down on the Enterprise Manager.

9. When the upgrade is completed successfully, select **Close**. If the upgrade is not successful, contact your ForeScout representative and **do not** continue with more upgrades.

Upgrading High Availability Devices

For High Availability devices, back up the pair before you upgrade. The pair must be up when you upgrade. For High Availability upgrade information, refer to the section on upgrading High Availability systems in the *CounterACT Administration Guide*. See [Additional CounterACT Documentation](#) for information on how to access the guide.

To upgrade a single active High Availability node when the Secondary node has failed or has not been set up:

1. Make sure the Secondary node is not accessible
2. Create the file `.ignorestandby` under `/etc/` on the node to be upgraded.

Upgrading to a New Version and Migrating to Centralized Licensing Mode (v8.0)

If you are running CounterACT version 7.0.0 and would like to upgrade your deployment to version 8.0 operating in Centralized Licensing Mode, perform the following upgrade/migration procedure.

- 📄 *All CounterACT releases prior to version 8.0 operate in Per-Appliance Licensing Mode. Refer to the CounterACT Administration Guide for more information about licensing. See [Additional CounterACT Documentation](#) for information on how to access the guide.*

Before performing the migration, contact your ForeScout representative to ensure you have a valid license entitlement for CounterACT version 8.0, operating in Centralized Licensing Mode. Verify that you have credentials to access the ForeScout Customer Portal and that the license entitlement has been added.

If you are using ForeScout Extended Modules, be aware that Integration Modules, packaging together *groups of related licensed modules*, are not supported when operating in Centralized Licensing Mode. Only Extended Modules, packaging *individual licensed modules* are supported. **Before migration, uninstall any Integration Modules and reinstall them as Extended Modules.** Refer to the sections on ForeScout Extended Modules and Module Packaging in the *CounterACT Administration Guide* for more information. See [Additional CounterACT Documentation](#) for information on how to access the guide.

To upgrade and migrate to Centralized Licensing Mode:

1. Back up Enterprise Manager system settings. Refer to the section on performing a one-time system backup in the *CounterACT Administration Guide*. See [Additional CounterACT Documentation](#) for information on how to access the guide.

2. Upgrade the Enterprise Manager to CounterACT Version 8.0. See [Upgrading to a New Version](#). Use the CounterACT Upgrade file (FSP) for version 8.0.

After the upgrade, the Console is upgraded automatically, and all Appliances will become disconnected from the Enterprise Manager. The Appliances will continue to function normally and will reconnect to the Enterprise Manager after you upgrade the Appliances to CounterACT Version 8.0 in step 6.

3. Upgrade the Recovery Enterprise Manager to CounterACT Version 8.0. This procedure is only relevant if your deployment has a Recovery Enterprise Manager. See [Upgrading to a New Version](#).

After the upgrade, the Recovery Enterprise Manager will reconnect to the Enterprise Manager.

4. Configure the Enterprise Manager to operate in Centralized Licensing mode:
 - a. Log in to the Enterprise Manager via the Console.
 - b. Navigate to **Options > Licenses** and select **Migrate**. Continuing with the migration will restart the CounterACT Console and the Enterprise Manager and all CounterACT devices in the deployment that are connected to the Enterprise Manager. The License Migration dialog box opens.
 - c. Select **Migrate**.

After the Enterprise Manager is up and running, the licenses are invalid and CounterACT features will not function properly.

5. Activate a new license file. Refer to the section on activating a new license file (Centralized Licensing Mode) in the *CounterACT Administration Guide*. See [Additional CounterACT Documentation](#) for information on how to access the guide.

 *If your deployment includes a Recovery Enterprise Manager or High Availability device, verify that it is connected to the Enterprise Manager before you activate the license file on your deployment.*

6. Upgrade each Appliance to CounterACT Version 8.0. See [Upgrading to a New Version](#). Use the CounterACT Upgrade file (FSP) for version 8.0.

After the upgrade, the Appliances will reconnect to the Enterprise Manager and then restart due to the change in licensing mode.

7. If the Failover Clustering Module is installed in your deployment, uninstall it from the Console (on the Enterprise Manager) in the Options>Modules page. In Centralized Licensing mode, Failover Clustering functionality is supported by the *Resiliency License*. Refer to the section on the Resiliency License in the *CounterACT Administration Guide*. See [Additional CounterACT Documentation](#) for information on how to access the guide.

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.

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, Gradual Upgrade Guide*. See [Additional CounterACT Documentation](#) for information on how to access the guide.

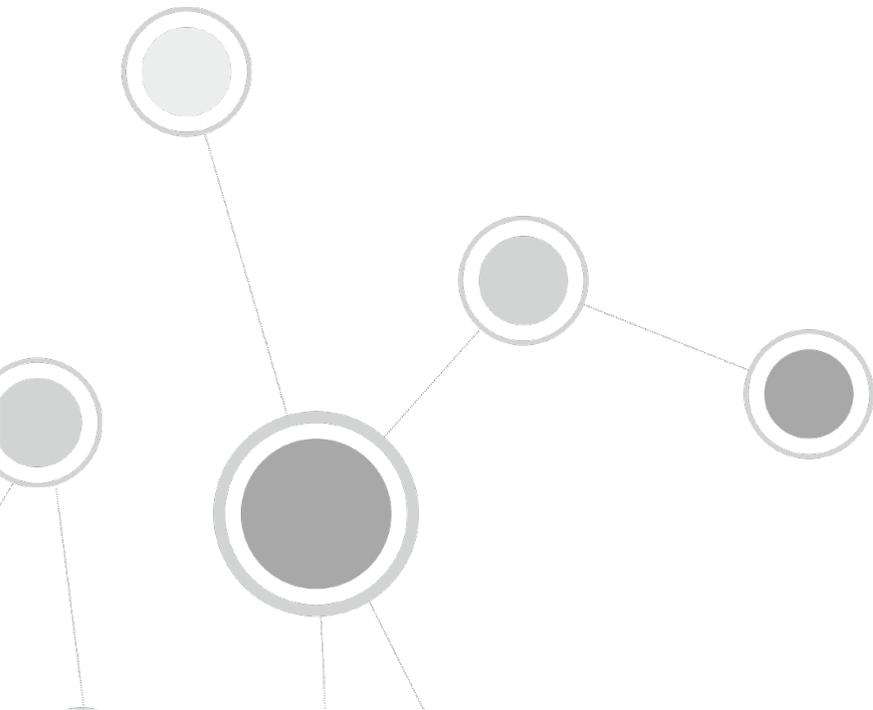
Chapter 6: Reimaging CounterACT Devices

[Reimaging CounterACT Devices](#)

[Prepare an Installation DVD](#)

[Prepare a Bootable USB Memory Device](#)

[Reimage the CounterACT Device](#)



Reimaging CounterACT Devices

If you need to reinstall CounterACT on a device (for example, where upgrade or configuration have failed and cannot be completed), you can reimage the device using a prepared DVD or USB memory device.

Prepare an Installation DVD

To prepare an installation DVD:

1. Download or obtain the CounterACT ISO image from the [CounterACT Product Downloads page](#).
2. Burn the ISO image to a DVD disk.

Prepare a Bootable USB Memory Device

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

To prepare the image on a USB memory device under Linux:

1. Download the CounterACT ISO 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, `sd`, `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 prepare the image on a USB memory device under Windows:

1. Download the image from the ForeScout website to a Windows machine.
2. Use a boot image utility to create a bootable USB memory device with the CounterACT installation image.

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

To change the BIOS boot 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 install the software. These procedures are detailed in [Configuring an Appliance](#). You can maintain previous values, which appear as the defaults, or define new values.

Remember to reset the BIOS boot settings after you complete the installation.

Reimage the CounterACT Device

To reimage the CounterACT device:

1. Insert the DVD with the ISO image or connect the USB memory device to the CounterACT device and restart the device.
2. Proceed with the CounterACT installation.

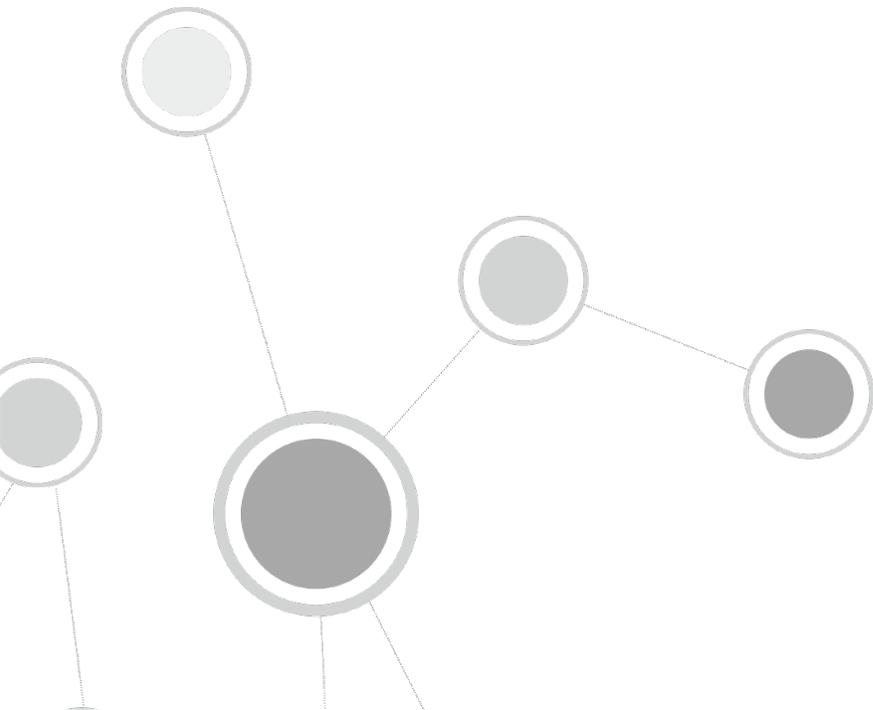
Chapter 7: Installing the CounterACT Console

[About the CounterACT Console Installation](#)

[Logging In](#)

[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 ForeScout Portals](#)
- [Install from a Browser on Your Appliance](#)

It is recommended to [Install from ForeScout Portals](#) 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.

Information Required by Wizard	Value
NTP server address used by your organization (optional)	
Internal mail relay IP address to allow delivery of email alerts if SMTP traffic is not allowed from the Appliance (optional)	
CounterACT administrator email address	
Monitor and response interfaces	
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	
IP address range that this Appliance will monitor (all the internal addresses, including unused addresses)	
LDAP user account information and the LDAP server IP address	
Domain credentials, including the domain administrative account name and password	
Authentication servers, so that CounterACT can analyze which network hosts have successfully been authenticated	
Switch IP Address, Vendor and SNMP Parameters	

Install from ForeScout Portals

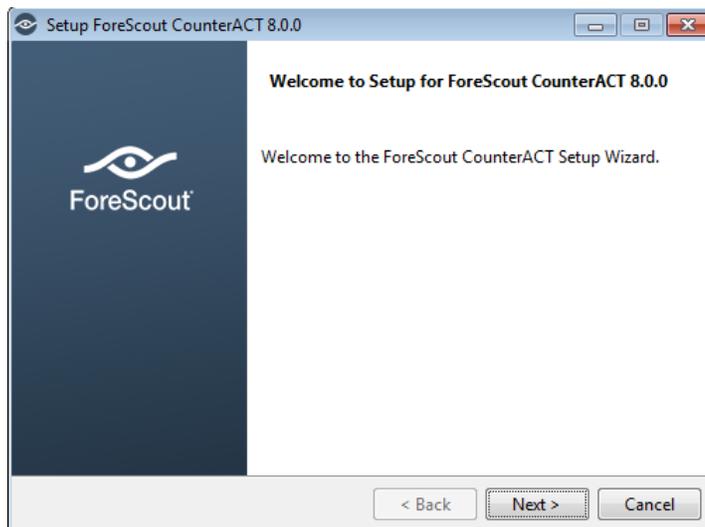
To install from a ForeScout Portal:

1. Navigate to one of the following ForeScout portals, depending on which licensing mode your deployment is using, and download the *CounterACT Console Setup* file:
 - [Product Updates Portal](#) - **Per-Appliance Licensing Mode**
 - [Customer Portal](#), Downloads Page - **Centralized Licensing Mode**See [Licensing Mode](#) for more information on licensing modes and to find out which mode you are using.
2. Select the *CounterACT Console Setup* file. The CounterACT Console software download screen opens.

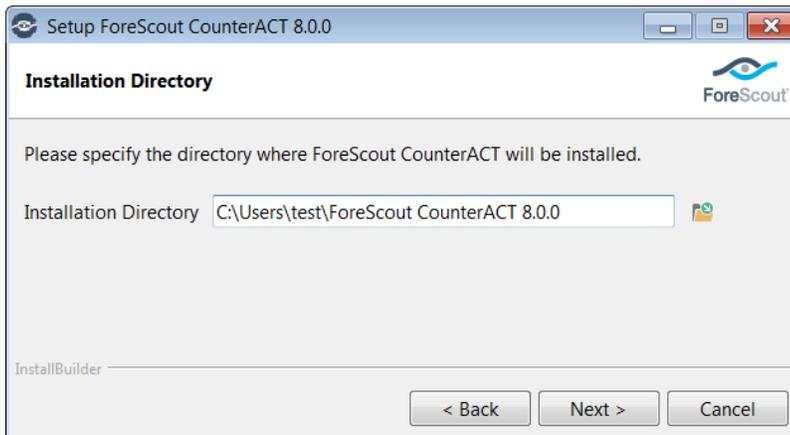


CounterACT Console Software Download Screen

3. Select the download link required and save the EXE file.
4. Select and run the file to begin the installation. The Setup Wizard opens.

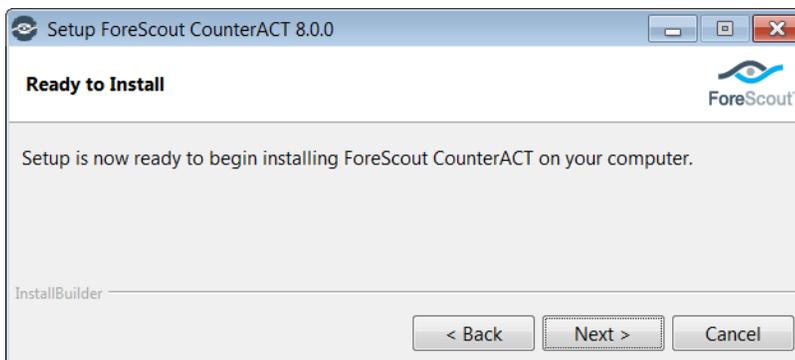


5. Select **Next**. The Installation Directory screen opens.



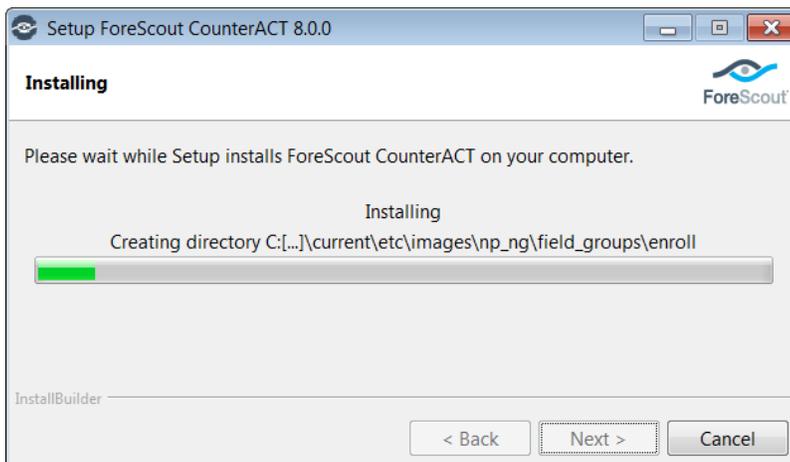
Installation Directory Screen

6. Accept the default location or define a new location to install the Console and then select **Next**. The Ready to Install screen opens.



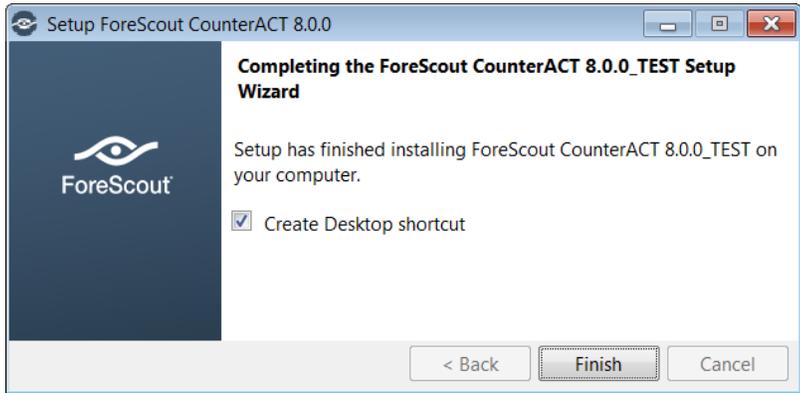
Ready to Install Screen

7. Select **Next**. The Installing screen opens and the Console installation begins.



Installing Screen

8. After installation is complete, the Completing the ForeScout CounterACT Setup Wizard screen opens.



Completing the ForeScout CounterACT Setup Wizard Screen

9. Select **Finish**.

Install from a Browser on 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 Console computer.
2. Type the following into the browser address line:

`http://<Appliance_ip>/install`

Where Appliance_ip is the IP address of this Appliance. The browser displays the Console 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.



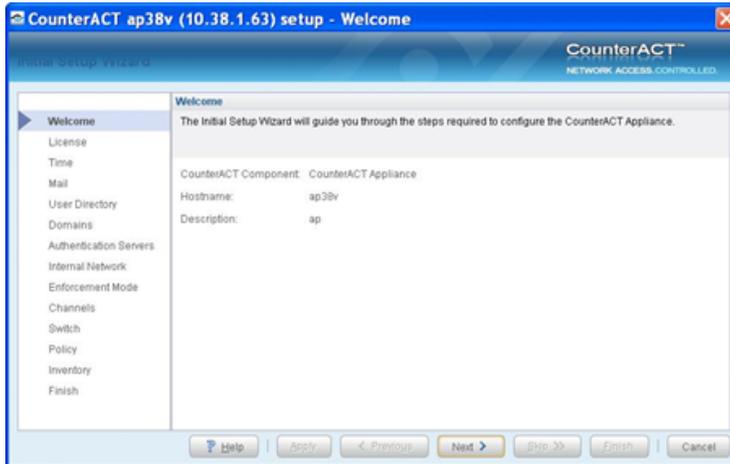
CounterACT Login Dialog Box

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 Administration Guide* for more information about login methods. See [Additional CounterACT Documentation](#) for information on how to access the guide.
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 Administration Guide* for more information about this utility. See [Additional CounterACT Documentation](#) for information on how to access the guide.

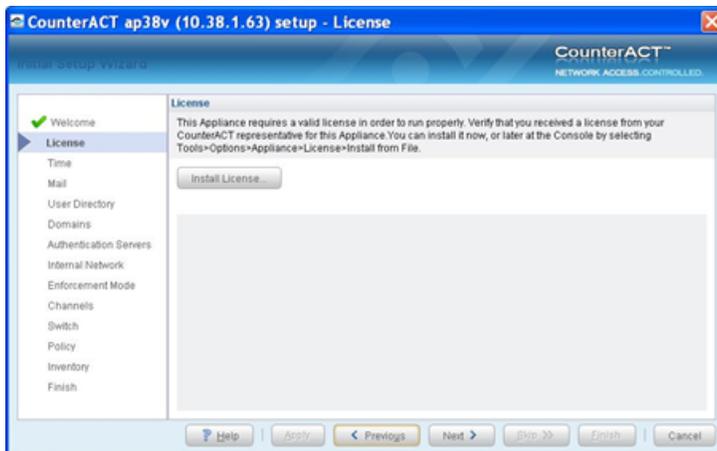
Running the Initial Setup Wizard on the Console

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.



Initial Setup Wizard

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



License Installation from Initial Setup Wizard – Virtual System

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 8: CounterACT Virtual Systems

About CounterACT Virtual Systems

What to Do

Virtual System Requirements

Virtual Environment Setup - Define Real NICs

VMware Virtual Systems

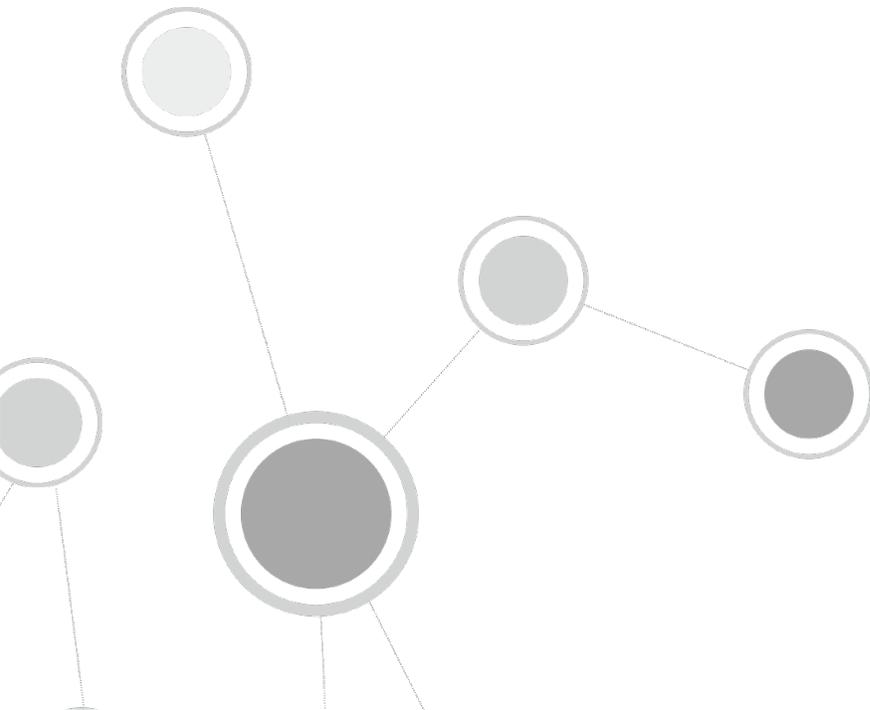
Hyper-V Virtual Systems

KVM 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.

If you are operating in Centralized Licensing Mode, all licensing-related procedures for virtual systems are identical to those for physical systems. Refer to the chapter on license management in the *CounterACT Administration Guide* for more information. If you are operating in Per-Appliance Licensing Mode, see [Install a Virtual License \(Per-Appliance Licensing Mode Only\)](#) 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 Administration Guide* or the Console Online Help for details. See [Additional CounterACT Documentation](#) for information on how to access the guide.

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](#) and [Perform the Initial Console Setup](#).

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

Refer to the [ForeScout Licensing and Sizing Guide](#) for information on virtual hardware minimum requirements.

Network Connection Requirements for CounterACT Virtual Devices

- 📄 *This requirement is only relevant if your deployment is operating in Per-Appliance Licensing Mode.*

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.

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

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 v6.5
- VMware ESXi v6.0
- VMware ESXi v5.5
- VMware ESXi v5.1

The guest OS is defined as *Other Linux-2.6 64bit 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.

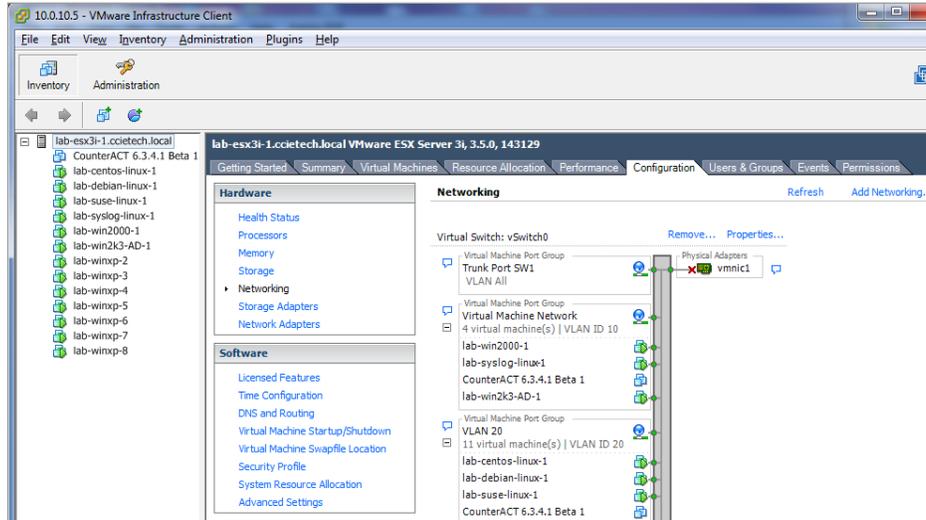
- 📄 *There are other ways to deploy a CounterACT virtual device: this document describes one alternative. (For example, you do not need a virtual switch for each port as vSwitches are generally trunk ports. The management interface and the response interface could be on one virtual switch with two logical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



Hardware Networking Option

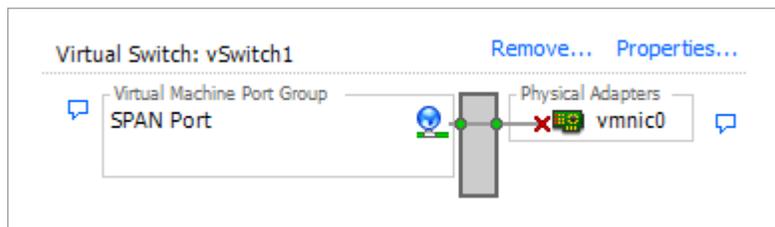
6. To create a virtual switch, select the **Add Networking** link.
The Connection Type page of the Add Network Wizard opens.
7. Select **Virtual Machine** and then select **Next**.
The Network Access page of the Add Network Wizard opens.
8. Select **Create a virtual switch**, select the available **vmnic**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

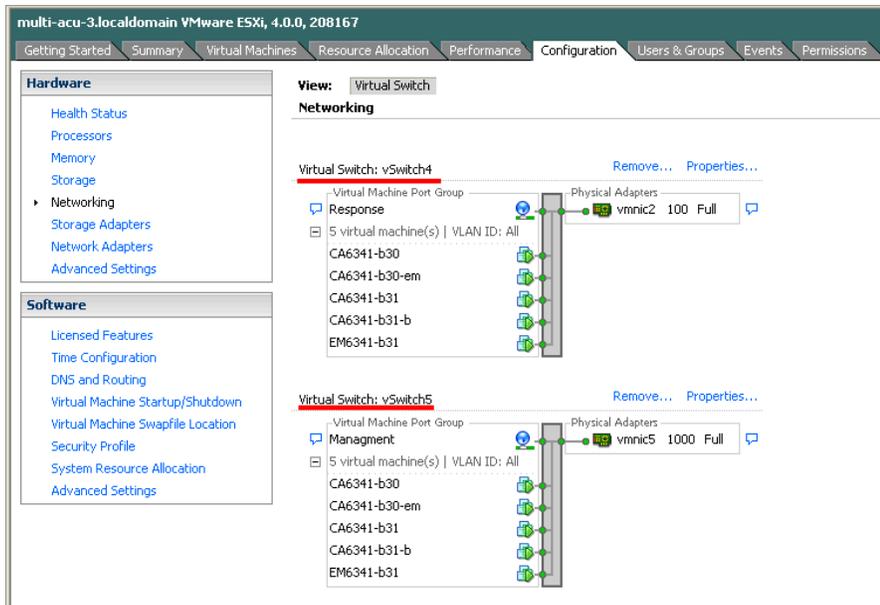
The wizard closes and returns to the Configuration tab of the Inventory window. The new switch is added in the window.



New Virtual Switch

Configuring Virtual Switches

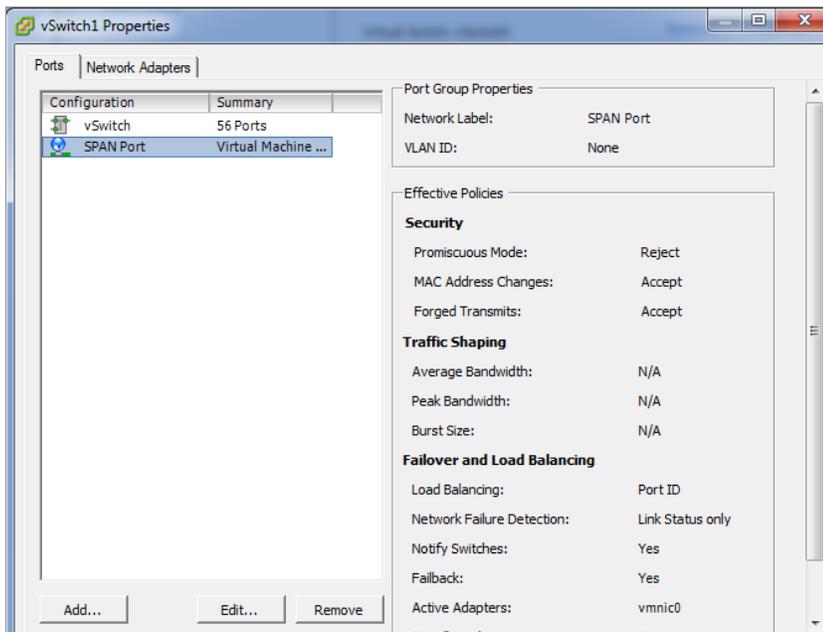
After creating virtual switches for the monitor, management and response interfaces, you must configure them:



Virtual Switches

To configure a virtual switch:

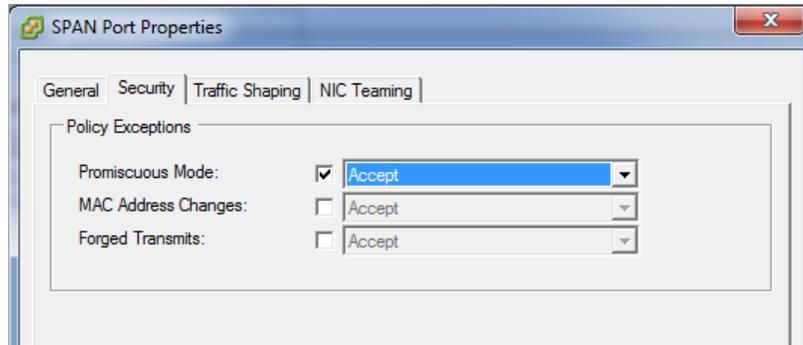
1. Select the **Properties** link for the virtual switch.



Switch Properties – Ports Tab

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

- 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 either:

- A unique license to each CounterACT device (Per-Appliance Licensing Mode).
- A single license to the Enterprise Manager or Standalone Appliance (Centralized Licensing Mode).

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.*

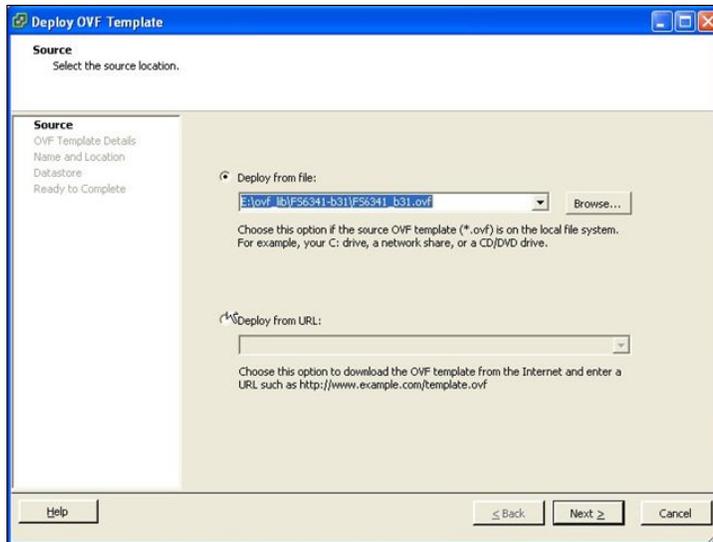
Deploy CounterACT Virtual Devices

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

To deploy a CounterACT virtual device:

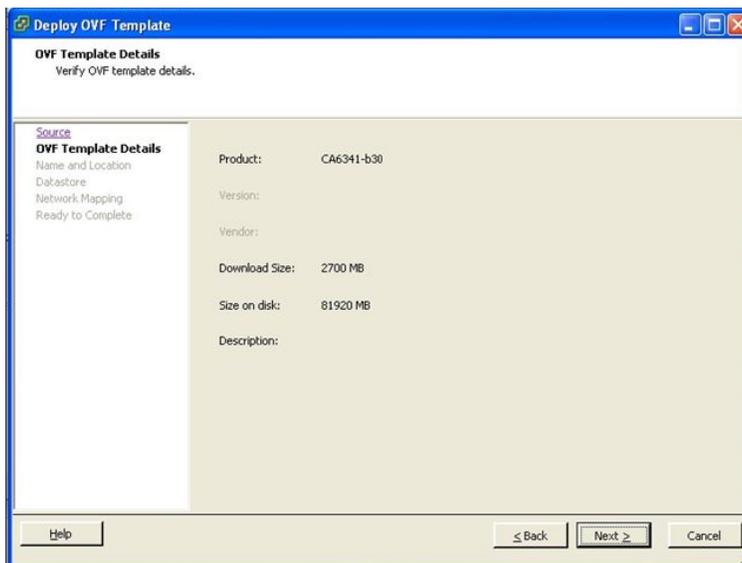
1. Access the vSphere Console.
2. Select **File>Deploy from file (OVF template)**.

The Deploy OVF Template wizard opens at the Source page.



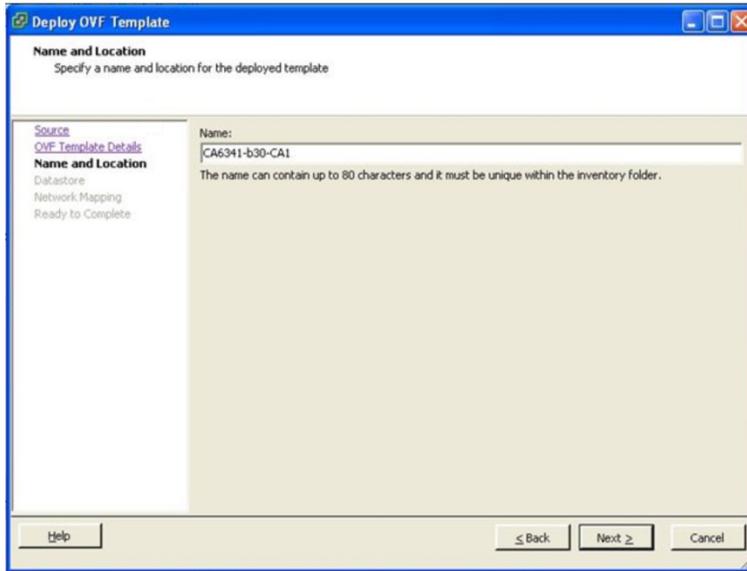
Deploy OVF Template Wizard – Source Page

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.



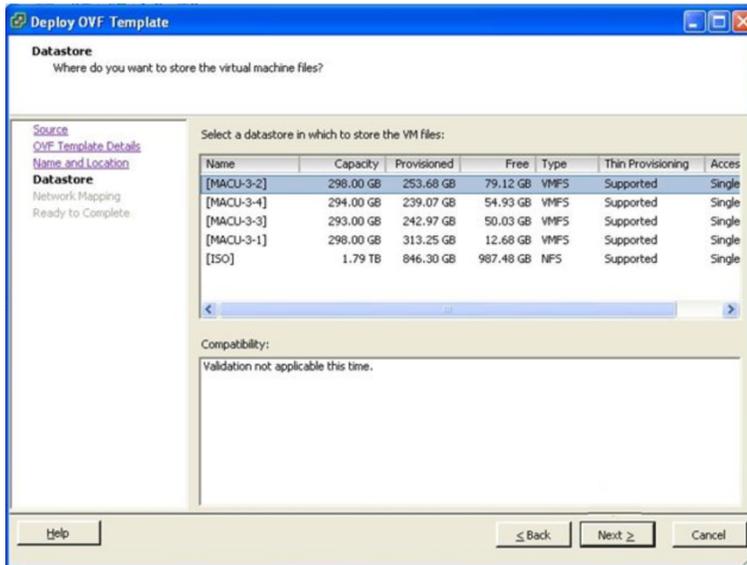
Deploy OVF Template Wizard – OVF Template Details Page

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



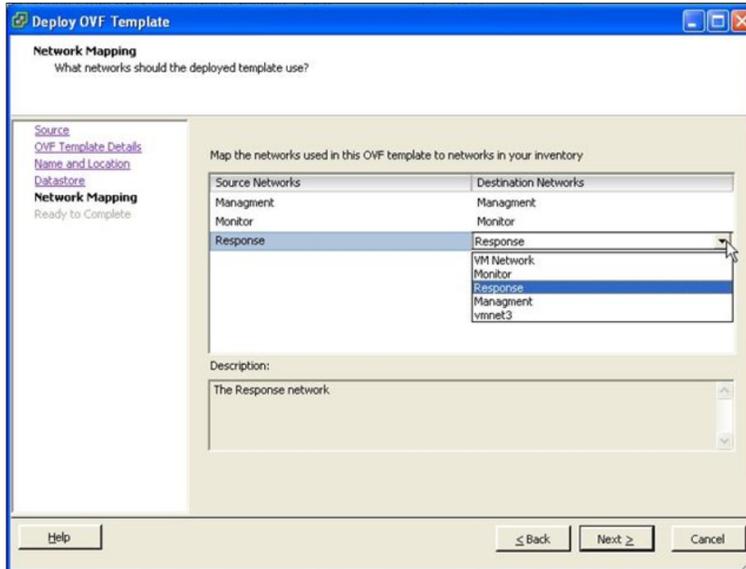
Deploy OVF Template Wizard – Name and Location Page

5. Specify a name and then select **Next**. The Datastore page opens.



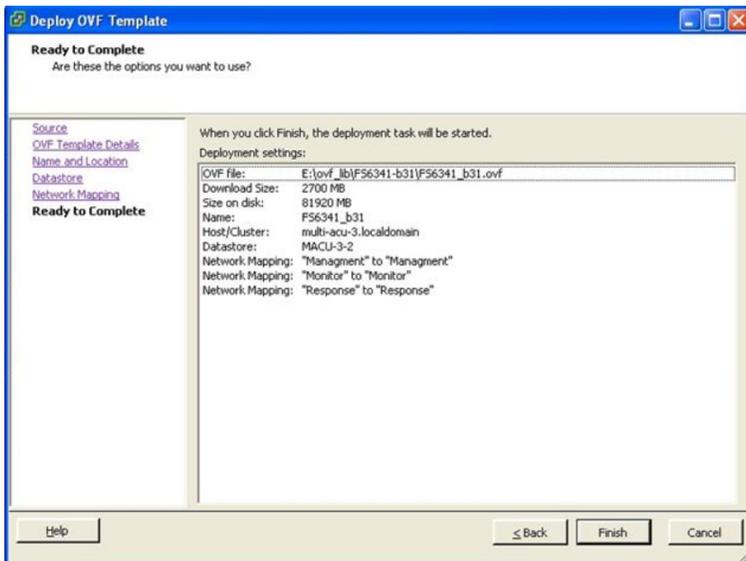
Deploy OVF Template Wizard – Datastore Page

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

- Map the physical and virtual interfaces and then select **Next**. The Ready to Complete page opens.



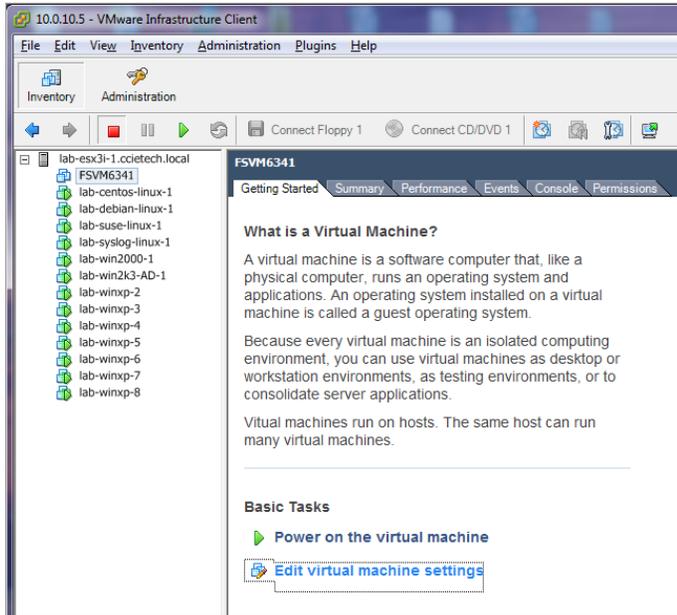
Deploy OVF Template Wizard – Ready to Complete Page

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

Post-Deployment Verification and VMware Configuration

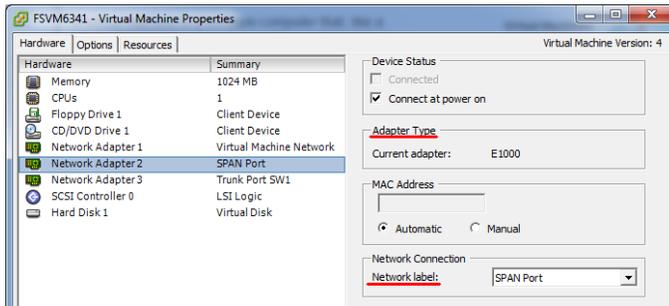
You should verify virtual host properties after deployment.

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



Machine Selection

2. Select **Edit virtual machine settings**. The **Virtual Machine Properties** dialog box opens.



Virtual Machine Properties Dialog Box

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.

VM Interface	CounterACT Interface
Network Adapter 1	eth0 (Management)
Network Adapter 2	eth1 (Monitor)
Network Adapter 3	eth2 (Response)

- 📄 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 2016
- Hyper-V Server 2012
- Hyper-V Server 2012 R2

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

Hyper-V Requirements

- CounterACT 8.0
 - 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.
- Configure the Enterprise Manager/Standalone Appliance (and any High Availability pair or Recovery Enterprise Manager connected to the Enterprise Manager/Standalone Appliance) Management interface to use Static MAC Address connectivity.
- 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.*

Refer to the section about working with channel assignments in the *CounterACT Administration Guide*. See [Additional CounterACT Documentation](#) for information on how to access the guide.

- 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.

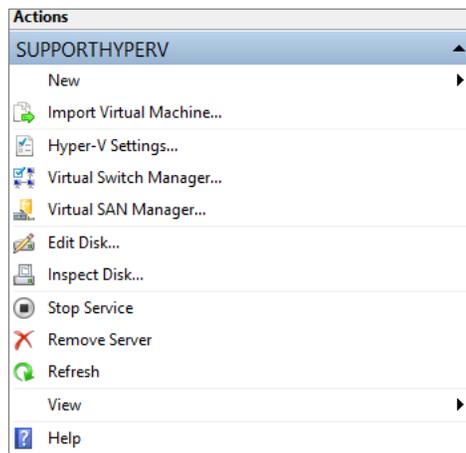
- [Configuring Virtual Switches](#)
- [Create a Hyper-V Virtual Machine](#)
- [Modify Virtual Processor Settings](#)
- [Configuring Network Adapters](#)

Configuring Virtual Switches

Create and configure two virtual switches, parallel to the Management and Monitor interfaces.

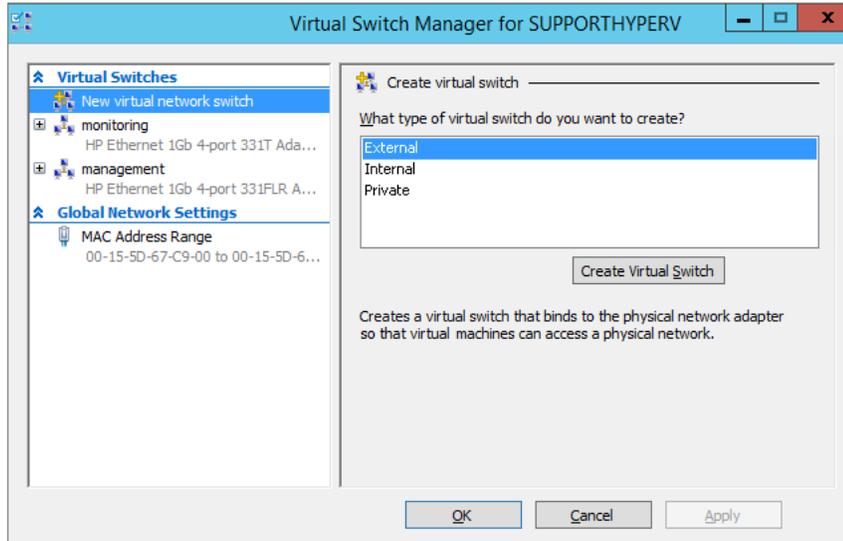
To create virtual switches:

1. Select **Virtual Switch Manager** from the Hyper-V Manager Actions pane.



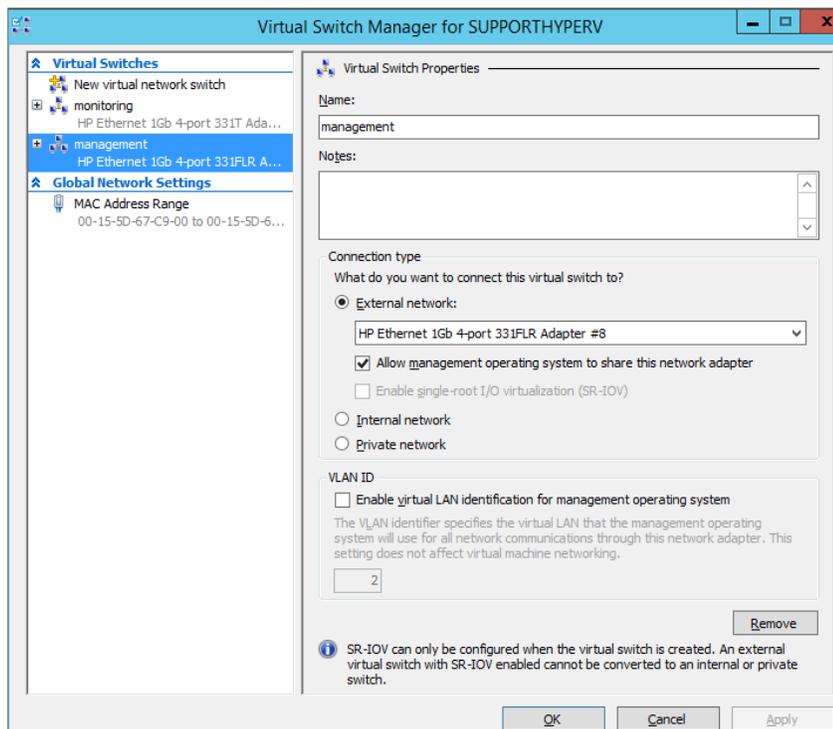
Hyper-V Manager - Actions

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



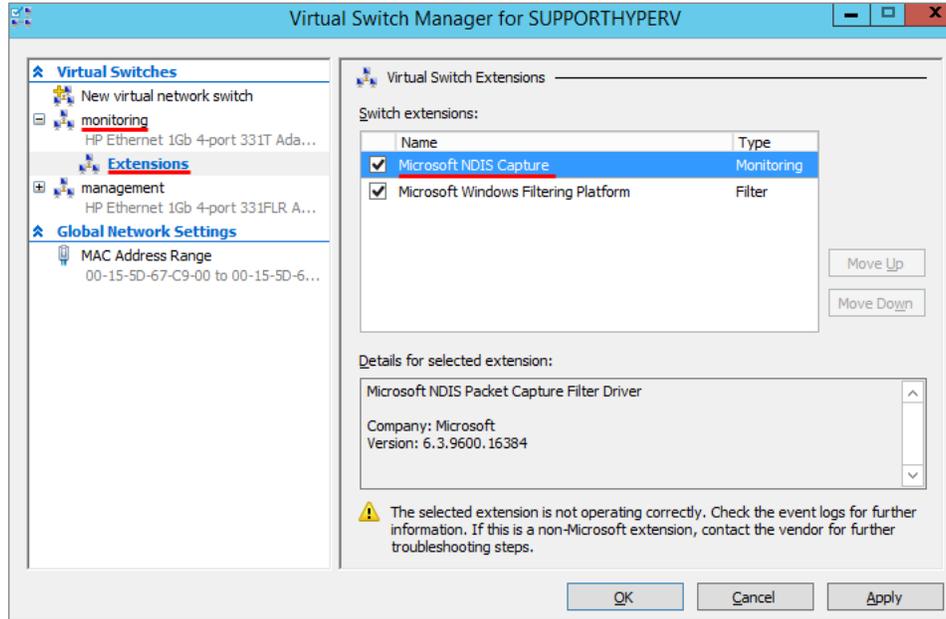
Virtual Switch Manager – New Switch

3. Select **Create Virtual Switch**.
4. Name the switch and configure any relevant settings in the Virtual Switch Manager window.



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**.



Virtual Switch Manager – Extensions

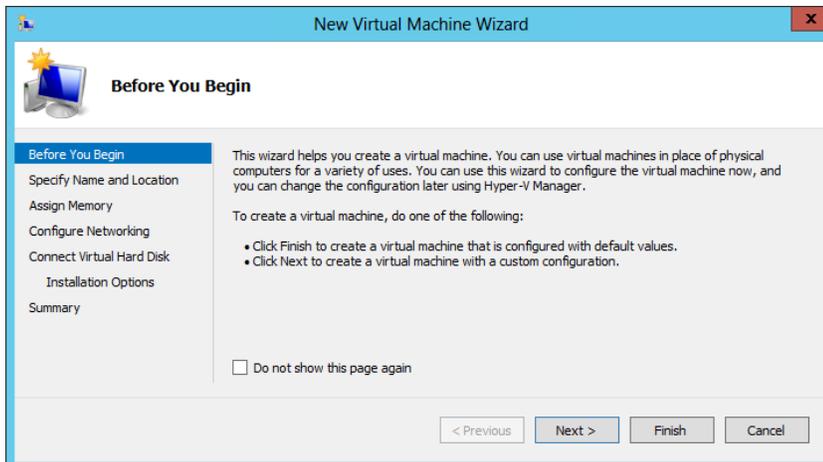
7. Select **OK**.

Create a Hyper-V Virtual Machine

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

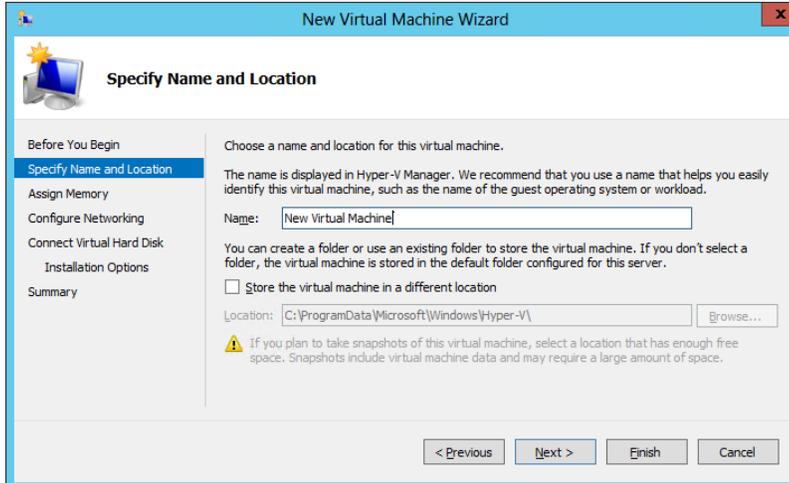
To create a Hyper-V Virtual Machine:

1. Select **New > Virtual Machine** from the Hyper-V Manager Actions pane, and then select **Next**.



New Virtual Machine – Before You Begin

2. Choose a name and location for the virtual machine and select **Next**.



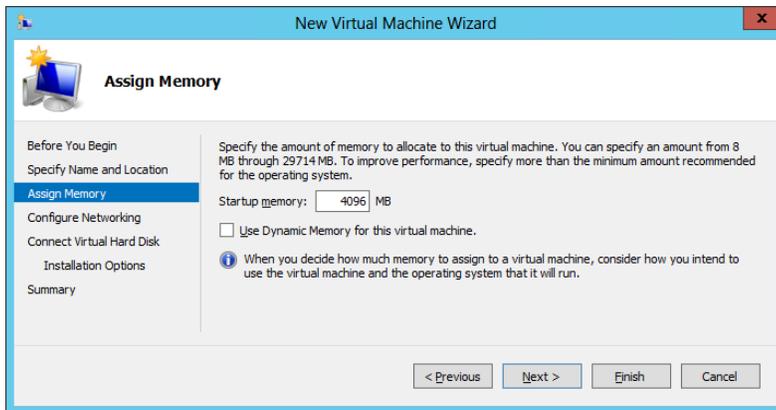
New Virtual Machine – Specify Name and Location

3. Select **Generation 1** and select **Next**.

 *This step is only relevant for Hyper-V Server 2012 R2.*

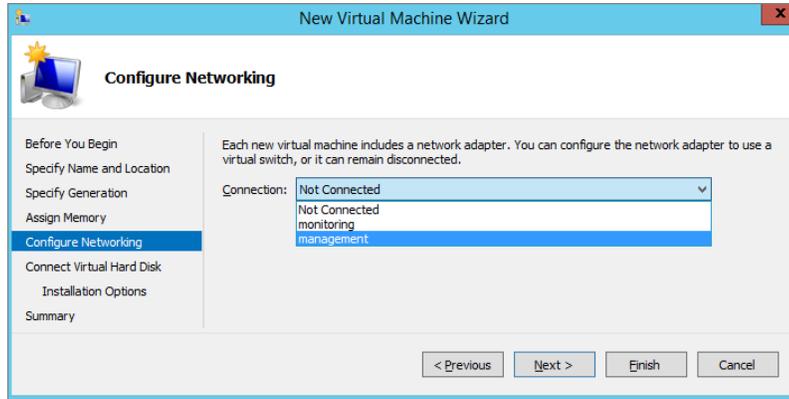


4. Specify the amount of memory to allocate to the virtual machine and select **Next**. See [Hardware Minimum Requirements](#) for more information.



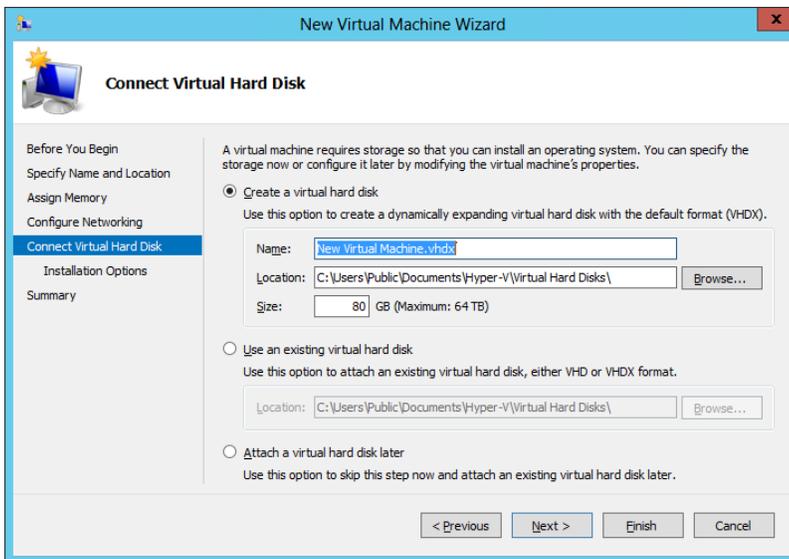
New Virtual Machine – Assign Memory

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.



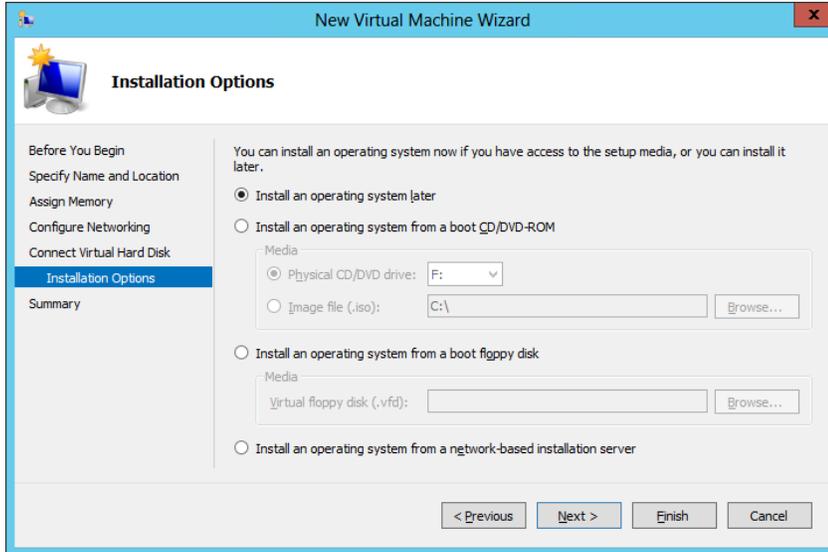
New Virtual Machine – Configure Networking

6. Create a virtual hard disk, specifying the name, location and size and select **Next**. See [Hardware Minimum Requirements](#) for more information.



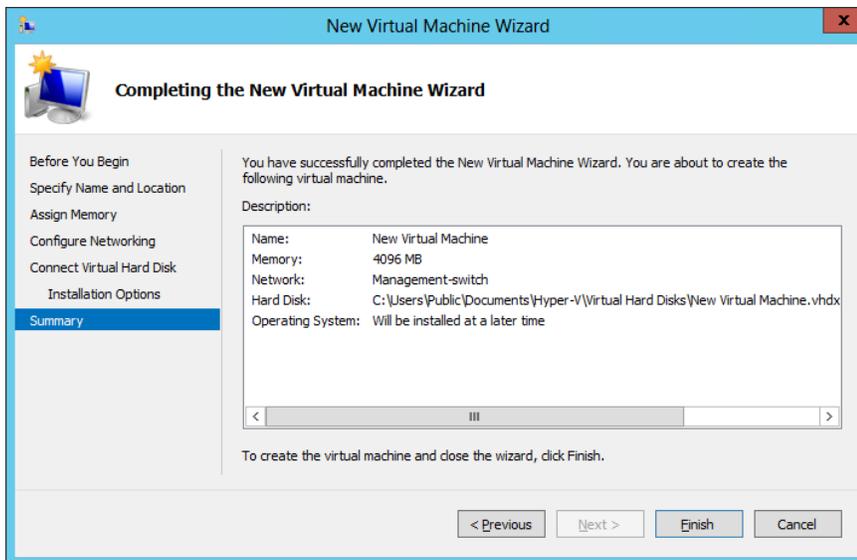
Connect Virtual Hard Disk

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

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



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.

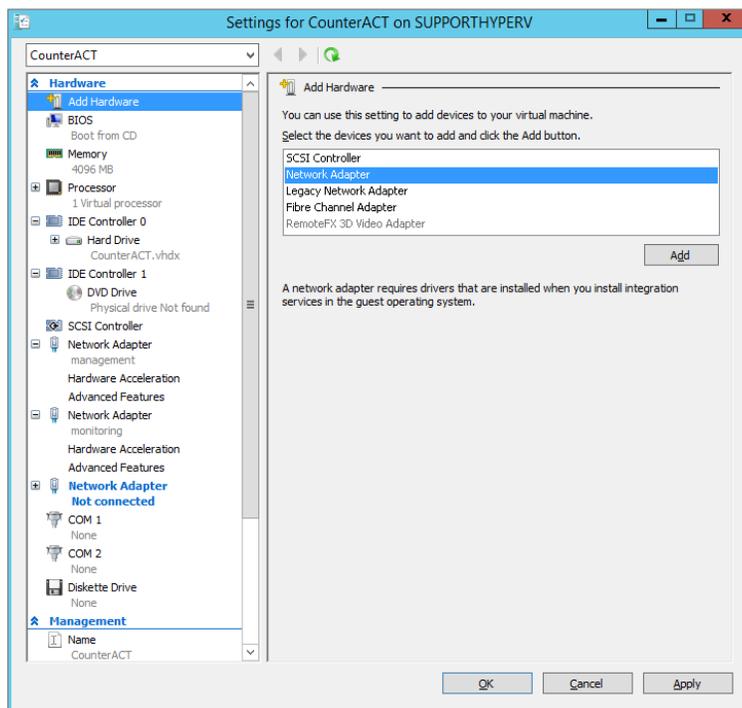
The following table shows the mapping between the interfaces.

VM Interface	CounterACT Interface
Network Adapter 1	eth0 (Management)
Network Adapter 2	eth1 (Monitor)

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:

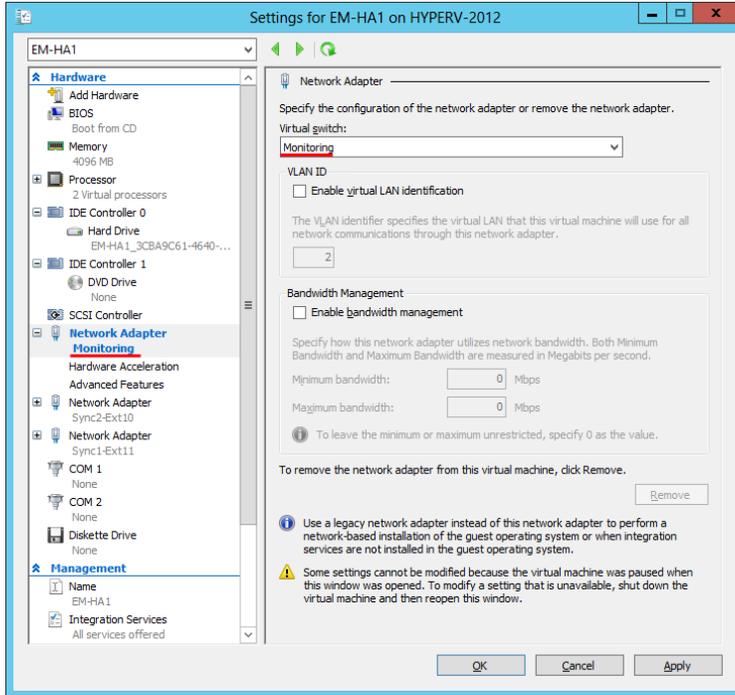
1. Select **Add Hardware** from the Virtual Machine Settings window.
2. Select **Network Adapter** and then select **Add**.



Virtual Machine Settings – Add Hardware

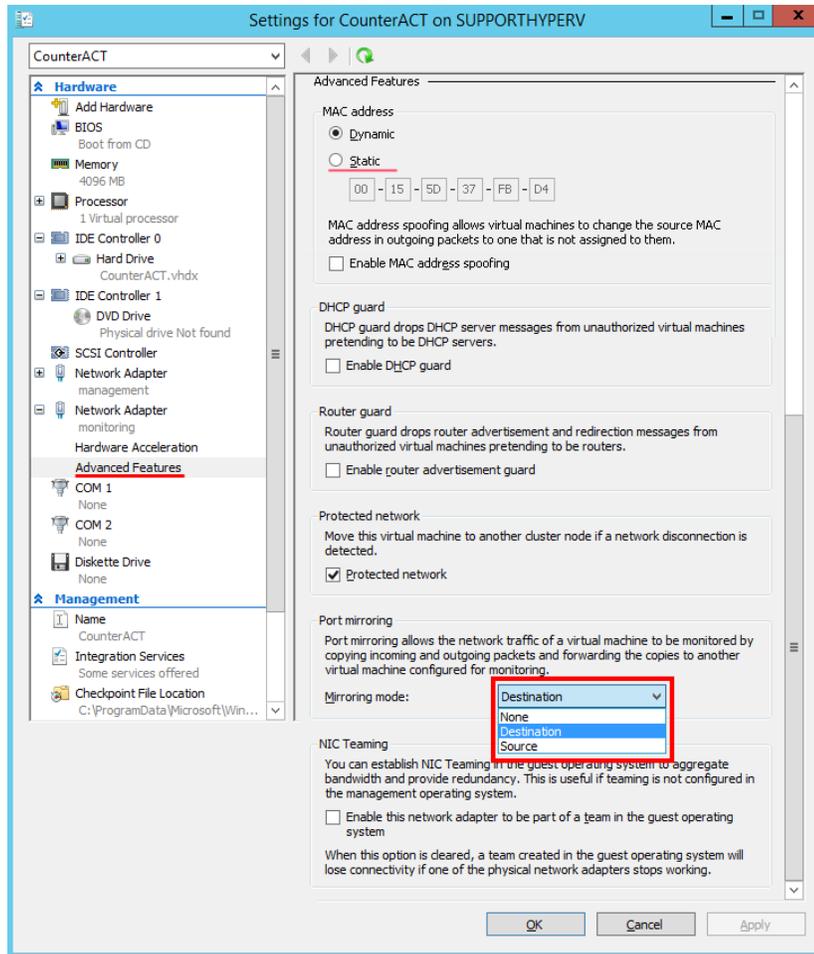
3. Select the newly created Network Adapter from the Virtual Machine Settings designated as the Monitor Interface.

*If you are using a single VLAN, you can select **Enable virtual LAN identification**.*



Virtual Machine Settings – Virtual Switch

4. Select **Advanced Features**, and configure the following:
 - Set the MAC address to **Static**.
 - 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**.*



Virtual Machine Settings – Advanced Features

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:

```
$a = Get-VMSystemSwitchExtensionPortFeature -FeatureId 776e0ba7-94a1-41c8-8f28-951f524251b5
```
 - b. After you receive a response, run the following PowerShell cmdlet to allow monitoring traffic:

```
$a.SettingData.MonitorMode = 2
```
 - c. Run the following PowerShell cmdlet:

```
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:

```
$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:

```
$a.SettingData.MonitorMode = 2
```
 - c. Run the following PowerShell cmdlet:

```
Set-VMSwitchExtensionPortFeature -ExternalPort -SwitchName <virtual_switch_name> -VMSwitchExtensionFeature $a
```

To disable vSwitch from operating in Promiscuous mode:

1. Run the following PowerShell cmdlet:

```
$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:

```
$a.SettingData.MonitorMode = 0
```

```
set-VMSwitchExtensionPortFeature -ExternalPort -SwitchName <virtual_switch_name> -VMSwitchExtensionFeature $a
```

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 Administration Guide* for more information. See [Additional CounterACT Documentation](#) for information on how to access the guide.

To configure VLAN filter settings:

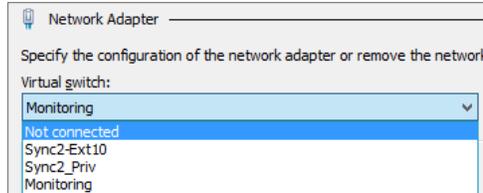
1. Run the following PowerShell cmdlet:

```
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:

```
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.

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:

```
fstool conf --template
```

This command prepares CounterACT and its virtual hard disk for template creation.

In a High Availability environment, run this command:

- 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 User Guide* for more information. See [Additional CounterACT Documentation](#) for information on how to access the guide.

 *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 RHEL/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.

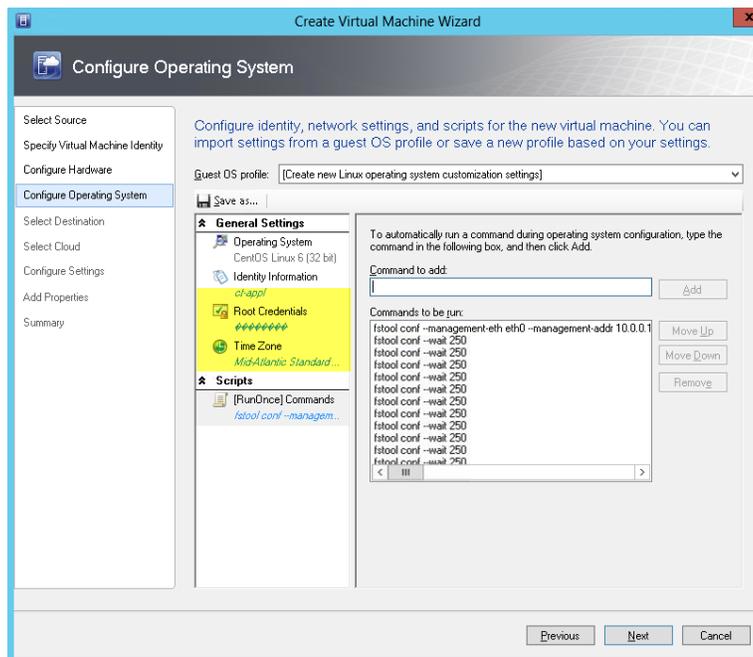
When a deployed High Availability Standby node machine is created, the Active node should be running to allow the Standby node to synchronize with it.

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 `fstool 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 `fstool conf --wait` command should be run at least 14 times to guarantee that the first command has enough time to be properly completed. See [FStool Samples for Automated Deployments](#) for details.



Configure Operating System – fstool 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.

- After deploying the template, connect the Appliance to the Enterprise Manager, verify/set Appliance configuration and install licenses on Appliances (Per-Appliance Licensing Mode) or on the Enterprise Manager/Standalone Appliance (Centralized Licensing Mode). The licensing installation workflow is identical to the standard procedure for virtual Appliances. See [Install a Virtual License](#) for details.

Setup Notes

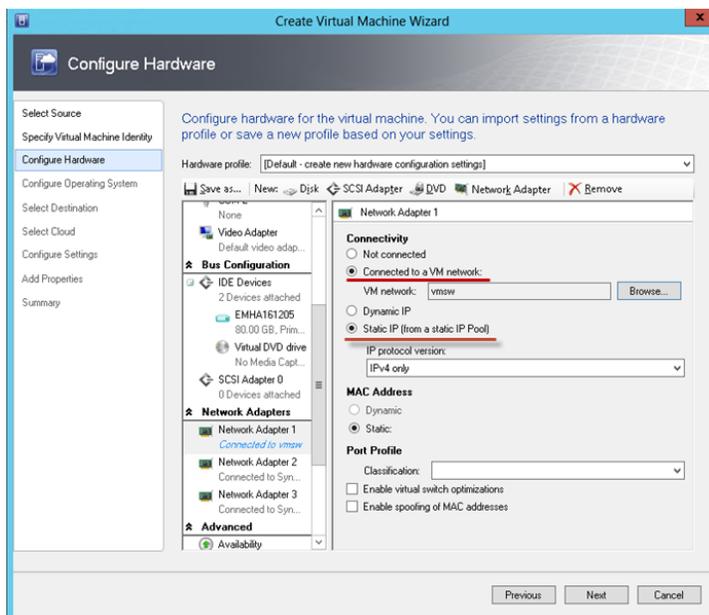
When creating/deploying the template:

- 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

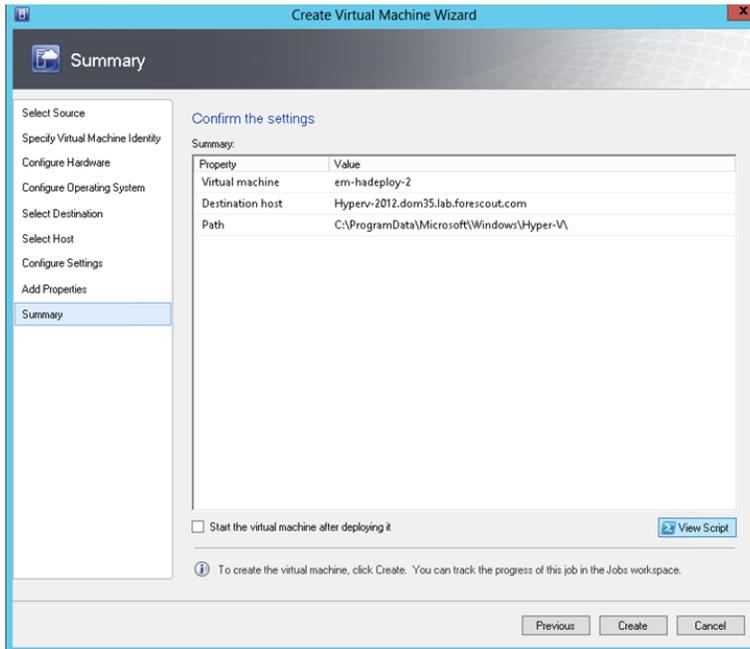
When configuring network adaptors in the Virtual Machine Wizard:

- 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.



Configuration Recommendations

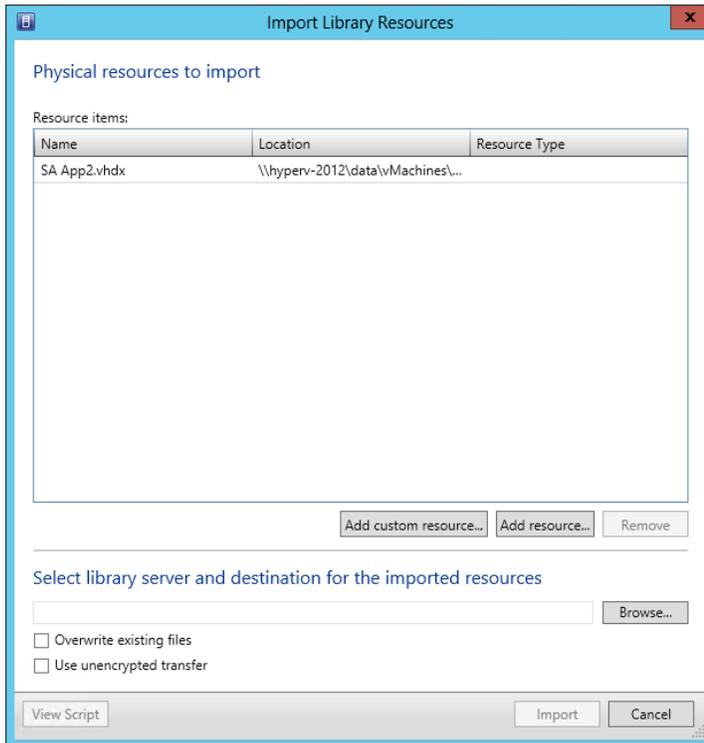
Save and Reuse the Original Script



Save and Reuse 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.



Add Virtual Hard Disk to Library

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)
```

<code>--domain</code>	<code>domain</code>	(optional)
<code>--dns</code>	<code>dns_server_address</code>	(optional)
<code>--ha-secondary-addr</code>	<code>secondary_private_address</code>	(optional)
<code>--ha-sync-subnet</code>	<code>sync_subnet</code>	(optional)
<code>--ha-sync-netmask</code>	<code>sync_netmask</code>	(optional)
<code>--ha-sync-eth-primary</code>	<code>sync_interface_primary</code>	(optional)
<code>--ha-sync-eth-secondary</code>	<code>sync_interface_secondary</code>	(optional)
<code>--ha-sync-subnet</code>	<code>sync_subnet</code>	(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)
```

KVM Virtual Systems

This section describes how to deploy CounterACT on KVM virtual systems.

- 📄 *Under certain circumstances, when CounterACT is deployed on KVM virtual systems, the CounterACT Packet Engine restarts every 2 hours, causing a range of traffic monitoring functionality to temporarily stop. Appliances which do not utilize SPAN/mirrored traffic are not affected.*

KVM Requirements

- Recommended - Linux RHEL/CentOS 7 operating system

Deploy CounterACT on a KVM virtual system

To deploy CounterACT on a KVM virtual system:

1. Obtain the CounterACT installation ISO image file and save it to a location accessible to the KVM virtual machine.
2. Log in to the KVM virtual machine.
3. Edit the interface configuration file `/etc/sysconfig/network-scripts/ifcfg-
<bridge interface name>`, and set the Bridging options property as follows:
`BRIDGING_OPTS="ageing_time=0"`
4. Save the file.
5. In the **Virtual Machine Manager**, select **File > New Virtual Machine**. The new VM dialog opens.
6. Select **Local install media (ISO image or CDROM)**, and select **Forward**.
7. Select **Use ISO image** and browse to the location of the saved CounterACT installation ISO image. Make sure that **Automatically detect operating system based on install media** is selected.
8. Select **Forward**.
9. Define the minimum required RAM memory and number of CPUs, and select **Forward**. See [Hardware Minimum Requirements](#) for recommended VM minimum requirements.
10. Select **Enable storage for this virtual machine**, and define the disk image size. See [Hardware Minimum Requirements](#) for recommended VM minimum requirements.
11. Select **Forward**.
12. Provide a name for the new VM and select **Finish**. The ForeScout Linux boot menu opens.



13. Select **Boot from local drive** and press **Enter**.
14. Continue with CounterACT installation and configuration described in [Configuring an Appliance](#) and [Configuring the Enterprise Manager](#).

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. See [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:

```
A reboot is required to renumber network interfaces.
Renumber? (yes/no) :
```

Verify Switch-Appliance Connectivity

Verify that the virtual switch is properly connected to the Appliance.

To verify connectivity:

1. Log in to the Console and navigate to **Options > Channels**.
2. 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.

 *If you are operating in Per-Appliance Licensing Mode, 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)

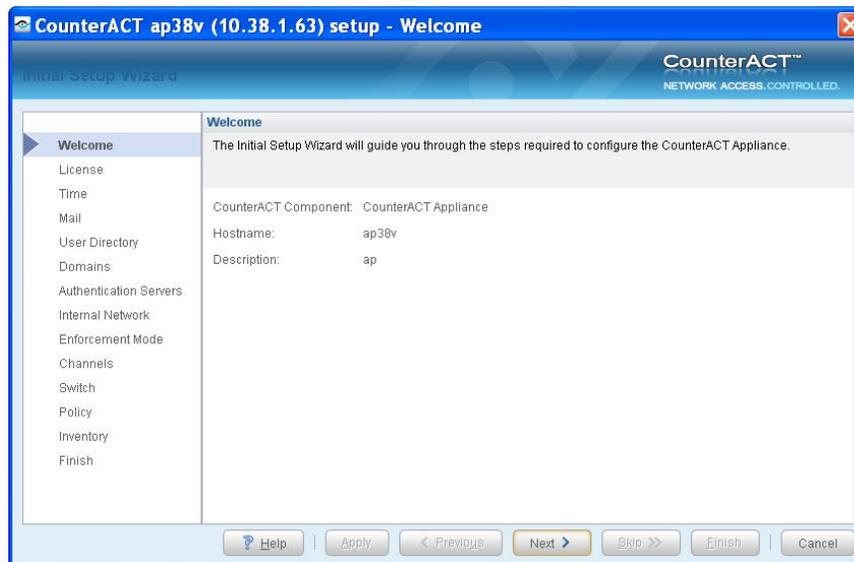
The browser displays the Console installation window.

3. Follow the on-screen instructions.

For more information, see [Chapter 7: Installing the CounterACT Console](#).

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

Refer to the *CounterACT Administration Guide* for information about working with the Wizard. See [Additional CounterACT Documentation](#) for information on how to access the guide.

Before You Begin

Before working with the Wizard:

- If you are operating in Per-Appliance Licensing Mode, 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](#).

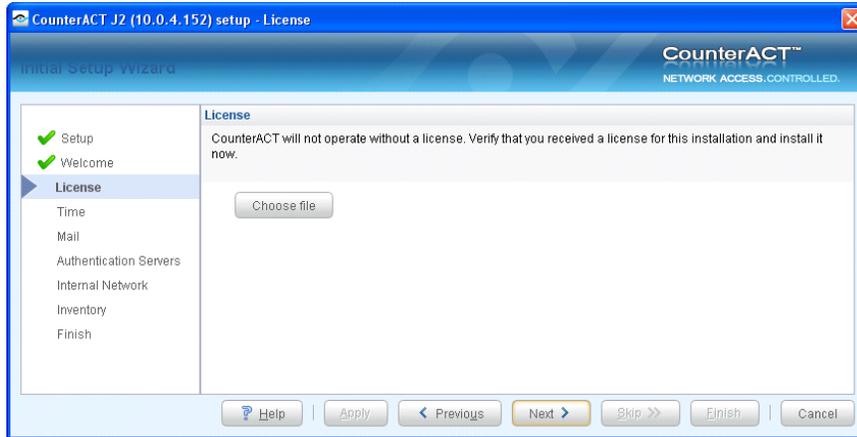
Installing a Demo License (Per-Appliance Licensing Mode Only)

In the License page, select a virtual demo license that you received from ForeScout. See [Install a Virtual License](#) for details.

- 📄 *If you are operating in Centralized Licensing Mode, license installation is performed later, after the Initial Setup Wizard is complete.*

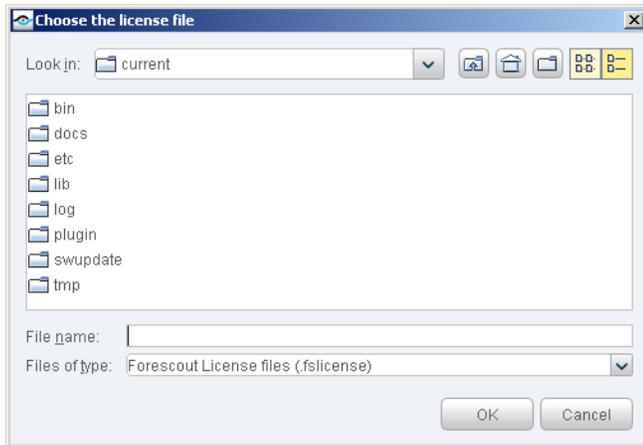
To install a demo license:

1. In the License page, select **Choose file**.



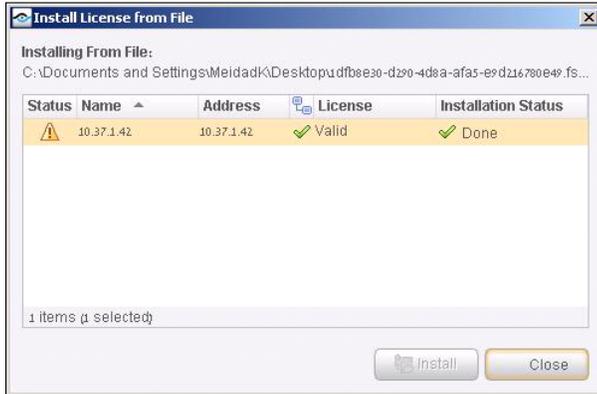
Initial Setup Wizard – License Page

2. The Choose the license file dialog box opens.



Choose the License File Dialog Box

3. 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 (Per-Appliance Licensing Mode Only)

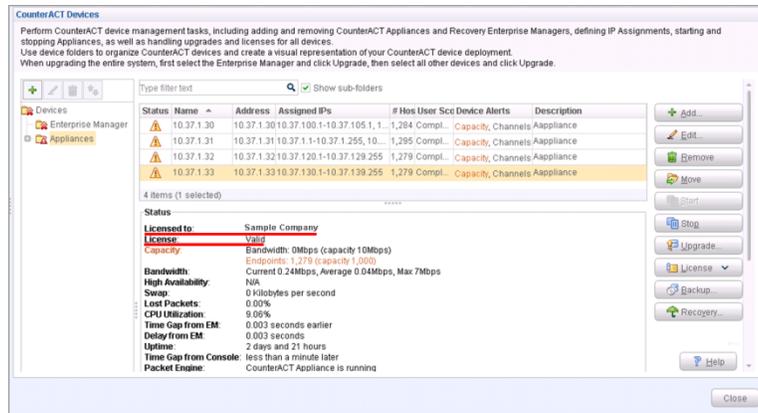
The license feature is designed to meet the needs of users working in Virtual IT environments, including environments that require a proxy server. This feature ensures that virtual users are working with authorized, secure and protected licenses.

ⓘ If are you operating in Centralized Licensing Mode, all licensing-related procedures for virtual systems are identical to those for physical systems. Refer to the chapter on license management in the CounterACT Administration Guide for more information.

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 the *CounterACT Administration Guide*. See [Additional CounterACT Documentation](#) for information on how to access the guide.

 *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 Administration Guide*. See [Additional CounterACT Documentation](#) for information on how to access the guide.

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

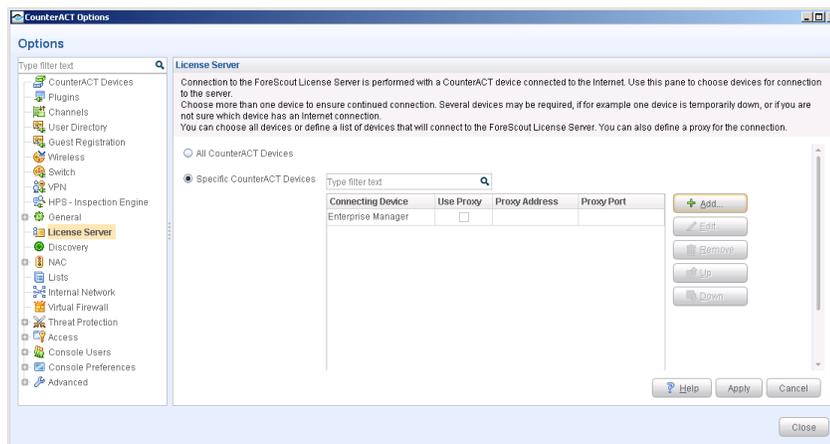
Connection to the ForeScout License server is performed via a CounterACT device connected to the Internet. By default, CounterACT assumes that all devices are connected.

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:

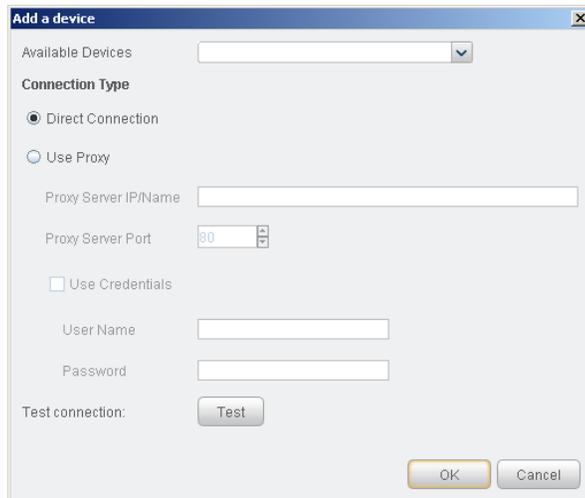
1. Select the **Options** icon from the Console toolbar and then select **License Server**.



License Server Options

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

The Add a device dialog box opens.



Add a Device Dialog Box

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

If you are using **Per-Appliance Licensing Mode**, 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.

If you are using **Centralized Licensing Mode**, you can freely duplicate virtual Appliances, but any new endpoints on the duplicate Appliances will count against the license capacity. If you duplicate a virtual Enterprise Manager, the license on the new device will be invalid. You must install a unique license on the new Enterprise Manager.

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.

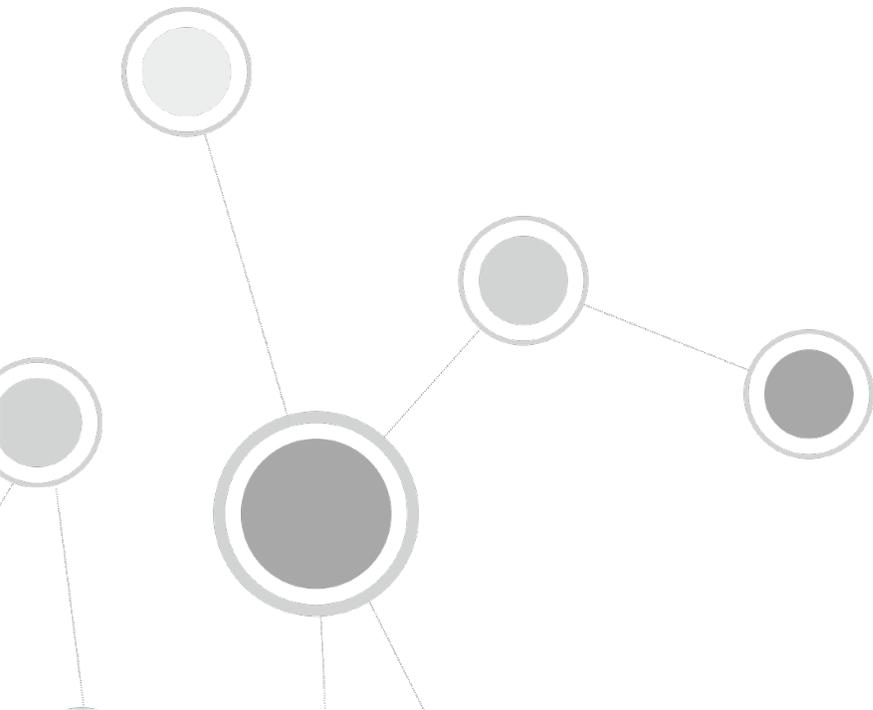
Moving Virtual Devices

You can 'move' a CounterACT virtual device to a new virtual server 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.

Subject	Item	Value
Communication Information	CounterACT IP address	
	Subnet mask	
	Default gateway	
	Mail-relay server address	
	DNS server host name and address	
	Email addresses used for sending alerts regarding worm attack attempts	
	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)	

Subject	Item	Value
Internal Network	Address ranges of protected network (It is recommended to use your enterprise's entire internal IP address range)	

Subject	Item	Value
Management	Operating system on PC running CounterACT Console or CounterACT Enterprise Manager	
	Allowed addresses for CounterACT Console or CounterACT Enterprise Manager connectivity	
	Addresses of hosts allowed to control CounterACT through SSH	

Subject	Item	Possible Values
Communication Equipment	Communication equipment to which the CounterACT is connected	Switch with mirroring port – supports traffic response
		Switch with mirroring port – does not support traffic response Vendor and model:
Logistics	Available space: How near/far is rack/shelf space from a network connection and power connection (specify cable requirements)	19" Rack
		Shelf space Available space
	Socket and cable availability	Standard power socket + cable Network socket + cable

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

Subject	Item	Value
Contact Details	Name	
	Phone number	
	Email address	

Legal Notice

© 2018 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.

2018-05-07 11:51