



Fore Scout

Fore Scout Installation Guide v8.3



Contact Information

Forescout Technologies, Inc.

190 West Tasman Drive

San Jose, CA 95134 USA

<https://www.forescout.com/support-hub/>

Toll-Free (US): 1.866.377.8771

Tel (Intl): 1.408.213.3191

Support: 1.708.237.6591

About the Documentation

- Refer to the Documentation Portal for additional technical documentation: <https://docs.forescout.com/>
- Have feedback or questions? Write to us at documentation@forescout.com

Legal Notice

© 2022 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.

Last Updated: 4 February 2022

PDF Created: 14 June 2022

Part Number: \${part-number}

Table of Contents

Installation Overview.	5
System Components and Requirements.	7
Forescout Components.	7
System Requirements.	9
Security and Compliance and RMM.	15
Network Setup.	18
About the Forescout Installation.	18
Appliance Interface Connections.	18
Set up Switch Connections.	21
Creating an Out-of-Band IP Management Interface.	24
Appliance Setup and Configuration and Post-Installation.	26
Set up an Appliance.	26
Configure an Appliance.	27
Appliance Post-Installation Procedures.	32
Additional Installation Tools.	40
EM Setup and Configuration and Post-Installation.	43
Set up the Enterprise Manager.	43
Configure the Enterprise Manager.	43
Enterprise Manager Post-Installation Procedures.	48
Restore Enterprise Manager System Settings.	48
Re-image Forescout Devices.	51
Install and Log in to the Forescout Console.	57
Forescout Virtual Systems.	64
About Forescout Virtual Systems.	64
How to Work With Virtual Devices.	64
Virtual System Requirements.	65
Virtual Environment Setup - Define Real NICs.	65
VMware Virtual Systems.	66
VMware Requirements and Support.	66
Create and Configure Virtual Switches.	66
Forescout Virtual Device Deployment in VMware.	67
Post-Deployment Verification and VMware Configuration.	68
Hyper-V Virtual Systems.	68
Hyper-V Requirements and Support.	69
Deploy Forescout Virtual Devices in Hyper-V.	69
Configure Hyper-V to Work with Forescout Devices.	77

Automate Forescout Deployment in Hyper-V Environments.	79
KVM Virtual Systems.	85
Configure a Forescout Virtual Device.	86
Duplicate a Virtual Device.	92
Move a Virtual Device to a New Server.	93
Forescout Platform Cloud Deployments.	94
Forescout Platform Cloud Strategies and Best Practices.	94
Install Forescout Platform in the AWS Cloud.	101
Install Forescout Platform in the Microsoft Azure Cloud.	104
Appendix A - Site Preparation Form.	109
Appendix B - Limited Appliance Mode.	111
Appendix C - Inter-Enterprise Manager and Appliance Authentication.	114
Create a Certificate Sign Request.	114
Import a Signed Certificate.	114
Configure Certificate Verification Enforcement.	114

Installation Overview

This topic provides an overview of the Forescout platform installation.

About the Forescout Platform

The Forescout platform provides infrastructure and device visibility, policy management, orchestration and workflow streamlining to enhance network security. The platform provides enterprises with real-time contextual information of devices and users on the network. Policies are defined using this contextual information that helps ensure compliance, remediation, appropriate network access and streamlining of service operations.

Refer to the [Forescout Administration Guide](#) for more information about these capabilities.

About This Guide

This guide details the Forescout 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
- Forescout Console management application

Information about setting up switch connections is also included.

The **Forescout Upgrade Guide** covers the Forescout software upgrade procedures. Refer to [About Forescout Platform Upgrades to the Latest Version](#).

This Installation Guide contains the following sections:

System Components and Requirements	Forescout system requirements, including hardware and networking requirements
Security and Compliance and RMM	
Network Setup	Information about hardware setup options
Appliance Setup and Configuration and Post-Installation	How to install and upgrade Forescout Appliances
EM Setup and Configuration and Post-Installation	How to install and upgrade the Forescout Enterprise Manager
Re-image Forescout Devices	How to reinstall Forescout on a device using a prepared DVD or USB memory device.
Install and Log in to the Forescout Console	How to install the Forescout Console
Forescout Virtual Systems	How to install and configure Forescout virtual systems
Forescout Platform Cloud Deployments	How to install and configure Forescout on the AWS and Microsoft Azure cloud platforms
Appendix A - Site Preparation Form	A Forescout site preparation form with required site parameters
Appendix B - Limited Appliance Mode	Limited Appliance mode for the 5110 and CT-R series Appliances (runs a subset of Forescout plugins)

[Appendix C - Inter-Enterprise Manager and Appliance Authentication](#)

How to generate certificate sign requests to a CA Service, and import the signed certificate and its certificate chains, for Enterprise Manager and Appliance

Forescout Package Contents

For the list of components that are supplied with each Forescout Appliance, refer to the **Getting Started** document that is packaged with each Appliance. A **Getting Started** document is available for the following Appliances:

- CT-xxxx Appliances based on hardware revision 5x
- Forescout 51xx Appliances
- Forescout 41xx Appliances

See [Forescout Components](#) for an overview of each component.

If you are working with a High Availability system, you should receive a separate package with another Appliance or Enterprise Manager. Refer to [High Availability Pairing](#) in the **Resiliency Solutions User Guide** for more information about this solution.

Virtual Devices

If you are installing Forescout virtual devices, you should receive:

- A link to a Forescout virtual package image
- One of the following, depending on the [Licensing Mode](#) of your deployment:
 - **Flexx Licensing Mode.** An email from Forescout with purchase entitlement details, including your Deployment ID and links to the Forescout Customer Support 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 **Forescout Quick Installation Guide** and the complete **Forescout Installation Guide**.

See [Licensing Mode](#) for more information on licensing modes and to find out which mode you are using. Refer to [License Management](#) in the **Forescout Administration Guide** for information about licensing management and licensing modes.

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

See [Forescout Virtual Systems](#) for details on installing virtual systems and their licenses.

System Components and Requirements




This section covers the following topics:

- [Forescout Components](#)
- [System Requirements](#)

Forescout Components

This topic describes the Forescout components:



-  *Virtual systems are also available. See [Forescout Virtual Systems](#) for more information.*
-  *Refer to the [Forescout Enterprise Manager Appliance Communication Technical Note](#) for information about Enterprise Manager/Appliance communication.*
-  *You can use IPv6 addresses when installing Forescout devices.*

Forescout Appliance

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

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

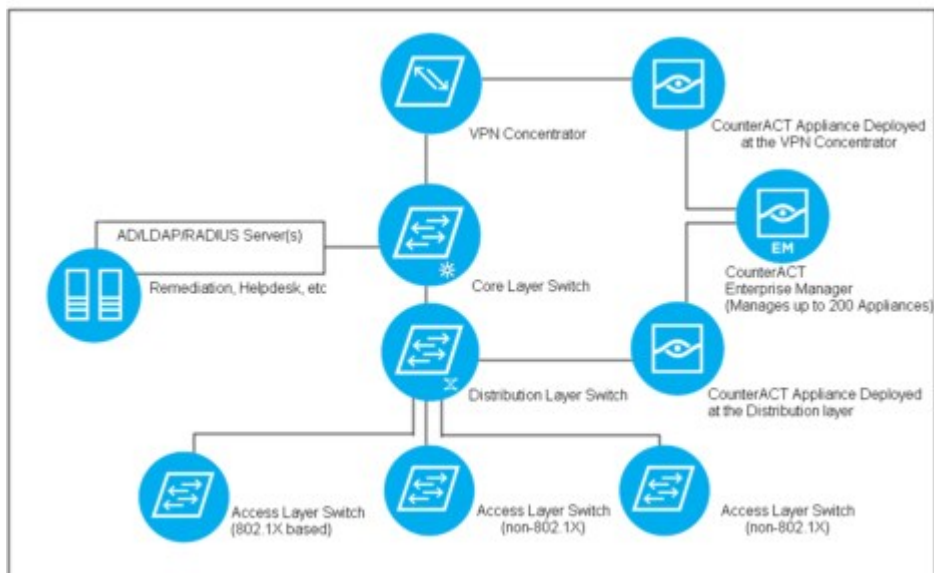
- At the connection point between a protected network area and the rest of the network. This enables protection of a specific network range against infection attempts initiated from the rest of the network and network protection against infection attempts generated from a specific network area (for example, a contractor's 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

Enterprise Manager

The Forescout Enterprise Manager is an aggregation device that communicates with multiple Forescout Appliances distributed across an enterprise. It manages Appliance 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 the Forescout platform. This information is available for display and reporting at the Forescout Console.

Recovery Enterprise Manager

The Forescout Recovery Enterprise Manager is used as a recovery device for an Enterprise Manager that is no longer functioning, for example, due to 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 Forescout component. Refer to [Disaster Recovery for Enterprise Manager](#) in the **Resiliency Solutions User Guide** for more information.

Forescout Console

The Console is the Forescout 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 Forescout platform. The Console also provides a number of tools:

- Policy tools that let you 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 the Forescout platform'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 the Forescout platform protects or the time zone setting). Other control tools let you communicate with your Network Management application and to work with third-party plugin applications.

Refer to [Working in the Console](#) in the **Forescout Administration Guide** for more information.

High Availability Systems

A Forescout 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 [High Availability Pairing](#) in the **Resiliency Solutions User Guide** for more information about this solution.

System Requirements

Before you begin installation, verify that the following requirements are met and that you have completed a Site Preparation Form (see [Appendix A - Site Preparation Form](#)).

- [Licensing Mode](#)
- [Supported Physical Forescout Devices](#)
- [Forescout Console Hardware Requirements](#)
- [Network Access Requirements](#)
- [Network Deployment Requirements](#)
- [Appliance Information Requirements](#)
- [Enterprise Manager Information Requirements](#)
- [Network Connection Requirements](#)
- [Bandwidth Requirements](#)

Requirements may vary for virtual systems. See [Virtual System Requirements](#) for details.

Licensing Mode

This version of Forescout supports two different licensing modes. Each Forescout deployment operates in a single mode, however, you may have multiple deployments that use different licensing modes. License requirements differ according to licensing mode.

Refer to [License Management](#) in the **Forescout Administration Guide** for information about licensing management and licensing modes.

To identify your licensing mode:

- From the Console, select **Help > About Forescout CounterACT...**

Supported Physical Forescout Devices

For information about physical hardware models and their supported Forescout platform versions (up to this version), see the [Forescout Hardware & Software Interoperability Matrix Reference Guide](#).

Due to memory limitations, 5110 and CT-R series Appliances do not fully support Forescout platform versions 8.2.x. For customers owning CT-R or 5110 hardware, the **Limited Appliance mode** is available for use on these Forescout hardware devices. Therefore, with the installation of versions 8.2.x – 8.3, you enable the Limited Appliance mode on your 5110 and CT-R series Appliances; this mode provides a subset of Forescout plugins that run on the Appliance and provide their Forescout eyeSight and eyeControl capabilities. For more information, see [Appendix B - Limited Appliance Mode](#).

The CT Appliance series, **revision 30**, does not support running Forescout platform version 8.3. Refer to the [Forescout Hardware & Software Interoperability Matrix Reference Guide](#).

To run Forescout platform version 8.3 on CT-100 and CT-1000 Appliances, **revision 40**, you must observe the following Forescout guidelines to avoid processing overload from occurring on these Appliances:

- Ensure that you monitor Appliance performance or run a health check on these Appliances before you attempt to upgrade them. If your CT100/CT-1000 Appliance is already in a state of high utilization, Forescout does not recommend upgrading that Appliance to version 8.3.
- Limit the maximum traffic monitoring throughput of the Packet Engine Plugin, as follows:
 - For a CT-100 Appliance, ensure that the maximum traffic monitoring throughput of the Packet Engine Plugin does not exceed 200 MB per second.
 - For a CT-1000 Appliance, Forescout suggests reducing the traffic monitoring output to 500 MB per second.

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.

Forescout Console Hardware Requirements

You must supply a machine to host the Forescout 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 / 2019
 - Linux RHEL/CentOS 7 / 8
 - macOS 10.12 / 10.13 / 10.14 / 10.15 / 11
- 2GB RAM
- 1GB disk space

Network Access Requirements

Deploying the Forescout platform requires TCP/IP communication. This section details Forescout platform 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 Forescout Console. The connectivity listed in the following table is required.

Port	Service	To or From the Forescout Platform	Function
22/TCP	SSH	From	Allows remote inspection of OS X and Linux endpoints. Allows the Forescout platform to communicate with network switches and routers.
		To	Allows access to the Forescout platform command line interface.
2222/TCP	SSH	To	(High Availability) Allows access to the physical Appliances 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 the Forescout platform access to the enterprise mail relay.
53/UDP	DNS	From	Allows the Forescout platform to resolve internal IP addresses.
80/TCP	HTTP	To	Allows HTTP redirection.
123/UDP	NTP	From	Allows the Forescout platform access to a local time server or ntp.forescout.net. By default the Forescout platform 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 the Forescout platform to communicate with network switches and routers. For information about configuring SNMP, refer to the Forescout Administration Guide .

162/UDP	SNMP	To	Allows the Forescout platform to receive SNMP traps from network switches and routers. For information about configuring SNMP, refer to the Forescout Administration Guide .
389/TCP (636)	LDAP	From	Allows the Forescout platform to communicate with Active Directory. Allows communication with Forescout web-based portals.
443/TCP	HTTPS	To	Allows HTTP redirection over TLS.
10006/TCP	SecureConnector for Linux	To	Allows SecureConnector to create a secure connection, over TLS 1.2, to the Appliance from Linux machines. SecureConnector is a script-based agent that enables management of Linux endpoints while they are connected to the network.
10003/TCP	SecureConnector for Windows	To	Allows SecureConnector to create a secure (encrypted TLS) connection to the Appliance from Windows machines. SecureConnector is an agent that enables management of Windows endpoints while they are connected to the network. Refer to the Forescout Administration Guide 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. SecureConnector is an agent that enables management of OS X endpoints while they are connected to the network. Refer to the Forescout Administration Guide 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.
13000/TCP	Forescout platform	From/To	For deployments with only one Appliance – from the Console to the Appliance. For deployments with more than one Appliance – from the Console to the Appliance and from one Appliance to another. Appliance communication includes communication with the Enterprise Manager and the Recovery Enterprise Manager, over TLS.

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.

The Forescout platform supports deployment options for:

- Monitoring multiple VLANs (tagged traffic) – recommended, as 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 [Working with Appliance Channel Assignments](#) in the **Forescout Administration Guide** for more information about these features.

Important notes:

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

Appliance Information Requirements

The following information regarding each Forescout Appliance is required:

- Forescout Appliance IP address
- Forescout 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 Enterprise Manager information is required:

- Forescout Enterprise Manager IP address
- Forescout 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 Forescout Virtual Devices](#) for details.

Bandwidth Requirements

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

Security and Compliance and RMM

This topic covers security, FIPS and certification compliance and Remote System Management.

Certification Compliance

Certification Compliance mode is a hardened configuration mode that enables advanced security features. This mode is intended for organizations that need to comply with strict security requirements. You can configure the Forescout platform to run in Certification Compliance mode during the initial Enterprise Manager/Appliance CLI configuration of a clean Forescout platform installation.

Configuration of this mode is irreversible. Verify that your organization needs Forescout to run in this mode before configuring. Changing configuration requires a clean installation of the Appliance.

If your organization does not need to comply with a specific set of strict security requirements, but would still like to follow Forescout security best practices, refer to the guidelines laid out in the Security Deployment Hardening Best Practices section of the **Forescout Administration Guide**. Following these best practices allows you to harden your security stature in a more customizable manner, by manually configuring specific options in your Forescout environment.

See [Configure an Appliance](#) and [Configure the Enterprise Manager](#) for details on how to configure Certification Compliance mode.

When the Forescout platform is running in Certification Compliance mode, the following features are affected:

- **FS-CLI.** Users won't be able to access the Bash shell. FS-CLI, a proprietary Forescout command line interface, is the only CLI shell available.
- **TLS.** The TLS version will be set to v1.2 with no option to change to lower versions.
- **SNMP.** SNMPv3 will be set as the default. If you select a different version, a warning will appear.
- **NTP.** Authenticated NTP will be set as the default. If you use unsecure, unauthenticated NTP, a warning will appear.
- **Log and database partitions.** These partitions will be encrypted.
- **FIPS Compliance** will be enabled.
- **Legacy web portals.** The Assets Portal and the Reports Portal are disabled.
- Additional user actions will be written to the Audit Trails.

FIPS Compliance

The Forescout platform meets Federal Information Processing Standard (FIPS) 140-2 (level 2) requirements.

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

Enabling FIPS Mode

An `fstool` command lets you enable FIPS on Forescout devices.

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

To enable a Forescout device to work with FIPS:

- Log in to the Forescout 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 Forescout device CLI and run the following command:

```
fstool version
```

```
-----  
<Forescout_device_type> version information  
-----
```

```
Version : 8.3
```

```
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 with SecureConnector:

- Select **Tools > Options > HPS Inspection Engine** and select the SecureConnector tab.
- From the **TLS options** drop-down menu, select **TLS version1 (FIPS)**.

Password Encryption Algorithm

Users may be required to enter credentials when working with Forescout 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 provide location-independent and OS-independent remote access over the LAN or Internet to Forescout devices. Use the module for remote KVM access and power on/off/reset, and to perform troubleshooting and maintenance tasks.

CT-xxxx Appliances and Forescout 51xx Appliances support Integrated Dell Remote Access Controller (iDRAC). See [Integrate with Remote System Management](#) for information about setting up this module.

This integration is not applicable to virtual systems.

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 setting 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 Forescout 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**.

Network Setup

This section covers the procedures for setting up the network for the Forescout platform.

About the Forescout Installation

The Forescout platform 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 details. If you are installing a Forescout High Availability system, refer to [High Availability Pairing](#) in the **Resiliency Solutions User Guide** for more information about the configuration and wiring.

Related Documents

Cisco Switches

For information about port mirroring on Cisco switches, refer to the **Configuring the Cisco Switched Port Analyzer (SPAN)** document:

<https://www.Forescout.com/wp-content/uploads/2019/02/configuring-cisco-span.pdf>

Rack Mounting Instructions

For information regarding rack-mounting instructions, refer to:

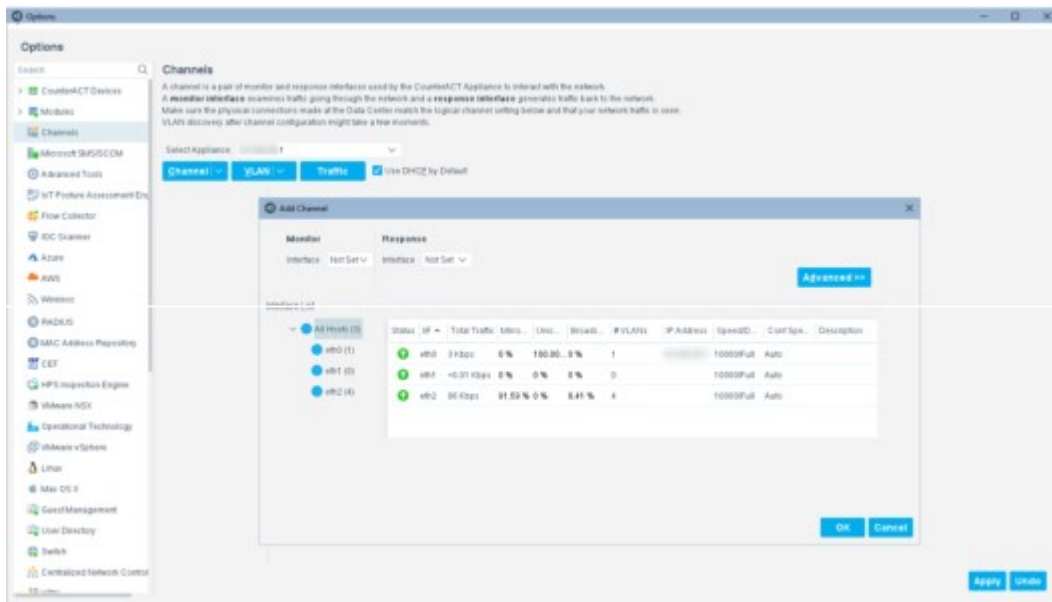
- For CT-xxxx Appliances based on hardware revision 3x/4x
 - CT-100 and CT-1000 Appliances:
<https://docs.forescout.com/bundle/rail-kit-ct-100-ct-1000/resource/rail-kit-ct-100-ct-1000.pdf>
 - CT-2000, CT-4000 and CT-10000 Appliances
<https://docs.forescout.com/bundle/rail-kit-ct-2000-ct-4000-ct-10000/resource/rail-kit-ct-2000-ct-4000-ct-10000.pdf>
- For CT-xxxx Appliances based on hardware revision 5x and Forescout 51xx Appliances (5120, 5140 and 5160):
<https://docs.forescout.com/bundle/rail-kit-51xx/resource/rail-kit-51xx.pdf>
- For Forescout 41xx Appliances (4130):
<https://docs.forescout.com/bundle/rail-kit-41xx/resource/rail-kit-41xx.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 [Working with Appliance Channel Assignments](#) in the **Forescout Administration Guide**.

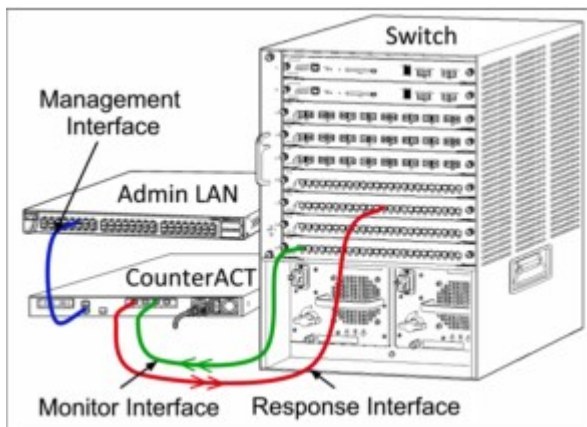


Management Interface

The management interface allows you to manage the Forescout platform 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 Console management application. The management port must have access to additional network services.

See [Network Access Requirements](#) for details.



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 Forescout 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. 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 [Set 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.

Set up Switch Connections

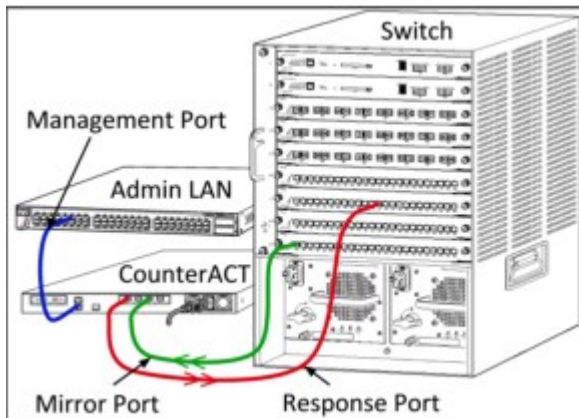
The Appliance was designed to seamlessly integrate with a wide variety of network environments. To successfully integrate the Appliance into your network, verify that your switch is set up to monitor required traffic.

Depending upon the configuration, you can combine ports to reduce the number of cables and ports needed for installation.

This topic covers the switch connection procedures and guidelines.

Recommended Installation: Separate Management, Monitor and Response Ports

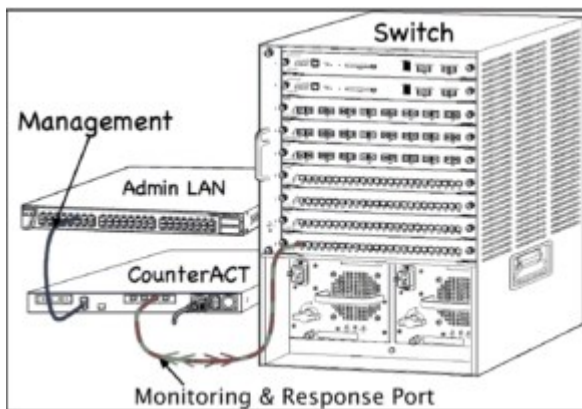
The recommended installation uses three separate cables as detailed in [Appliance Interface Connections](#).



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.

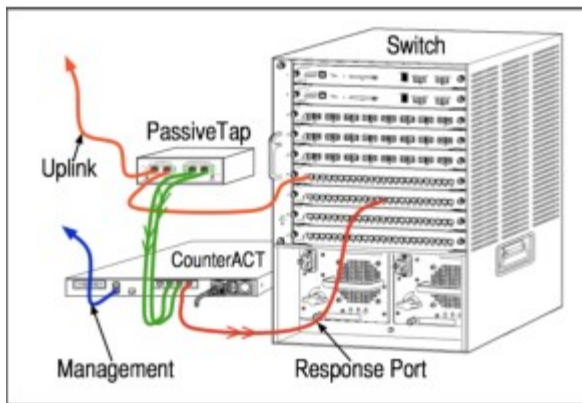


Combined Monitor and Response Port

Passive Inline Tap

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

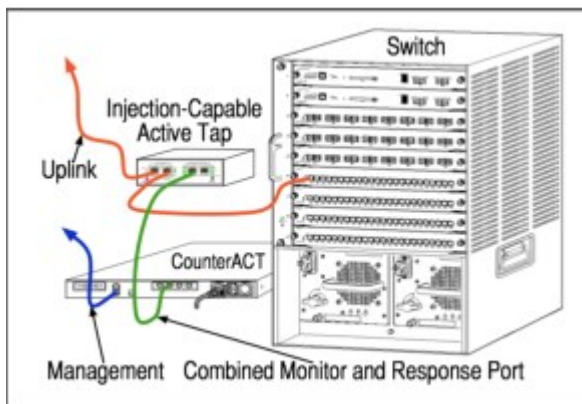
A passive inline tap requires two monitor ports (one for upstream traffic and one for downstream traffic), except in the case of a **recombination** tap, which combines the two duplex streams into a single port. Note that if the traffic on the tapped port is 802.1Q VLAN tagged, then the response port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

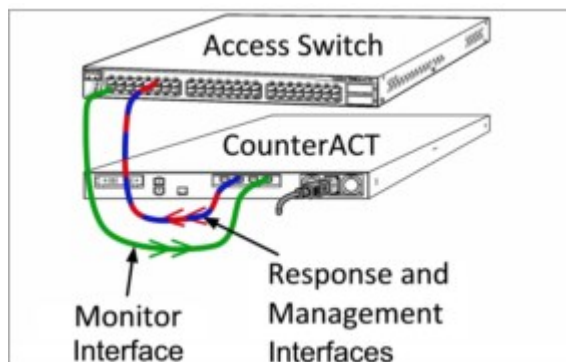
IP Layer Response (for Layer-3-Only Core Switch Installation)

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 address 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.

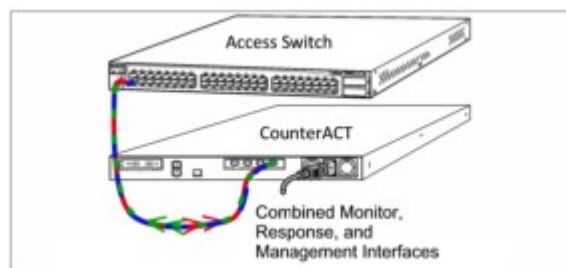


Combined Management and Response Port (Single VLAN Only)

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

If the Appliance is protecting a single VLAN, the management IP address 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 (such as 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.

In addition to 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 Forescout 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. 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 Netmask 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 Netmask 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 Forescout 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 Forescout 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 Forescout 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 Netmask** to 255.255.255.255.
6. Set the **Gateway IP Address** to the default gateway of the management interface

Appliance Setup and Configuration and Post-Installation

This topic covers Appliance setup and configuration and post-installation procedures:

- [Set up an Appliance](#)
- [Configure an Appliance](#)
- [Appliance Post-Installation Procedures](#)
- [Additional Installation Tools](#)

Set 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](#).
6. Power on the Appliance.
7. Configure the Appliance. For information about performing this configuration, see [Configure an Appliance](#).
8. Configure Intra-Enterprise Manager and Appliance authentication through CA certificate verification. See [Appendix C - Inter-Enterprise Manager and Appliance Authentication](#) for complete details.
9. 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 Forescout 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 Forescout device)
- A terminal client, such as **Hyper Terminal** (Windows) or **minicom** (Linux)

To set up a serial port connection:

1. Connect the Forescout device and the computer. Connect the serial cross cable to the Forescout 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.

- For a CT-100, type the following:

```
> console=ttyS0,19200
```

- For both a CT-1000 and a CT-2000, type the following:

```
> console=ttyS1,19200
```

- For a 4130 there are two available serial ports, type either of the following:

```
> console=ttyS0,19200
```

```
> console=ttyS1,19200
```


3. Continue the setup procedure.
 - Forescout Appliance: Continue with the next section, [Configure an Appliance](#).
 - Enterprise Manager: Continue with [Configure the Enterprise Manager](#).

Configure an Appliance

This section describes how to configure your Appliance. Most configuration definitions set here can later be changed through the Forescout Console. Refer to the [Forescout Administration Guide](#) for more information.

If the installation is interrupted or if you selected the wrong Forescout version, you will need to re-image the Appliance with the relevant version of the ISO file. See [Re-image Forescout Devices](#) for more information.

Some variations may apply to virtual systems. See [Forescout Virtual Systems](#) for details.

 *The following prompts are samples. Some Appliances may come preinstalled with earlier / later versions that have slightly different prompts.*

1. Power on the Appliance. If you have a Forescout 41xx Appliance or a Forescout 51xx Appliance, the following menu appears:

Forescout <version>-<build> options:

- 1) **Configure Forescout device**
- 2) **Restore saved Forescout configuration**
- 3) **Identify and renumber network interfaces**
- 4) **Configure keyboard layout**
- 5) **Turn machine off**

6) **Reboot the machine**

Choice (1-6) :

If you have a CT-xxxx Forescout 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**.

Forescout <version>-<build> options:

- 1) **Configure Forescout device**
- 2) **Restore saved Forescout 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. Type **1** and press **Enter**.


```
>>>>> Forescout platform Initial Setup <<<<<<
```

You are about to setup the Forescout platform. 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 Forescout Console.

Continue ? (yes/no) :

8. Type **Yes** and press **Enter**.

 The following prompt appears when running a clean installation of this version.

```
Certification Compliance Mode? (yes/no) [no] :
```

9. Unless your organization needs to comply with Common Criteria and DoDIN APL certification, type **No** and press **Enter**. See [Certification Compliance](#) for more information.

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

- 1) CounterACT Appliance
- 2) CounterACT Enterprise Manager

Choice (1-2) :

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

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

- 1) Per Appliance licensing mode
- 2) Flexx licensing mode

Choice (1-2) [1] :

11. 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.

 This option does not appear on Forescout 41xx and 51xx Appliances.

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

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

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

Description :

13. Type a description and press **Enter**.

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

This password is used to log in as 'cliadmin' to the machine Operating System and as 'admin' to the CounterACT Console. The password must be between 6 and 24 characters long and should contain at least one non-alphabetic character.

Administrator password :

14. 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) :

15. 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 :

16. 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 Forescout 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 Forescout components communicate. Add a VLAN ID for this interface only if the interface used to communicate between Forescout 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.

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

18. 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 :

19. 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

- 20.** Press **Enter**. The setup summary is displayed again.

- 21.** 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 <<<<<<
```

Forescout 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

- 22.** Press **Enter**.

After configuration, ensure that your Forescout device has a valid license. The default licensing state of your Forescout 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 Forescout virtual system, the demo license is not installed automatically at this stage. See [After creating virtual switches for the monitor, management, and response interfaces, configure them referring to docs.vmware.com and Configure the Security Policy for a vSphere Standard Switch or Standard Port Group for complete and up-to-date details about your version of VMware VSphere software.](#)

- 23.** [Configure the Security Policy settings for the standard switch or port group for Forescout:](#)

- [Select and Accept all three options \(Promiscuous Mode, MAC Address Changes, and Forged Transmits\) for the monitor and response interfaces.](#)
- [Select and Accept the Promiscuous Mode option for the monitor interface for mirrored/SPAN traffic.](#)

[Forescout 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 [Per-Appliance CounterACT Device License](#) in the **Forescout Administration Guide** for more information about demo license alerts.

- If you are using **Flexx Licensing Mode**, the **Entitlement administrator** should receive an email when the license entitlement is created and available in the Forescout Customer Support 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 **Forescout administrator** of the deployment can activate the license in the Forescout Console. Until the license is activated, Forescout 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 [License Management](#) in the **Forescout Administration Guide** for information about licensing management and licensing modes.

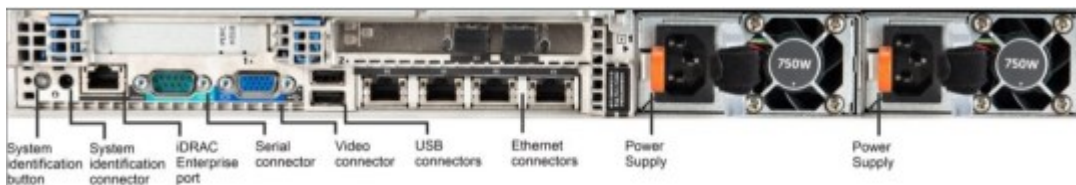
Appliance Post-Installation Procedures

After installing an Appliance, perform the following tasks:

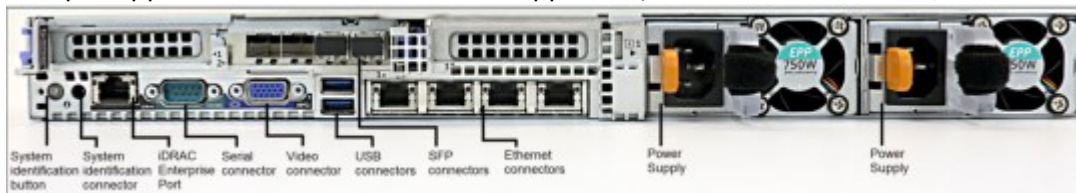
- [Connect an Appliance to the Network](#)
- [Integrate with Remote System Management](#)
- [Verify the Management Interface Connection](#)
- [Perform a Ping Test](#)
- [Generate a Configuration Summary for an Appliance](#)
- [Configure Password Protection for the Boot Loader](#)
- [Configure ICMP Settings](#)
- [Control Use of Root User Log In to Forescout Devices](#)
- Install the Forescout Console. See [Install and Log in to the Forescout Console](#).
- Run the Initial Setup Wizard. Refer to [Working with the Initial Setup Wizard](#) in the **Forescout Administration Guide**.

Connect an Appliance to the Network

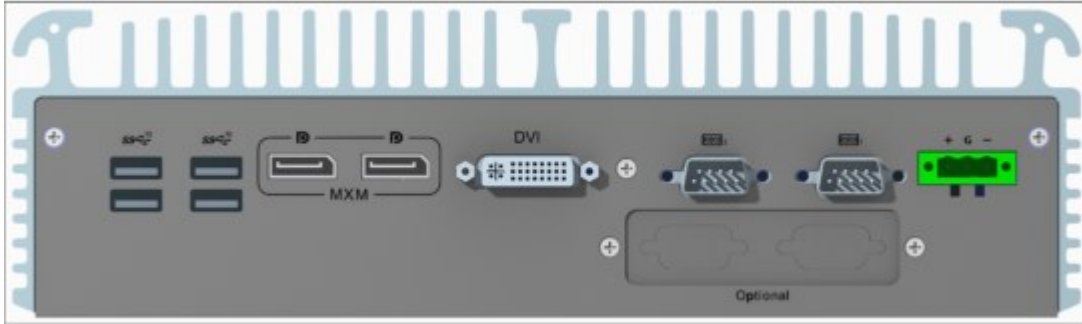
Connect the monitor and response interface cables to Ethernet ports on the rear panel of the Appliance and note the Appliance interfaces associated with the ports. You will need this information to define a **channel** when you run the Initial Setup Wizard from the Forescout Console (see [Run the Initial 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-100 Appliance, hardware revision 3x/4x



Sample Appliance Rear Panel – Forescout 51xx Appliance and CT-100 Appliance, hardware revision 5x



Sample Appliance Rear Panel – Forescout 4130 Appliance
 For CT-xxxx Appliances and Forescout 51xx (5120/5140/5160) Appliances, 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	
FTRJ1319P1BTL		
FTLF8519P3BNL	1Gb/s, 1000BASE-SX	
FTLF8519P2BCL		
FTLX1471D3BCL	10Gb/s 10GBase-LR SFP+	CT-xxxx, based on hardware revision 4x or lower
FTLX8571D3BCL / FTLX8574D3BCL	10Gb/s 10GBase-SR SFP+	
FTLX1471D3BCV	10G/1G Dual Rate (10GBASE-LR and 1000BASE-LX)	<ul style="list-style-type: none"> CT-xxxx, based on hardware revision 5x Forescout 5120/5140/5160
FTLX8574D3BCV	10G/1G Dual Rate (10GBASE-SR and 1000BASE-SX)	
571540003 (AMPHENOL)	Direct Attach 10G	

Integrate with Remote System Management

You can integrate CT-xxxx Appliances and Forescout 51xx Appliances with Remote System Management using iDRAC. This integration is not applicable to virtual systems.

Remote System Management features of Forescout 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.

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 Forescout 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 Forescout device. This section describes basic integration settings required for working with the Forescout platform.

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**.



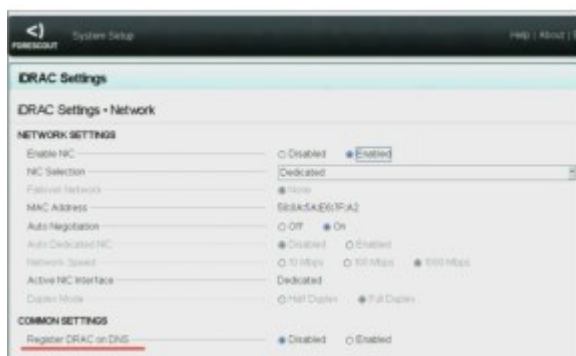
4. In the iDRAC Settings page, select **iDRAC Settings > Network**.



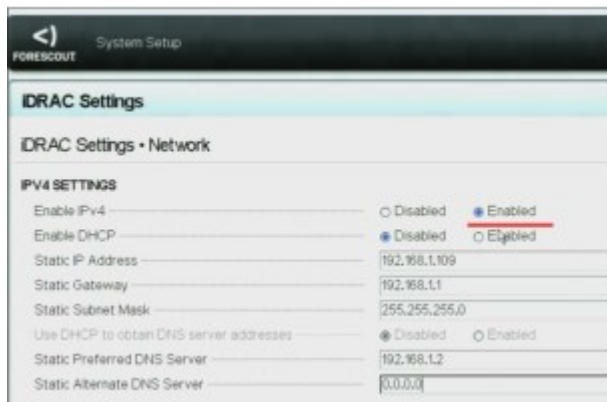
5. In **iDRAC Settings > Network > Network settings**, verify that the **Enable NIC** field is set to **Enabled**.



6. (optional) In **iDRAC Settings > Network > Common Settings**, to update a dynamic DNS:
 - a. Set **Register iDRAC on DNS** to **Enabled**.
 - b. in the **DNS iDRAC Name** field, enter the dynamic DNS.



7. In **iDRAC Settings > Network > IPV4 Settings**:

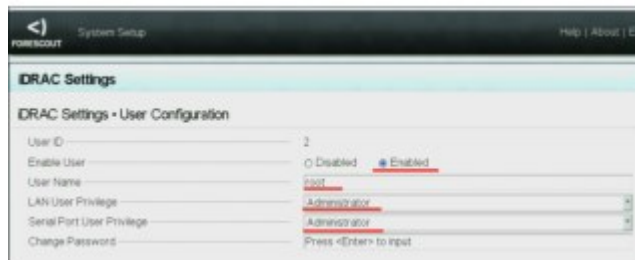


- Verify that the **Enable IPv4** field is set to **Enabled**.
- Set the **Enable DHCP** field to **Enabled** to use Dynamic IP Addressing. DHCP will automatically assign the IP Address, gateway, and subnet mask to iDRAC.

OR


Set the **Enable DHCP** field to **Disabled** to use Static IP Addressing, **and** enter values for the **Static IP Address**, **Static Gateway**, and **Static Subnet Mask** fields.

8. Select **Back**.
9. In **iDRAC Settings > User Configuration**:



Configure the following User Configuration fields for the 'root' user:

- Verify that the **Enable User** field is set to **Enabled**.

 The User Name (root) configured here is not the same as the Forescout user name.

- For **LAN User Privilege**, select **Administrator**.
- For **Serial Port User Privilege**, select **Administrator**.
- For **Change Password**, set a password for user login.

10. 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:

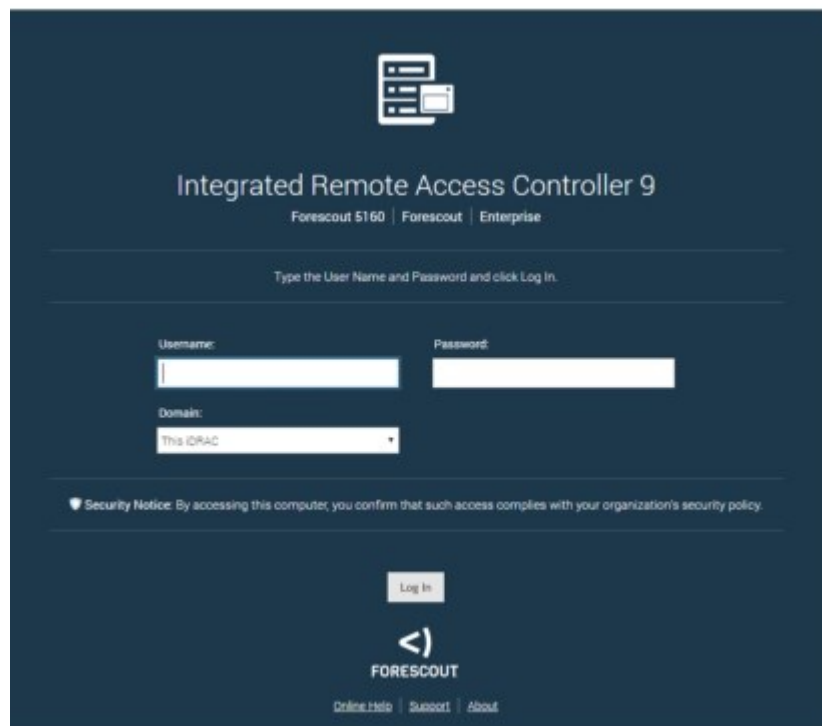


iDRAC port location

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**.

Refer to the **iDRAC User's Guide** for more information:

<https://Forescout.com/company/resources/idrac-9-user-guide/>

 *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:


```
summary
The following screen opens (sample):
CounterACT/Enterprise Manager Configuration Summary
-----
Version Information
-----
Version : <version number>
Build number : <build number>
Build date : Sun Mar 24 16:51:11 2019 GMT
-----
Host Information
-----
Hostname : <host name>
Domain name : <domain name>
Dns : <DNS>

-----
Network Information
-----
Gateway : "<gateway address>"
eth0 IPv4: <x.x.x.x>/255.255.255.0

-----
Channel Configuration Information
-----


-----
Enterprise Manager Configuration
-----
E-mail Privacy : no
Mail relay : <email server>
Operator mail : <email address>
Protected net : x.x.x.x-y.y.255.255
Management Clients : all_ips_allowed
SSH Clients : 0.0.0.0-255.255.255.255
```

2. Save the information required.

 If you defined an email server and address, the system provides you with the option of sending the configuration summary to the email address.

Configure Password Protection for the Boot Loader

Forescout 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 Forescout 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 Forescout 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`

Control Use of Root User Log In to Forescout Devices

Enhance the security of your deployment by controlling the user's ability to perform a **root** user log in, via SSH, to Forescout devices (Enterprise Manager and Appliances), whether physical devices or virtual devices.

- A new installation of the Forescout platform (version 8.2.2 or above) has, by default, the **root** user log in capability prohibited (disabled).
- An upgrade of the Forescout platform from version 8.2.1 or below to version 8.2.2 or above) keeps the existing control of the **root** user log in capability. In other words, if before the upgrade, this capability was allowed (enabled) in the `/etc/ssh/sshd_config` file of the SSH server, then after the upgrade this capability remains allowed (enabled). However, if before the upgrade, this capability was prohibited (disabled) in the `/etc/ssh/sshd_config` file of the SSH server, then after the upgrade this capability remains prohibited (disabled).

Forescout recommends prohibiting (disabling) use of the **root** user log in capability on your Forescout devices.

The following procedure must be separately performed on each Forescout device:

To control the use of "root" user to log in, via SSH, to a Forescout device:

1. Log in to the CLI of the Forescout device, using cliadmin user credentials.
2. To prohibit the use of root log in, enter the following parameter setting:
ssh_root_password_login disable
3. To allow the use of **root** log in, enter the following parameter setting:
ssh_root_password_login enable
4. Provide two password authentication, as follows:
 - a. When prompted, enter the **cliadmin** password.
 - b. When prompted, enter the shell password.

Additional Installation Tools

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

- [Configure the Interface Speed/Duplex](#)
- [Restore Appliance System Settings](#)

Configure 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**.

Restore 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 [Backing Up System and Component Settings](#) in the **Forescout Administration Guide** for more information about how to back up settings.

To restore system settings:

1. Power on the Appliance.
Forescout <version>-<build> options:

1) Configure Forescout Device
2) Restore saved Forescout 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 Forescout 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 [High Availability Backup and Restore](#) in the **Resiliency Solutions User Guide** for details about working with High Availability systems.

EM Setup and Configuration and Post-Installation

This chapter details the Enterprise Manager setup and configuration procedures. Many of the configuration definitions set here can later be updated through the Forescout Console. Refer to the [Forescout Administration Guide](#) for more information.

Some variations may apply to virtual systems. See [About Forescout Virtual Systems](#) for details.

- [Set up the Enterprise Manager](#)
- [Configure the Enterprise Manager](#)
- [Enterprise Manager Post-Installation Procedures](#)
- [Restore Enterprise Manager System Settings](#)

Set 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. Configure Intra-Enterprise Manager and Appliance authentication through CA certificate verification. See [Appendix C - Inter-Enterprise Manager and Appliance Authentication](#) for complete details.
7. 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.

Configure the Enterprise Manager

This section describes how to configure the Enterprise Manager.

If the installation is interrupted or if you selected the wrong Forescout version, you will need to re-image the Appliance with the relevant version of the ISO file. See [Re-image Forescout Devices](#) for more information.

 *The following prompts are samples. Some Appliances may come preinstalled with earlier / later versions that have slightly different prompts.*

1. Power on the Enterprise Manager. If you have a Forescout 51xx Enterprise Manager, the following menu appears:
Forescout <version>-<build> options:

1) **Configure Forescout Device**
2) **Restore saved Forescout configuration**

- 3) Identify and renumber network interfaces
- 4) Configure keyboard layout
- 5) Turn machine off
- 6) Reboot the machine

Choice (1-6) :

If you have a CT-xxxx Forescout 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. Refer to 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**.

Forescout <version>-<build> options:

- 1) Configure Forescout Device
- 2) Restore saved Forescout 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. Type **1** and press **Enter**.

```
>>>>> The Forescout platform Initial Setup <<<<<<
You are about to setup the Forescout platform. 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 continue the setup from the
Forescout Console.
Continue? (yes/no) [yes]
```

8. Type **Yes** and press **Enter**.

 The following prompt appears when running a clean installation of this version.

```
Certification Compliance Mode? (yes/no) [no] :
```

9. Unless your organization needs to comply with Common Criteria and DoDIN APL certification, type **No** and press **Enter**. See [Certification Compliance](#) for more information.

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

- ```
1) CounterACT Appliance
2) CounterACT Enterprise Manager
```

Choice (1-2) :

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

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

- ```
1) Per Appliance Licensing Mode
2) Flexx Licensing Mode
```

Choice (1-2) [1] :

11. 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.

 This option does not appear on Forescout 51xx Appliances.

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

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

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

```
Description [Enterprise Manager] :
```

12. Type a description and press **Enter**.

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

This password will be used to log in as 'cliadmin' to the machine Operating System and as 'admin' to the CounterACT Console.

The password must be between 6 and 24 characters long and should contain at least one non-alphabetic character.

Administrator password :

13. 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) :

14. 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 :

15. 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 Forescout 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 Forescout components communicate. Add a VLAN ID for this interface only if the interface used to communicate between Forescout 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.

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

17. 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 :

- 18.** 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

- 19.** Press **Enter**. The setup summary is displayed again.

- 20.** 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

- 21.** Press **Enter**.

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

- If your Forescout deployment is 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 Forescout virtual system, the demo license is not installed automatically at this stage. See [After creating virtual switches for the monitor, management, and response interfaces, configure them referring to docs.vmware.com and Configure the Security Policy for a vSphere Standard Switch or Standard Port Group for complete and up-to-date details about your version of VMware VSphere software.](#)

- 22.** [Configure the Security Policy settings for the standard switch or port group for Forescout:](#)

- [Select and Accept all three options \(Promiscuous Mode, MAC Address Changes, and Forged Transmits\) for the monitor and response interfaces.](#)
- [Select and Accept the Promiscuous Mode option for the monitor interface for mirrored/SPAN traffic.](#)

[Forescout 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 [Per-Appliance CounterACT Device License](#) in the **Forescout Administration Guide** for more information about demo license alerts.

- If your Forescout deployment is using **Flexx Licensing Mode**, the **Entitlement administrator** should receive an email when the license entitlement is created and available in the Forescout Customer Support Portal. Once available, the **Forescout administrator** of the deployment can activate the license in the Forescout Console. Until the license is activated, Forescout 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 [License Management](#) in the **Forescout Administration Guide** for information about licensing management and licensing modes.

Enterprise Manager 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](#)
- [Control Use of Root User Log In to Forescout Devices](#)

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

The Forescout platform 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 Forescout 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.

Restore 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 [Backing Up System and Component Settings](#) in the **Forescout Administration Guide** for more information about how to back up settings.

To restore system settings:

1. Power on the Enterprise Manager.
Forescout <version>-<build> options:
 - 1) **Configure Forescout Device**

- 2) Restore saved Forescout 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 Forescout 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.

Restore 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 [High Availability Backup and Restore](#) in the **Resiliency Solutions User Guide** for details about working with High Availability systems.

Re-image Forescout Devices

If you need to reinstall the Forescout platform on a Forescout device (Enterprise Manager, Appliance), for example, when upgrade or configuration have failed and cannot be completed. Re-image the Forescout device using any one of the following techniques:

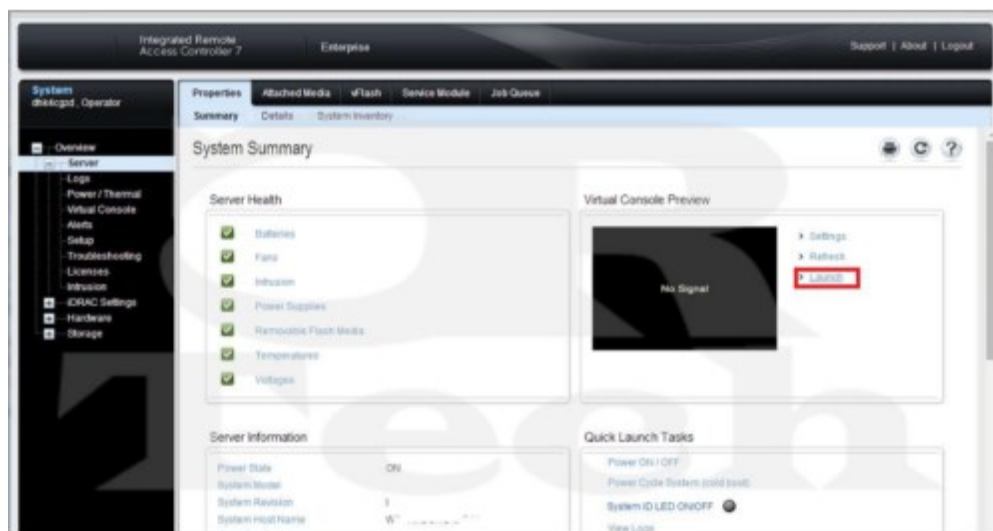
- [Remotely, using the iDRAC module of the Forescout device](#)
- [On-site, using either a prepared DVD or a USB memory device](#)

Remote Re-imaging

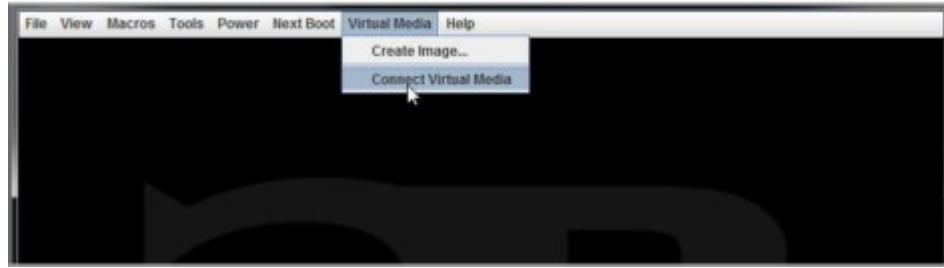
Forescout recommends to remotely re-image a Forescout device (physical hardware), using the device's iDRAC module. Therefore, it is also recommended to set up the iDRAC module on all physical hardware devices. See [Integrate with Remote System Management](#) for information about setting up the iDRAC module.

To remotely re-image the Forescout device:

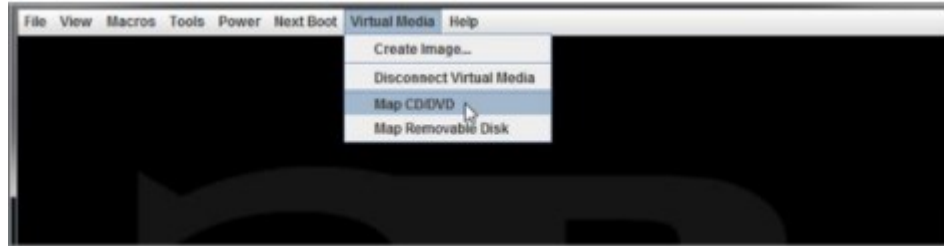
1. Download the Forescout platform ISO image (.iso file) from the Customer Support Portal:
Go to <https://Forescout.force.com/support/> and select **Downloads**.
2. Connect to the iDRAC module, using its IP address, and log in.
3. Select the Forescout device to receive the ISO image and then, in the **Properties** tab > **Summary** tab > **View Console Preview** pane, select **Launch** to launch the iDRAC console.



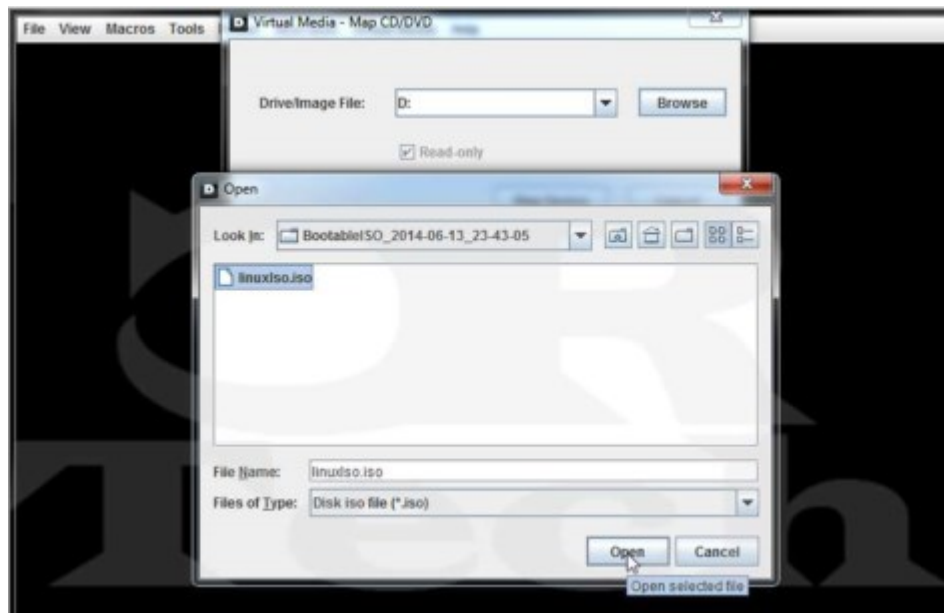
4. In the toolbar **Virtual Media** menu, select **Connect Virtual Media**.



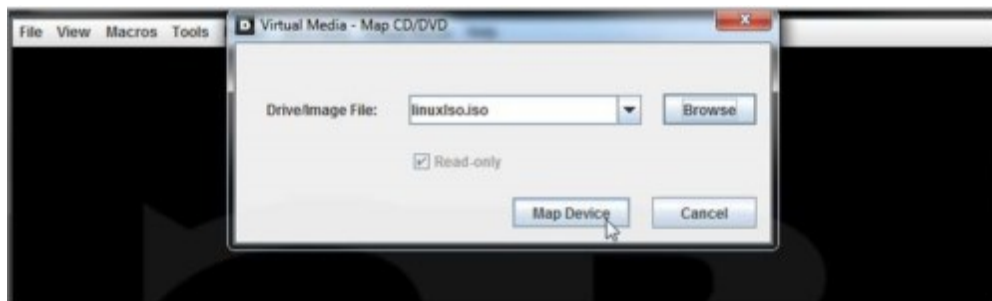
- 5. In the toolbar **Virtual Media** menu, select **Map CD/DVD**.



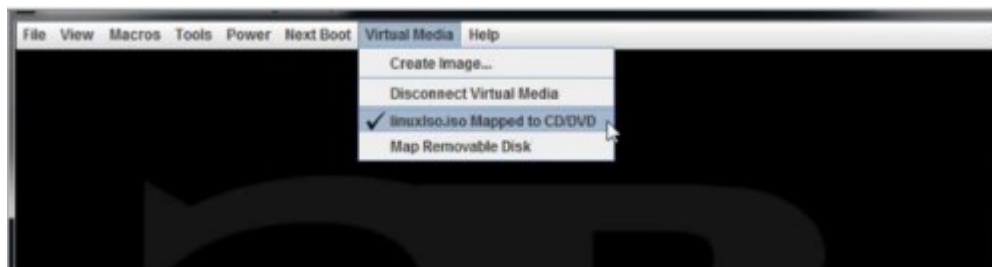
- 6. In the **Virtual Media – Map CD/DVD** dialog, select the `.iso` file, which was previously downloaded in step 1 of this procedure.



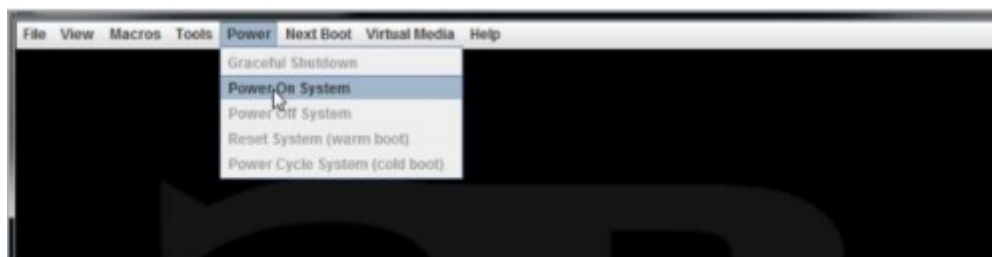
- 7. In the **Virtual Media – Map CD/DVD** dialog, select **Map Device**.



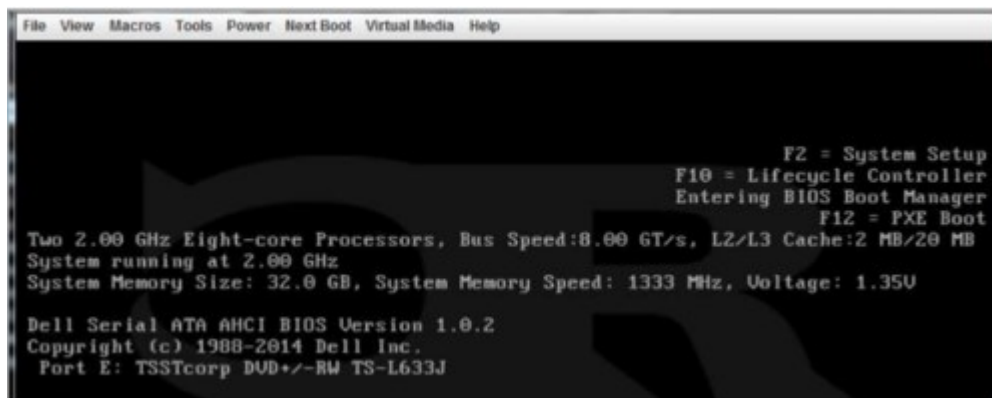
- 8. In the toolbar **Virtual Media** menu, confirm that the `.iso` file is mapped.



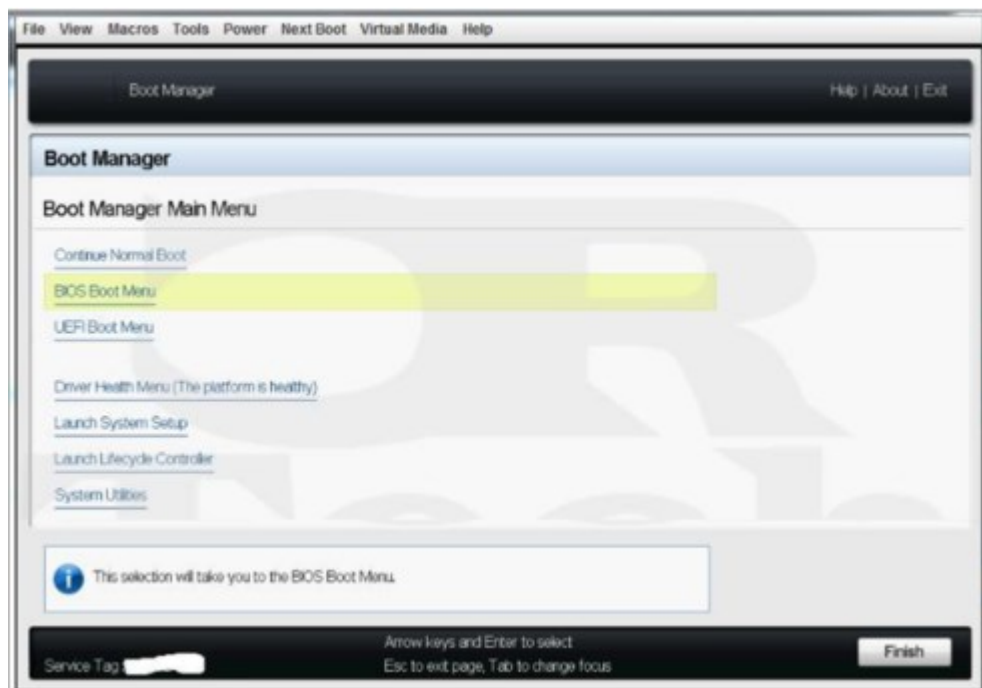
- 9. In the toolbar **Power** menu, do the following:
 - a. Select **Power Off System** to power off the Forescout device.
 - b. Select **Power On System** to power on the Forescout device.



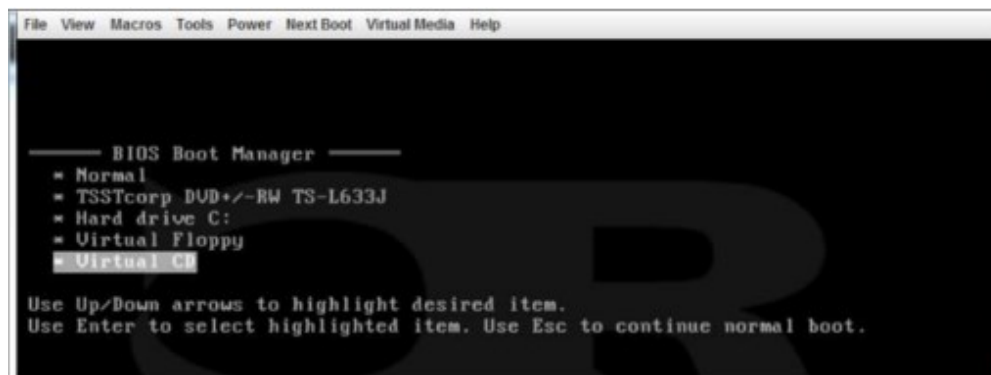
- 10. During BIOS boot of the Forescout device, select **F11**.



- 11. In the **Boot Manager Main Menu**, select **BIOS Boot Menu**.



12. In the **BIOS Boot Manager** menu, select the **Virtual CD** option and then press **Enter**. The **.iso** file begins its boot.



13. In the presented CounterACT install menu, select **Configure CounterACT**. See [Configure an Appliance](#) or [Configure the Enterprise Manager](#).
14. Proceed to work with any of the other options in the CounterACT install menu, as necessary. The available options are:
 - a. **Configure CounterACT**
 - b. **Restore saved CounterACT configuration**
 - c. **Identify and renumber network interfaces**
 - d. **Configure Keyboard layout**
 - e. **Turn machine off**
 - f. **Reboot the machine**

On-site Re-imaging

This topic covers the following procedures:

- [Prepare an Installation DVD](#)
- [Prepare a Bootable USB Memory Device](#)
- [Re-image the Forescout Device Using an Installation DVD or a USB Memory Device](#)

Prepare an Installation DVD

To prepare an installation DVD:

1. Download or obtain the Forescout platform ISO image from the Customer Support Portal: Go to <https://Forescout.force.com/support/> and select **Downloads**.
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 Forescout platform ISO image to a Linux machine from the Customer Support Portal: Go to <https://Forescout.force.com/support/> and select **Downloads**.
2. Plug in the USB memory device and determine its identity.
3. Log in to the Appliance/Linux machine and run the following command:

```
dd if=<image_location> of=/dev/sd<x> bs=10M
```

Where `sd<x>` can be, for example, `sdc`, `sdd` or `sde` depending on the memory device.
Note that the command must be `/dev/sd<x>` and not `/dev/sd<x>1` (that is, use the whole device rather than a single partition on the device).

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

1. Download the Forescout ISO image to a Windows machine.
2. Use a boot image utility to create a bootable USB memory device with the Forescout installation image.

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

To change the BIOS boot settings on a Forescout 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 [Configure 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.

Re-image the Forescout Device Using an Installation DVD or a USB Memory Device


To on-site re-image the Forescout device:

- 1.** Insert the DVD with the ISO image or connect the USB memory device to the Forescout device and restart the device.
- 2.** Proceed with the Forescout installation. See [Configure an Appliance](#) or [Configure the Enterprise Manager](#).

Install and Log in to the Forescout Console

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

This topic covers the following subjects:

- [Information Required Before You Install the Console](#)
- [Install from Forescout Portal](#)
-  It is recommended to install the Console, which you download from the Forescout Customer Support portal, to ensure that you receive the latest version.
- [Install from a Browser on Your Appliance](#)
- [Log in to the Console](#)
- [Run the Initial Setup Wizard on the Console](#)
- [Uninstall Previous Versions](#)

Information Required Before You Install the Console

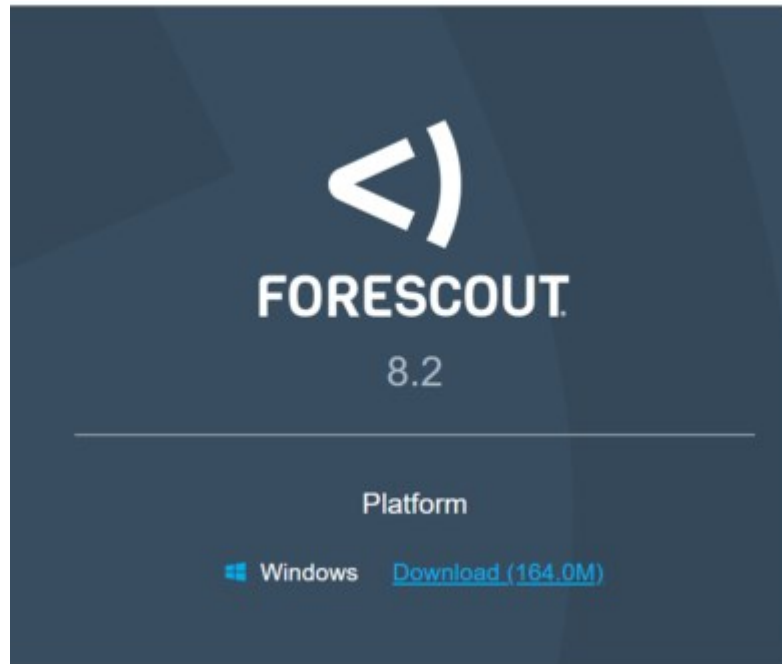
Before you install the Console, gather the information listed below and enter it in the **Value** column for easy access.

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)	
Forescout 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 the Forescout platform 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 the Forescout platform can analyze which network hosts have successfully been authenticated	
Switch IP Address, Vendor and SNMP Parameters	

Install from Forescout Portal

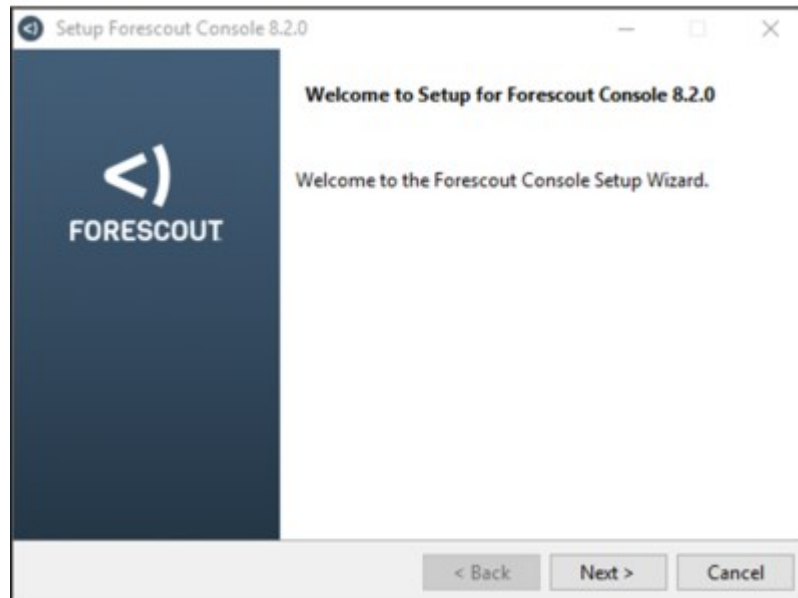
To install from the Forescout Portal:

1. Navigate to the Downloads page on the [Customer Support Portal](#) and download the **Forescout Console Setup** file.
2. Select the **Forescout Console Setup** file. The Forescout Console software download screen opens.

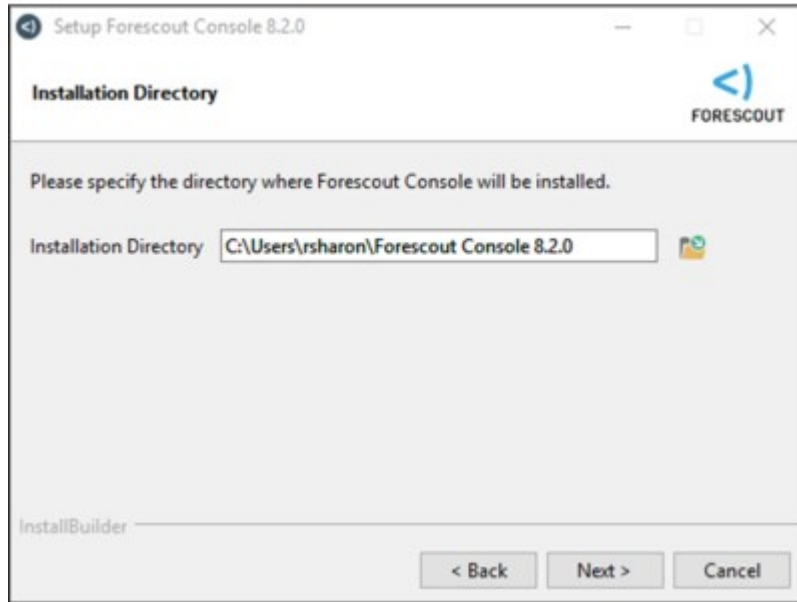


Forescout Console Software Download Screen

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.

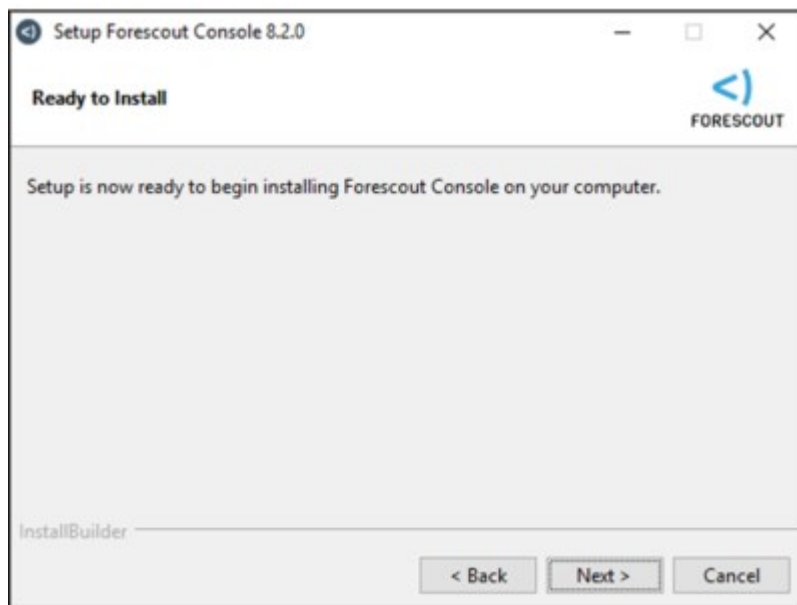


5. Select **Next**. The Installation Directory screen opens.



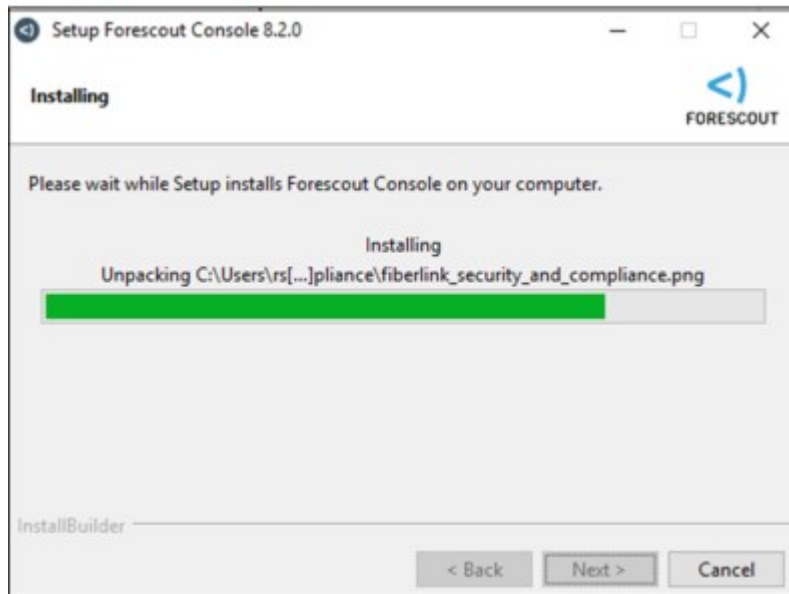
Installation Directory Screen

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



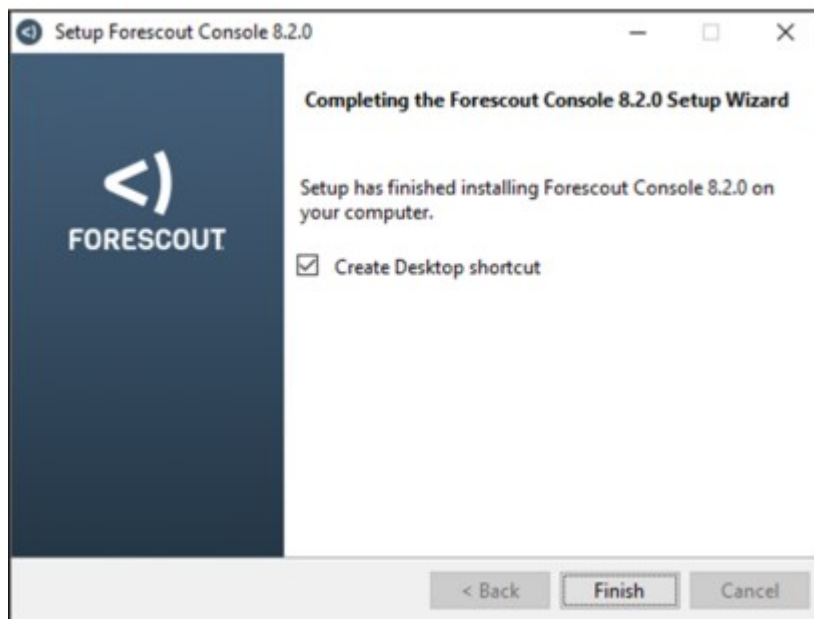
Ready to Install Screen

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



Installing Screen

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




Completing the Forescout Setup Wizard Screen

9. Select **Finish**.

Install from a Browser on Your Appliance

Use the installation software built into your Appliance to install the Forescout Console from a browser.

 *This option is not available when upgrading.*

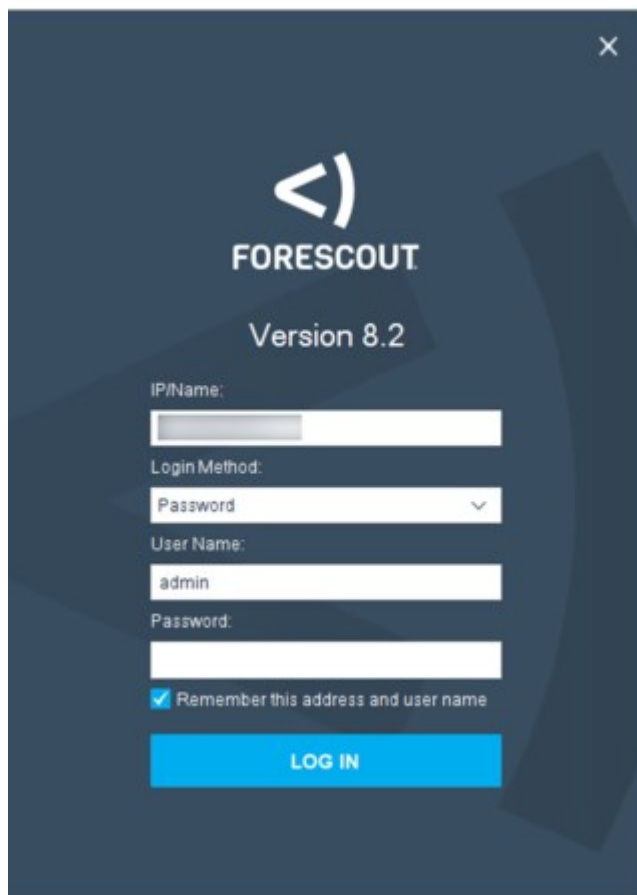
To install the Forescout Console from a browser:

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.

Log in to the Console

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

1. Select the **Forescout** icon from the shortcut that you created. The Forescout Login dialog box opens.



Forescout Login Dialog Box

2. In the **IP/Name** field, type the IP address or host name of a Forescout device.
3. Choose a login method from the **Login Method** drop-down list. Refer to [Creating Users and User Groups](#) in the **Forescout Administration Guide** for more information about login methods.
4. In the **User Name** field, type your user name.
5. In the **Password** field, type your password.
6. Select **Login** to open the Console.

The system comes with the predefined **admin** user. The user password and Forescout IP address are set during Forescout installation.

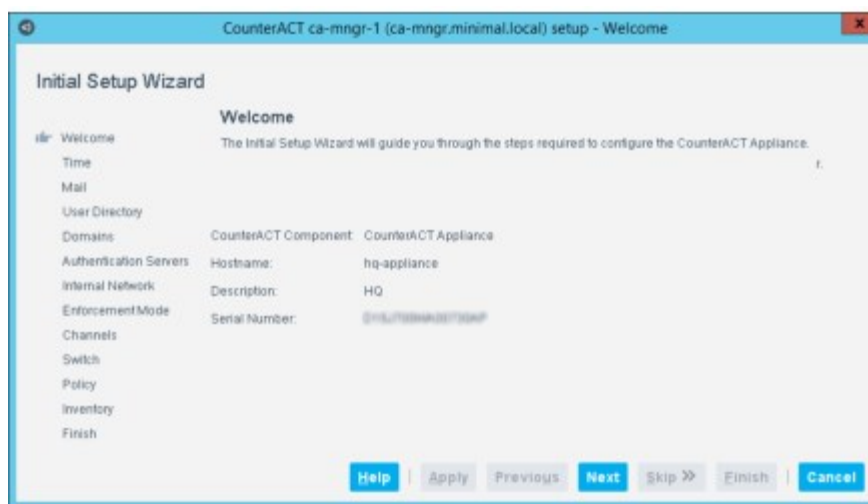
When logging in to the Console for the first time, you are prompted to verify that you are connecting to a trusted Forescout device.

If customer verification has not yet been completed, you might be prompted to complete the customer verification process. Refer to [Customer Verification](#) in the **Forescout Administration Guide** for more information.

You can change the password via the Console. Refer to [Managing Users](#) in the **Forescout Administration Guide** for more information.

Run 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 the Forescout platform is up and running quickly and efficiently. Refer to [Working with the Initial Setup Wizard](#) in the **Forescout Administration Guide** for more information.



Initial Setup Wizard

License installation can be performed from the Wizard when working with virtual systems. See [After creating virtual switches for the monitor, management, and response interfaces, configure them referring to docs.vmware.com and Configure the Security Policy for a vSphere Standard Switch or Standard Port Group for complete and up-to-date details about your version of VMware VSphere software.](#)

7. [Configure the Security Policy settings for the standard switch or port group for Forescout:](#)
 - [Select and Accept all three options \(Promiscuous Mode, MAC Address Changes, and Forged Transmits\) for the monitor and response interfaces.](#)
 - [Select and Accept the Promiscuous Mode option for the monitor interface for mirrored/SPAN traffic.](#)

[Forescout Virtual Device Deployment in VMware.](#)

Uninstall Previous Versions

To uninstall a previous Console version:

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

2. Alternatively, select the **Uninstall Forescout Console** icon from the Forescout program group on the Start menu.

Forescout Virtual Systems

This section covers the following topics:

- [About Forescout Virtual Systems](#)
- [How to Work With Virtual Devices](#)
- [Virtual System Requirements](#)
- [Virtual Environment Setup - Define Real NICs](#)
- [VMware Virtual Systems](#)
- [Hyper-V Virtual Systems](#)
- [KVM Virtual Systems](#)
- [Configure a Forescout Virtual Device](#)
- [Duplicate a Virtual Device](#)
- [Move a Virtual Device to a New Server](#)

About Forescout Virtual Systems

Forescout 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 Forescout 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 using Flexx Licensing Mode, all licensing-related procedures for virtual systems are identical to those for physical systems. Refer to the [Flexx Licensing How-to Guide](#) for information on Flexx licensing. If you are using Per-Appliance Licensing Mode, see [Install a Virtual License \(Per-Appliance Licensing Mode Only\)](#) for details.

Beyond changes to handling licenses, all other Forescout features and tools available when working with Forescout hardware are available in the virtual version. Refer to the [Forescout Administration Guide](#) for more information.

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.

How to Work With Virtual Devices

Perform the following 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 Forescout 8.3. See [Virtual Environment Setup - Define Real NICs](#).
3. Deploy the Forescout virtual devices. See [VMware Virtual Systems](#), [Hyper-V Virtual Systems](#) or [KVM Virtual Systems](#).
4. Configure the Forescout virtual devices and set up the Console. See [Configure a Forescout Virtual Device](#) and [Perform the Initial Console Setup](#)

You should have a solid understanding of virtual networking concepts and functionality when working with Forescout virtual devices.

Virtual System Requirements

This topic describes:


- [Hardware Minimum Requirements](#)
- [Network Connection Requirements for Forescout Virtual Devices](#)

Additional requirements described for physical deployments also apply. See [System Requirements](#).

Hardware Minimum Requirements

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

Network Connection Requirements for Forescout Virtual Devices

 *This requirement is only relevant if your deployment is using Per-Appliance Licensing Mode.*

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

The Forescout device connected to the Internet sends license authorization requests to the Forescout License server (<https://license2.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 the Forescout platform 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](#)

VMware Requirements and Support

This section describes requirements and supported VMware versions.

Supported VMware Versions


For information about the vendor models (hardware/software) and versions (product/OS) that are validated for integration with this Forescout component, refer to the [Forescout Compatibility Matrix](#).

vMotion Support

Forescout 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 Forescout 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 Forescout 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.)

Create Virtual Switches

Create virtual switches with these considerations:

1. Select a host to install the virtual Appliance and create virtual switches (**vSwitches**) for the host's **management**, **monitor** and **response** NICs with these considerations:
 - If using a standard vSwitch, select a host on which to install the virtual Appliance and create virtual switches (**vSwitches**) for the host's **management**, **monitor** and **response** NICs.
 - To centrally manage the network configuration of multiple hosts when using a vSphere distributed Switch, create vSphere distributed switches and associated port groups for **management**, **monitor**, and **response** on a data center.
2. Use the **SPAN Port** for the standard switch or port group handling mirrored/SPAN traffic for the monitor interface. Set the switch to **trunk mode** by using **VLAN ID 4095**.

Refer to docs.vmware.com and [Create a vSphere Standard Switch](#) or [Create a vSphere Distributed Switch](#) for complete and up-to-date details about your version of VMware vSphere software.

Configure Virtual Switches

Configure virtual switches with these considerations:

1. After creating virtual switches for the **monitor**, **management**, and **response** interfaces, configure them referring to docs.vmware.com and [Configure the Security Policy for a vSphere Standard Switch or Standard Port Group](#) for complete and up-to-date details about your version of VMware vSphere software.
2. Configure the Security Policy settings for the standard switch or port group for Forescout:
 - Select and Accept all three options (Promiscuous Mode, MAC Address Changes, and Forged Transmits) for the **monitor** and **response** interfaces.
 - Select and Accept the **Promiscuous Mode** option for the **monitor** interface for mirrored/SPAN traffic.

Forescout Virtual Device Deployment in VMware

To work with your Forescout virtual system, you must extract the image files from the Forescout virtual system package that you received. You can use the image to deploy several devices and then apply either:

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

See [Install a Virtual License](#) for details.


Extract Deployment Files from the Forescout Virtual System Package

Your Forescout virtual system package is a zip file that contains all the files required to deploy a Forescout virtual device. 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 Forescout Virtual Devices

1. After creating and configuring virtual switches for the **monitor**, **management**, and **response** interfaces, deploy them referring to docs.vmware.com and [Deploy a Virtual Machine from an OVF or OVA File in the VMware Host Client](#) for complete and up-to-date details about your version of VMware VSphere software.
2. On the **Datastore** page, the location defined to store the virtual machine must have a minimum of 200 GB total disk space.

The following table shows the network selections of the OVF for Forescout:


VM Interface	Forescout Interface
Management	Management Port Group
Monitor	Monitor Port Group
Response	Response Port Group

Post-Deployment Verification and VMware Configuration

1. After creating, configuring, and deploying virtual switches for the **monitor**, **management**, and **response** interfaces, verify the following host properties referring to docs.vmware.com for complete and up-to-date details about your version of VMware VSphere software.
2. For each interface, verify that the **Adapter Type** is defined as **E1000 OR VMX3**.
3. For each interface, verify that the **Network label** is configured with the correct virtual switch.

The following table shows the mapping between the interfaces:

VM Interface	Forescout 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 Forescout deployment in a Layer 3 configuration.

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

Hyper-V Virtual Systems

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

- [Hyper-V Requirements and Support](#)
- [Deploy Forescout Virtual Devices in Hyper-V](#)
- [Configure Hyper-V to Work with Forescout Devices](#)

- [Automate Forescout Deployment in Hyper-V Environments](#)


Hyper-V Requirements and Support

The Forescout virtual system is supported when running on Microsoft Hyper-V.

Supported Operating Systems

- For information about the vendor models (hardware/software) and versions (product/OS) that are validated for integration with this Forescout component, refer to the [Forescout Compatibility Matrix](#).

Hyper-V Requirements

- Forescout 8.3
 - It is recommended **not** to mount the Forescout 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. <http://support.microsoft.com/kb/2885541>
 - Configure the outgoing interface as IP Layer in the Forescout platform.
 -  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 [Working with Appliance Channel Assignments](#) in the **Forescout Administration Guide** for more information.
- 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 Forescout Virtual Devices in Hyper-V

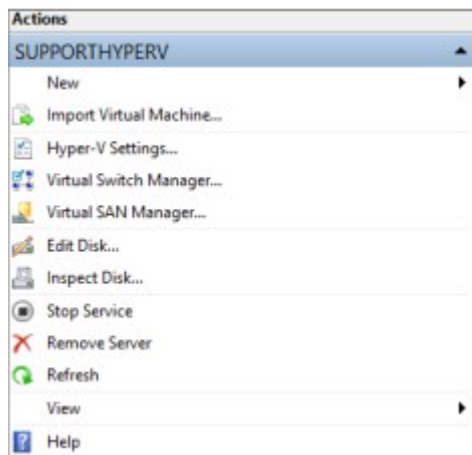
Perform the following procedures for each Forescout virtual device that you plan to deploy.

Configure Virtual Switches

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

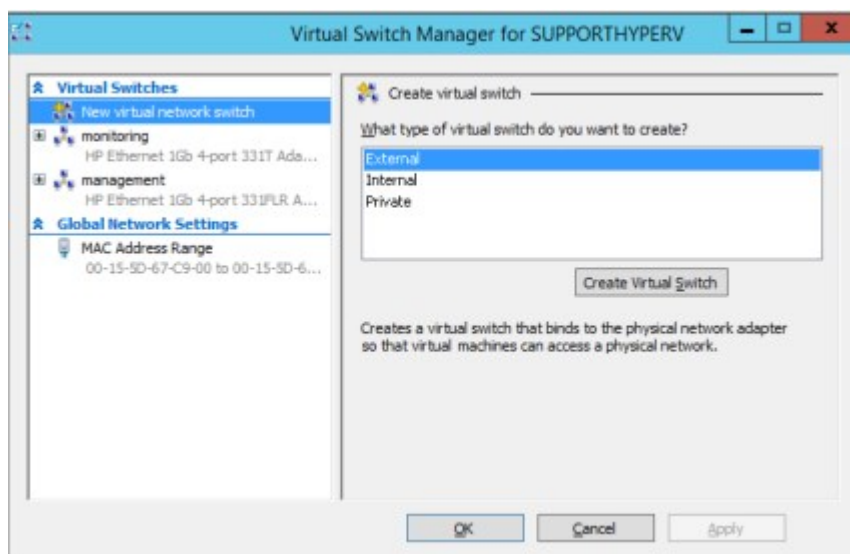
To create virtual switches:

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



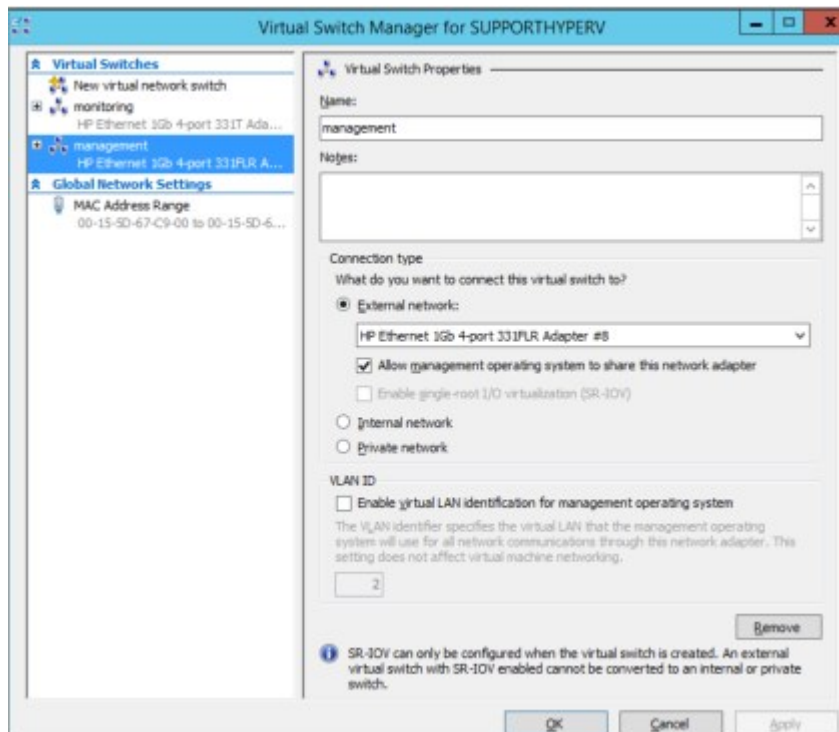
Hyper-V Manager - Actions

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



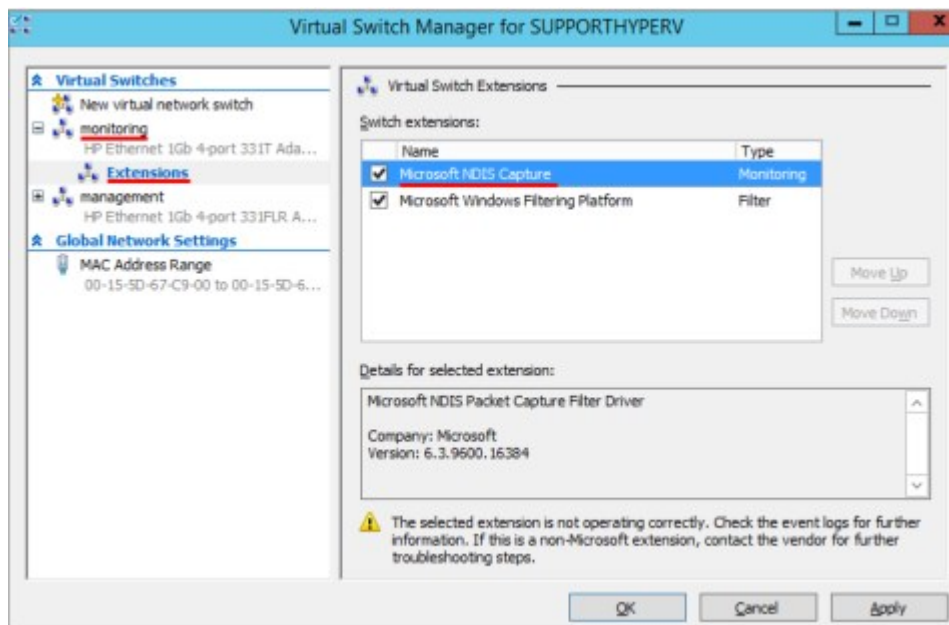
Virtual Switch Manager – New Switch

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

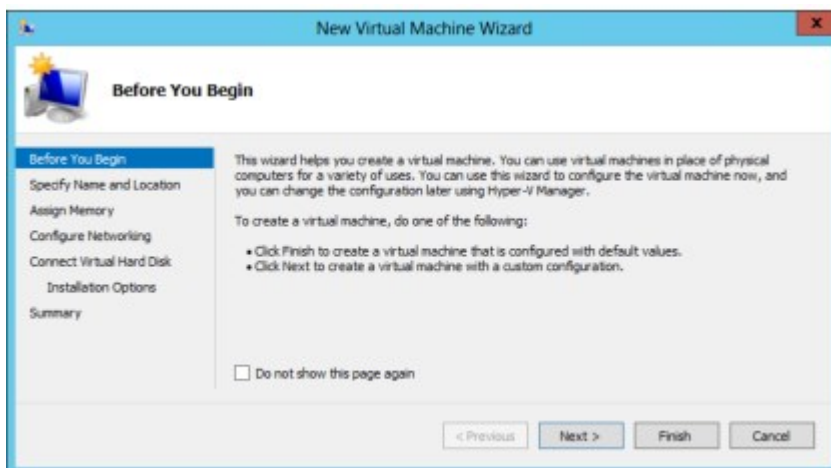
7. Select **OK**.

Create a Hyper-V Virtual Machine

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

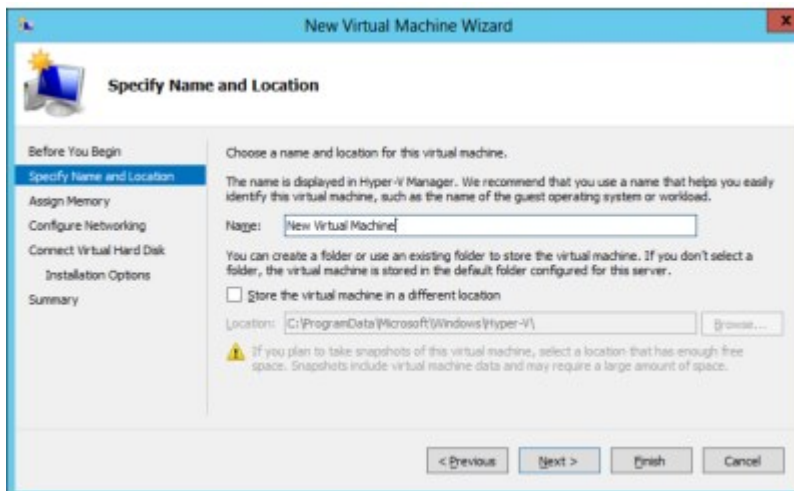
To create a Hyper-V Virtual Machine:

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



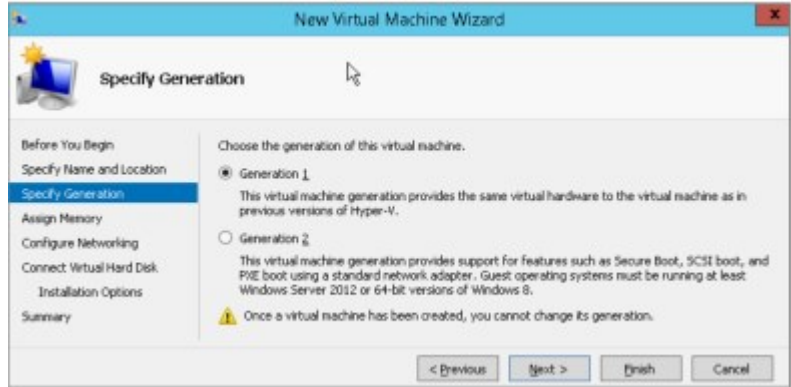
New Virtual Machine – Before You Begin

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**.



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



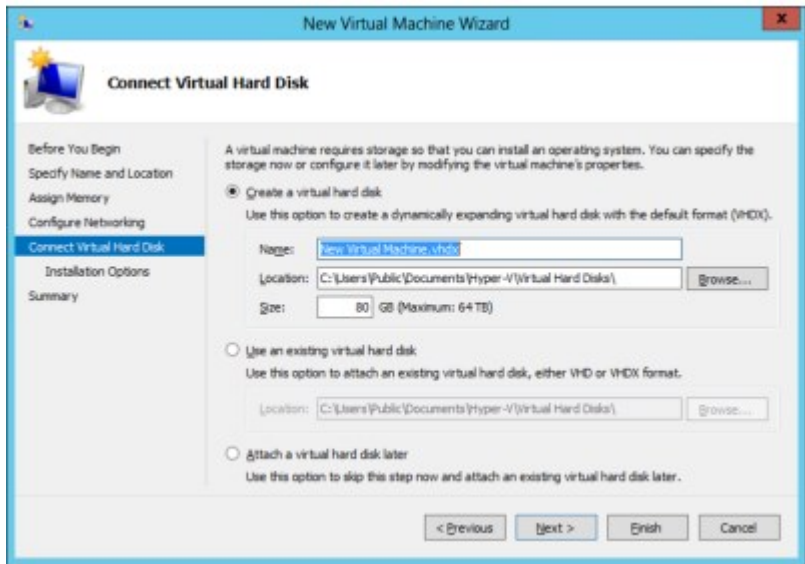
New Virtual Machine – Assign Memory

- 5. Select the Management network adaptor configured in [Configure Virtual Switches](#) and select **Next**. You can also configure this later. Legacy Network Adapters should not be used.



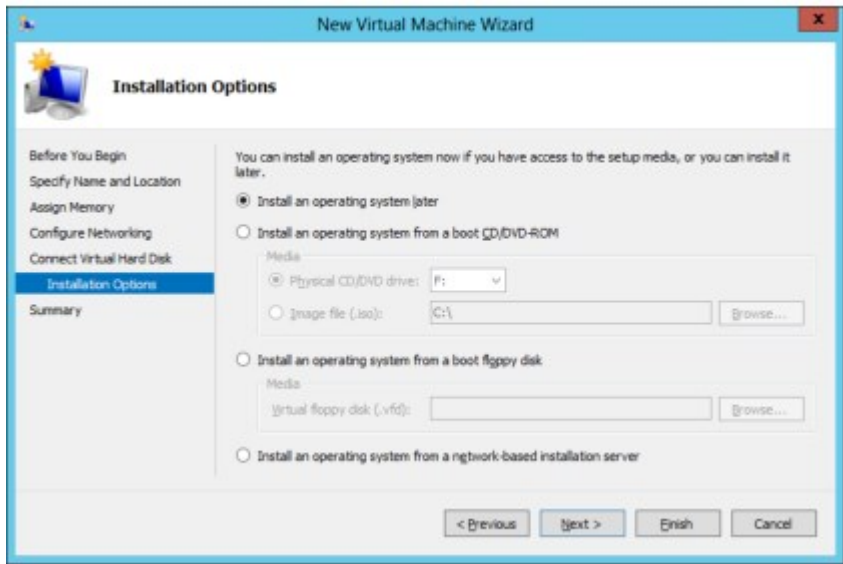
New Virtual Machine – Configure Networking

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



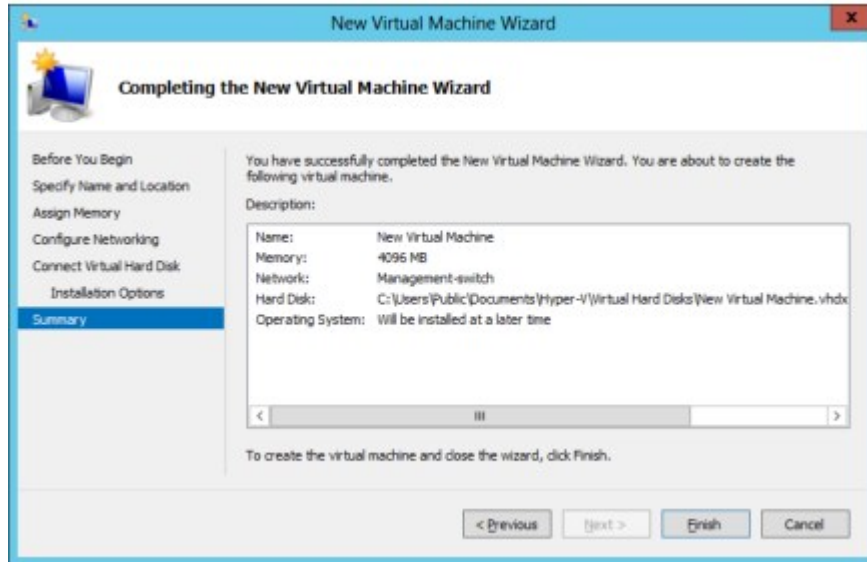
Connect Virtual Hard Disk

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.

Configure Network Adapters

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

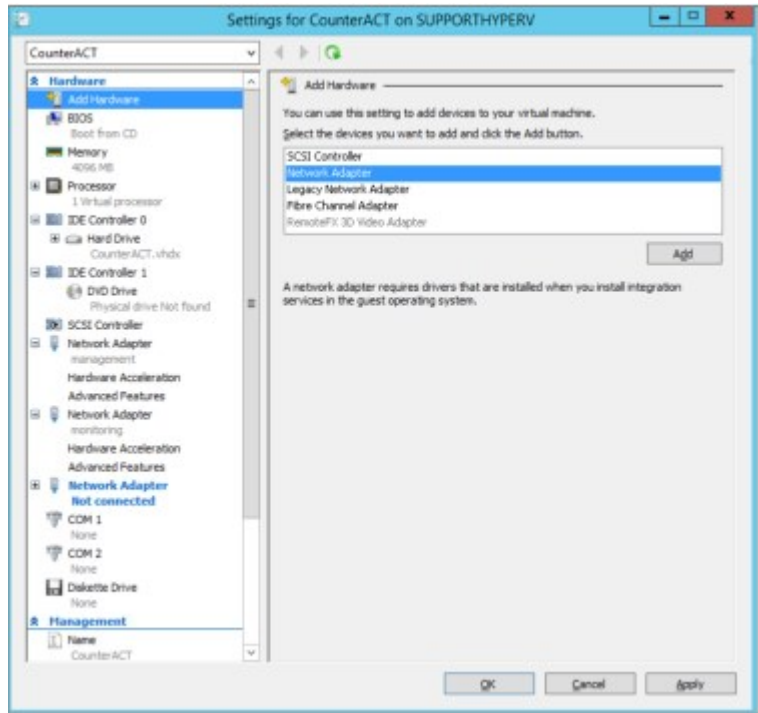
The following table shows the mapping between the interfaces:

VM Interface	Forescout 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:

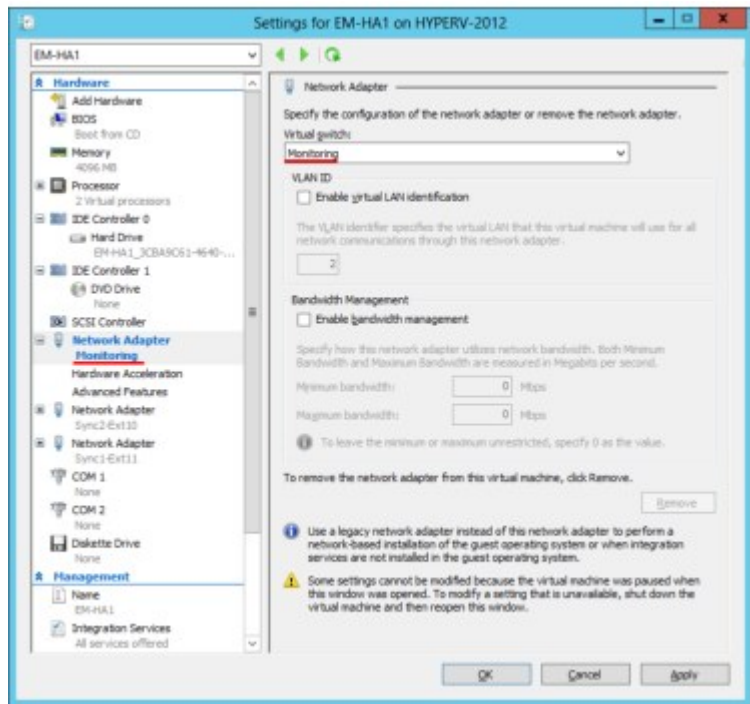
1. Select **Add Hardware** from the Virtual Machine Settings window.
2. Select **Network Adapter** and then select **Add**.



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**.

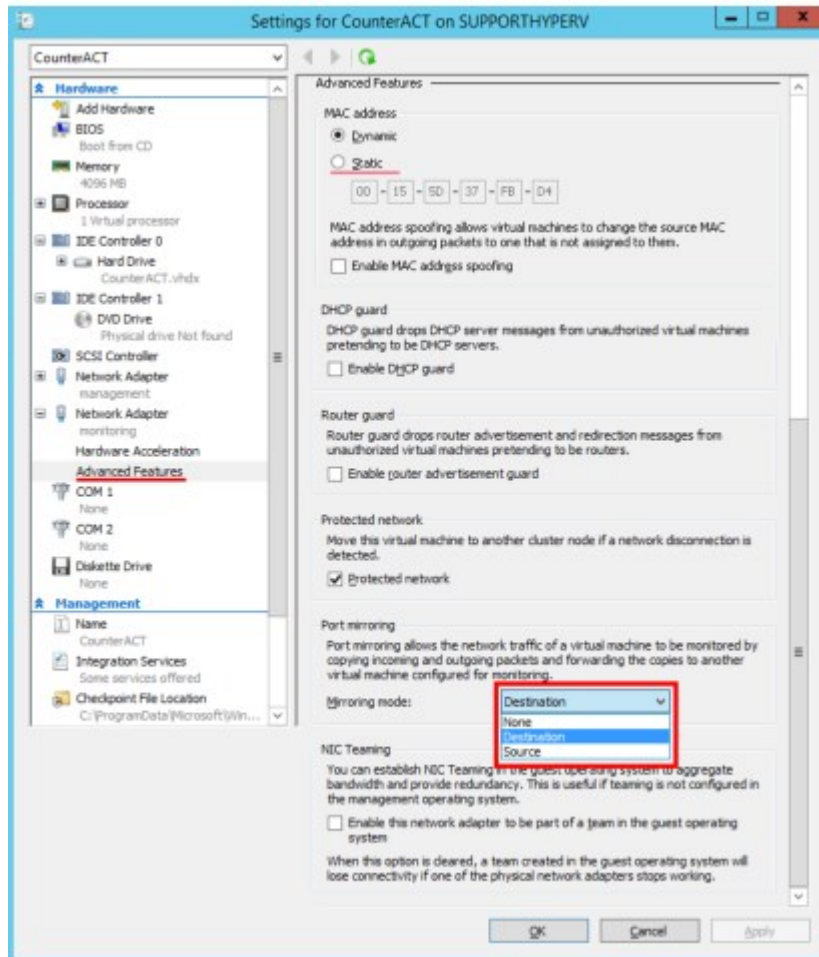


Virtual Machine Settings – Virtual Switch

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

Configure Hyper-V to Work with Forescout Devices

By default, Hyper-V 2012 R2 / 2016 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 the Forescout platform to respond to network traffic. Manually configure Hyper-V to operate in Promiscuous mode for the Forescout platform to fully monitor and respond to this traffic.

Configure 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
```

Configure 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 Forescout Console for the Monitor interface must be set to monitor **All Traffic** or **All Tagged Traffic**. Refer to [Working with Appliance Channel Assignments](#) in the **Forescout Administration Guide** for more information.

To configure VLAN filter settings:

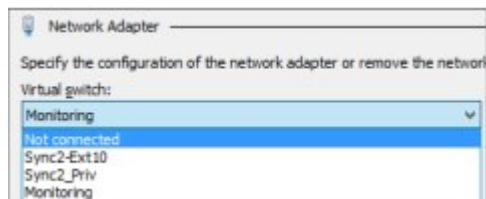
1. Run the following PowerShell cmdlet:

```
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>]
```

Automate Forescout Deployment in Hyper-V Environments


This topic provides information regarding how to automate Forescout deployment in Hyper-V environments. The automation process involves preparing a newly installed version of Forescout for template creation, creating a template using the Hyper-V Manager and then deploying the template using Hyper-V and an fstool command line.

Forescout 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 Forescout 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 Forescout 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. Run the following command:
`fstool conf --template`
This command prepares the Forescout platform 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 [Failover Clustering](#) in the **Resiliency Solutions User Guide** for more information.

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

3. 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.

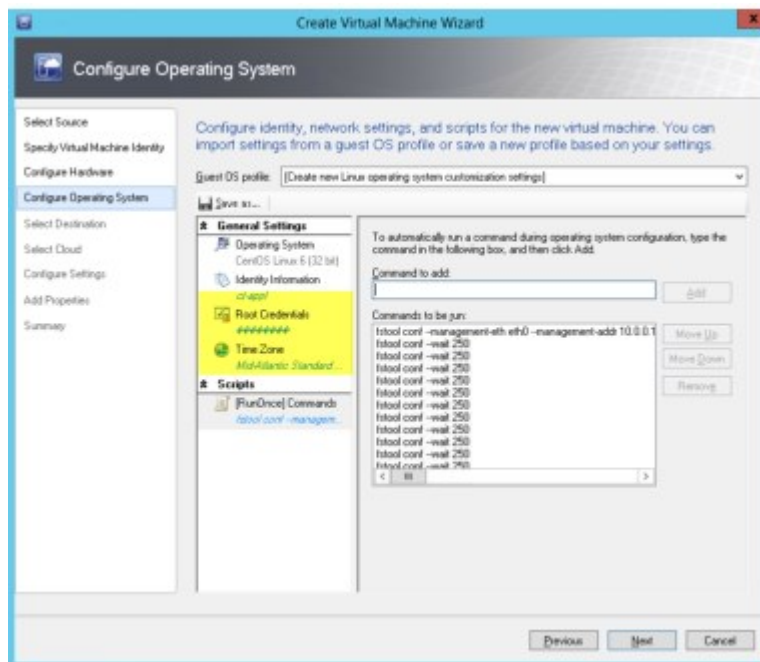
When a deployed High Availability Standby node machine is created, the Active node should be running to allow the Standby node to synchronize with it.

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).
- Run `fstool ha_setup --ha_reset` on the active node (primary) before you deploy the secondary. This command enables to fetch the initial HA configuration for a new node, limited for a period of 10 minutes.
- 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 (Flexx Licensing Mode). The licensing installation workflow is identical to the standard procedure for virtual Appliances. See [Install a Virtual License](#) for details.

Setup Notes

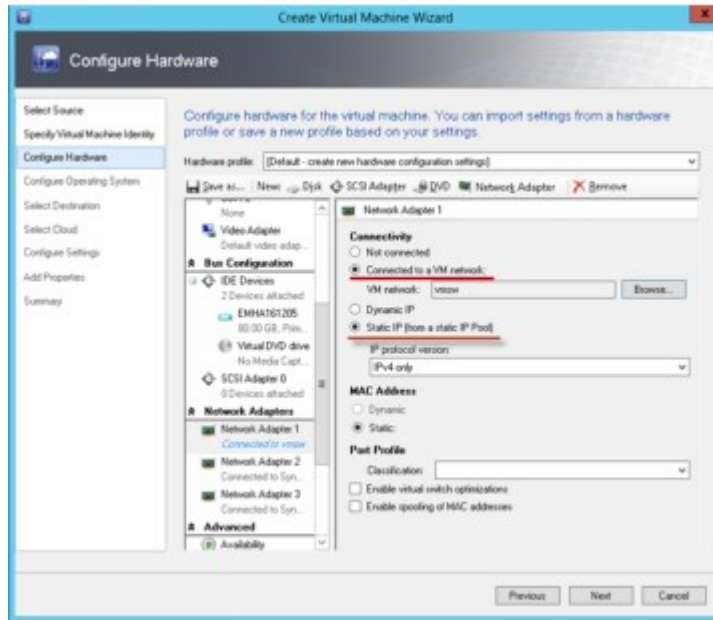
When creating/deploying the template:

- 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.

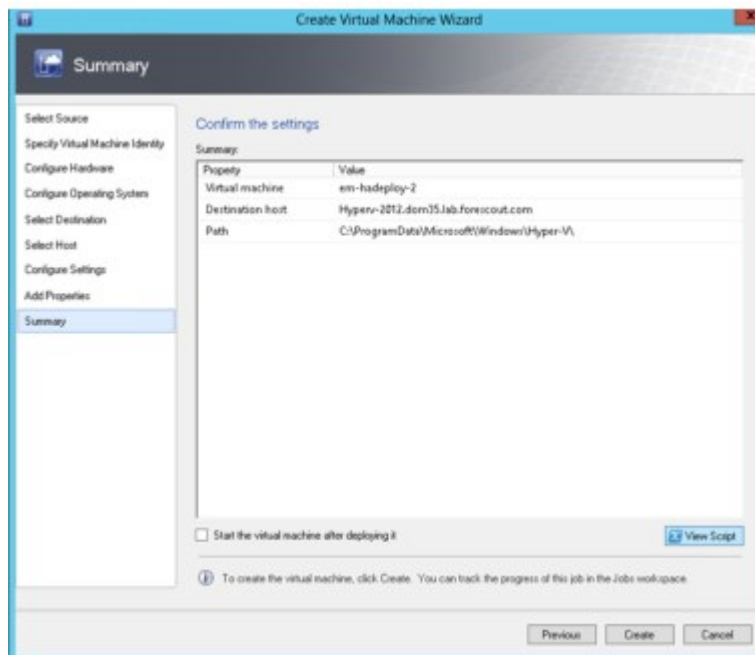
Configuration Recommendations

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.



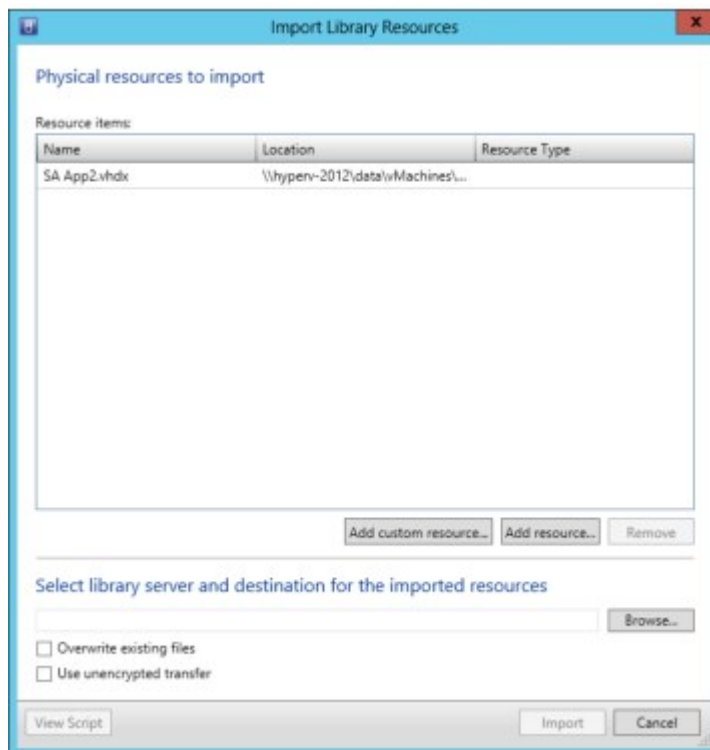
Configuration Recommendations
Save and Reuse the Original Script



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

 Forescout supports SCVMM using scvmmguestagent 1.0.2.1075.

FStool Samples for Automated Deployments

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

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

Single Setup

```
--management-eth management_interface
--management-addr management_address
--management-gw default_gateway_address
--hostname hostname
```

```
--management-netmask management_netmask (optional)
--domain domain (optional)
--dns dns_server_address (optional)
```

Single Sample

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

Primary High Availability Setup

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

Primary High Availability Sample

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

(x14)

Secondary High Availability Setup

```
--ha-secondary  
--ha-sync-eth-primary sync_interface_primary  
--ha-sync-subnet sync_subnet
```

Secondary High Availability Sample

```
fstool conf --ha-secondary  
--ha-sync-eth-primary eth3  
--ha-sync-subnet 172.17.2  
fstool conf --wait 250
```

(x14)

KVM Virtual Systems

This section describes how to deploy the Forescout platform on KVM virtual systems.

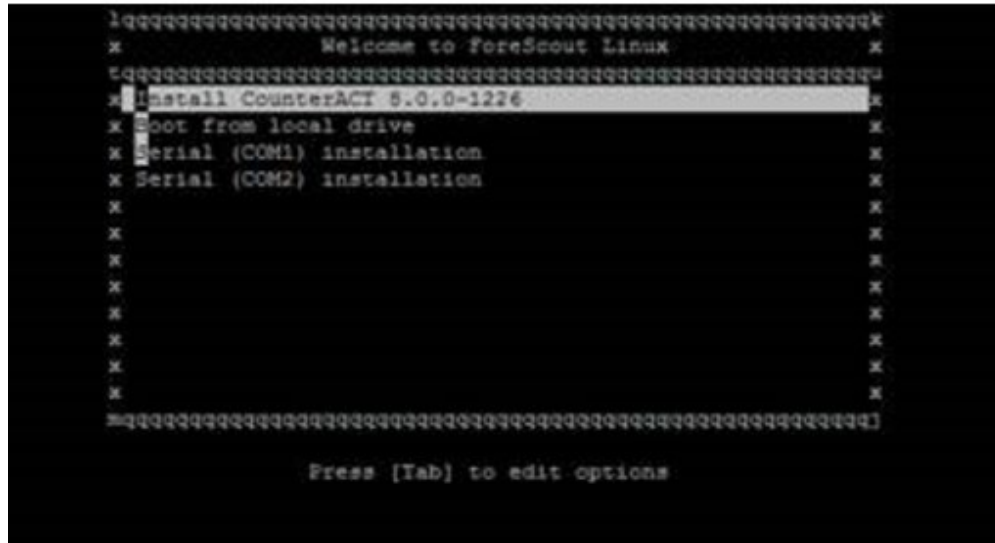
Supported Operating Systems

For information about the vendor models (hardware/software) and versions (product/OS) that are validated for integration with this Forescout component, refer to the [Forescout Compatibility Matrix](#).

Deploy the Forescout Platform on a KVM virtual system

To deploy on a KVM virtual system:

1. Obtain the Forescout 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 Forescout 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 **Install Forescout 8.3-<build number>** and press **Enter**.
14. Continue with Forescout installation and configuration described in [Configure an Appliance](#) and [Configure the Enterprise Manager](#).

Configure a Forescout Virtual Device

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](#)

After configuring the Forescout virtual devices, enhance the security of your deployment by controlling users ability to perform a **root** user log in, via SSH, to Forescout devices (Enterprise Manager and Appliances), whether physical devices or virtual devices. See [Control Use of Root User Log In to Forescout Devices](#).

Configure the Virtual Enterprise Manager and Appliances

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

Forescout device host name	
Forescout admin password	
Management interface	
Appliance IP address	
Network mask	
Default gateway IP address	

DNS domain name	
DNS server addresses	

To configure the Forescout device:

1. Start the Forescout virtual device.
2. Open SSH to the machine.
Forescout <version>-<build> options:

- 1) Configure Forescout Device
- 2) Restore saved Forescout 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 [Configure an Appliance](#) and [Configure the Enterprise Manager](#) for details.

Cloned Forescout Devices

If you cloned a Forescout 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. The Forescout platform 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.

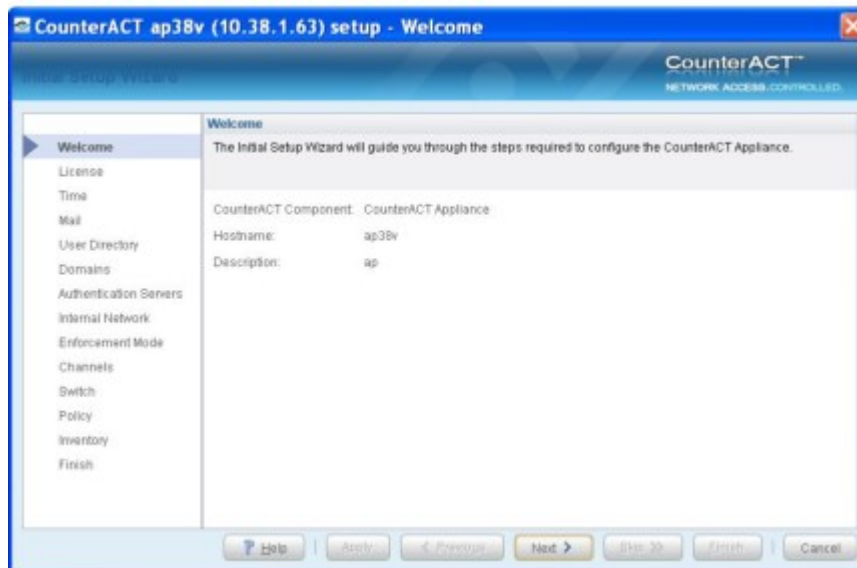
Install the Console

See [Install and Log in to the Forescout Console](#).

 If you are using Per-Appliance Licensing Mode, acquire and save the demo license files on the machine that will run the 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 the Forescout platform is up-and-running quickly and efficiently.



Initial Setup Wizard – Welcome Page

Refer to [Working with the Initial Setup Wizard](#) in the **Forescout Administration Guide** for more information.


Before You Begin

Before working with the Wizard:

- If you are using Per-Appliance Licensing Mode, prepare the location of the demo license files received from your Forescout representative.
- Fill in the table that appears in [Information Required Before You Install the Console](#).

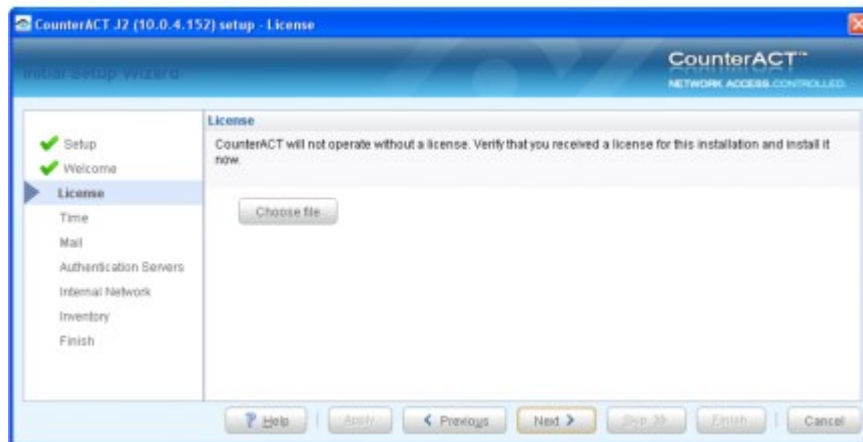
Install a Demo License (Per-Appliance Licensing Mode Only)

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

 *If you are using Flexx Licensing Mode, license installation is performed later, after the Initial Setup Wizard is complete.*

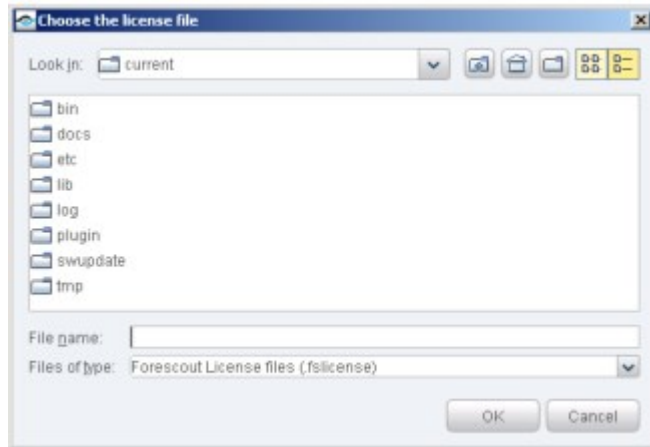
To install a demo license:

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



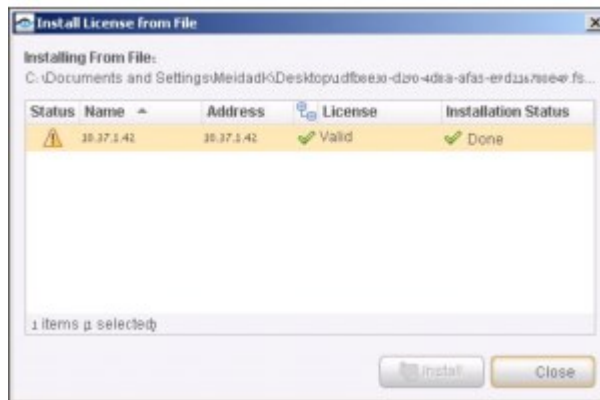
Initial Setup Wizard – License Page

2. The Choose the license file dialog box opens.



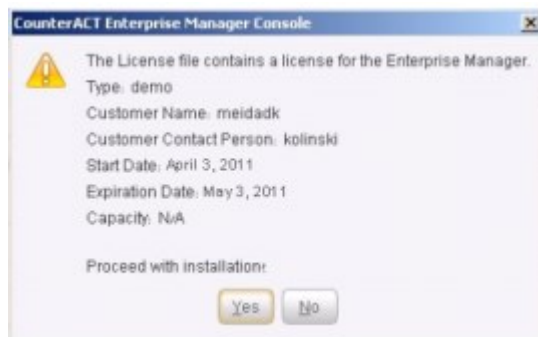
Choose the License File Dialog Box

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)

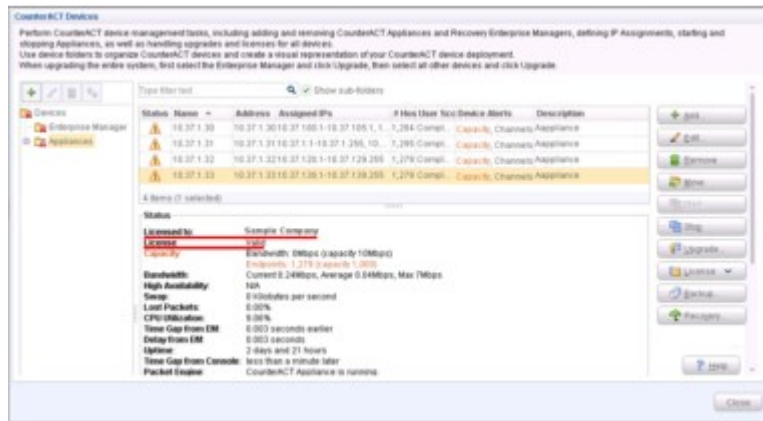
The license feature is designed to meet the needs of users working in Virtual IT environments, including environments that require a proxy server. This feature ensures that virtual users are working with authorized, secure and protected licenses.

 *If are you using Flexx Licensing Mode, all licensing-related procedures for virtual systems are identical to those for physical systems. Refer to [the Flexx Licensing How-to Guide](#) for information on Flexx licensing.*

Demo Virtual License

After installing a virtual Appliance, you must install the demo license you received from your Forescout 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 Forescout 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 [Per-Appliance CounterACT Device License](#) in the **Forescout Administration 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 Forescout 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 Forescout 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 Policy Manager](#) in the **Forescout Administration Guide**.

License Capacity per Forescout Virtual System Image

You can install several licenses for each Forescout 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

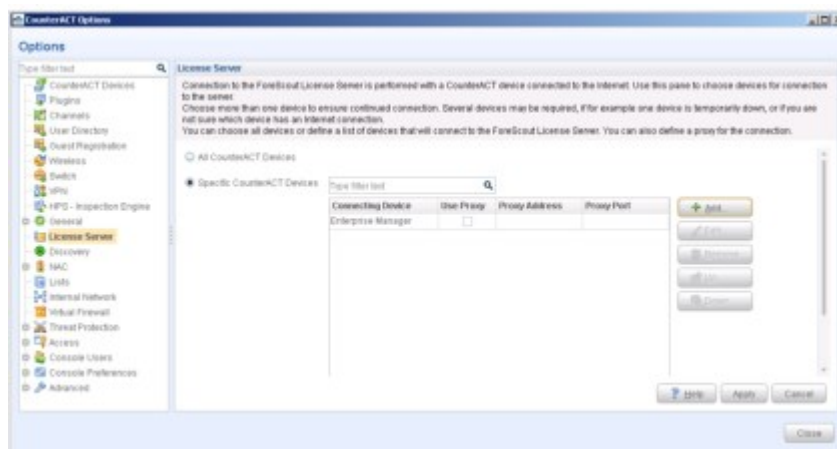
Connection to the Forescout License server is performed via a Forescout device connected to the Internet. By default, the Forescout platform assumes that all devices are connected.

License authorization requests are sent to the Forescout License (at <https://license2.forescout.com>) server via port 443 (HTTP-Secure –TLS based).

At least one Forescout 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.

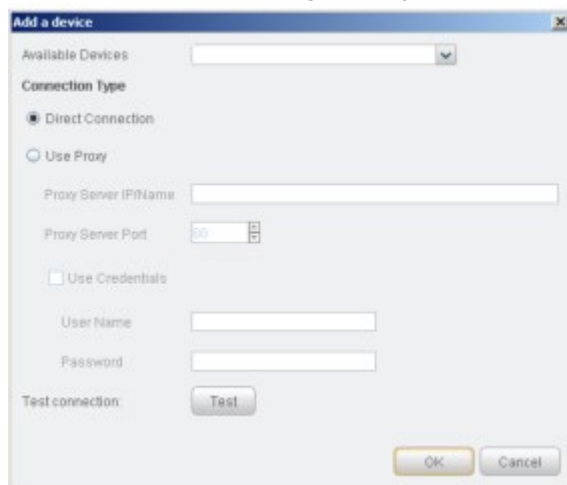
To specify a device to connect to the Forescout License server:

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.

Duplicate a Virtual Device

If you are using **Per-Appliance Licensing Mode**, you can duplicate a virtual device that does not have a Forescout 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 **Flexx 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:

- 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.

Move a Virtual Device to a New Server

You can 'move' a Forescout virtual device to a new virtual server by using the Forescout backup and restore features.

To move a licensed Forescout (CounterACT) device:

1. Back up the Forescout (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.

Forescout Platform Cloud Deployments

This section covers the following topics:

- [Forescout Platform Cloud Strategies and Best Practices](#)
- [Install Forescout Platform in the AWS Cloud](#)
- [Install Forescout Platform in the Microsoft Azure Cloud](#)

Forescout Platform Cloud Strategies and Best Practices


Forescout Enterprise Managers and Appliances can be deployed either on-premises, or in the cloud.

For hybrid (cloud-based / on-premises) solutions, VPN infrastructure must be deployed between the premises and the cloud. The VPN infrastructure can be a native VPN gateway, or a proprietary VPN service, such as **Amazon AWS Direct Connect** or **Microsoft Azure ExpressRoute** (depending on your service provider).

- Our recommended best practices to optimize functionality and minimize costs are to keep Appliances near the assets (devices and switches) with which they interact. So deploy as follows:
 - Use cloud-based Appliances to manage cloud-based assets.
 - Use on-premises Appliances to manage on-premises assets.
 - Use a mixture of cloud-based and on-premises Appliances to manage hybrid assets.
 - Use focal and dedicated Appliances close to the third-party applications with which they interact.

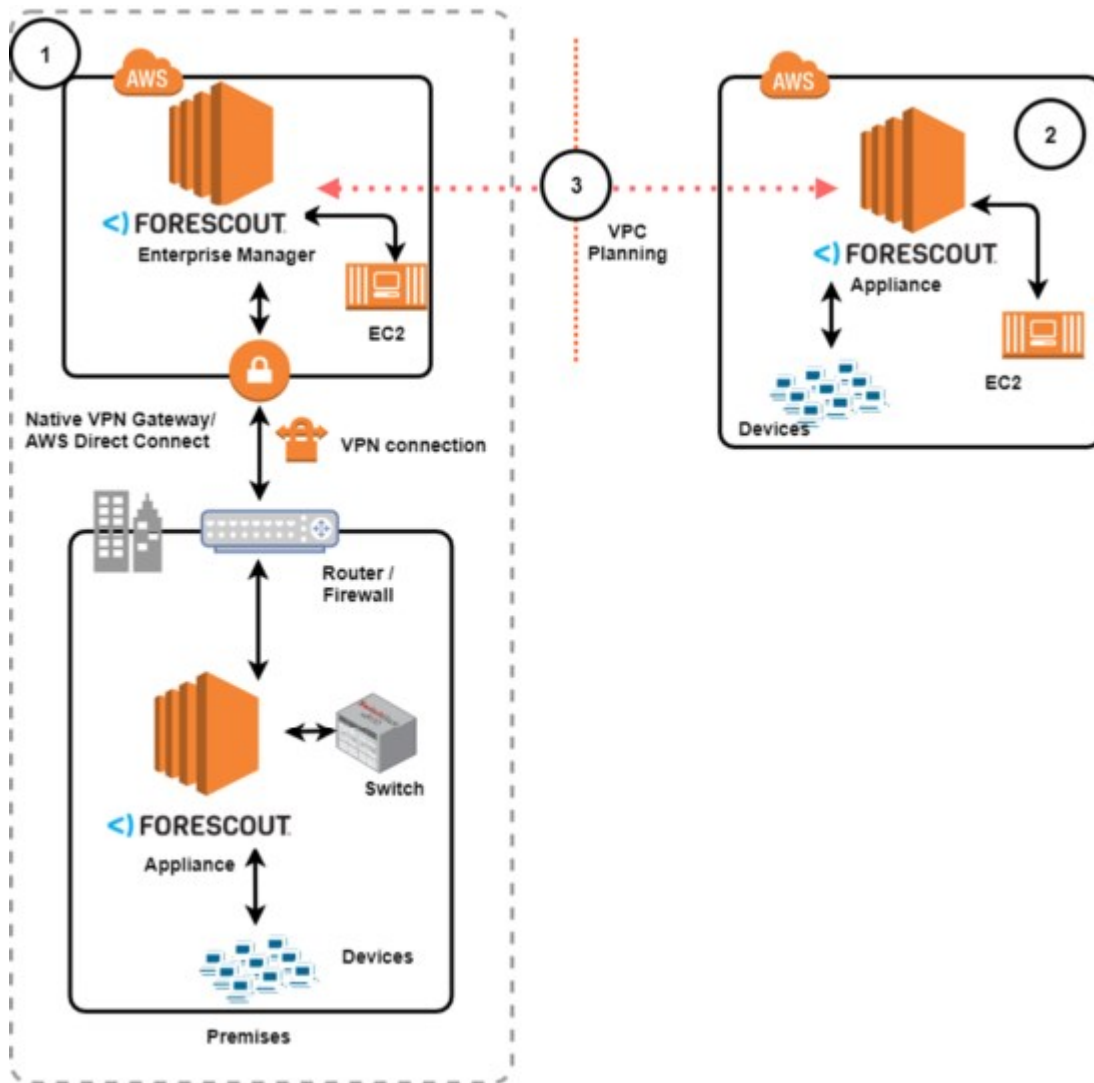
Use Cases

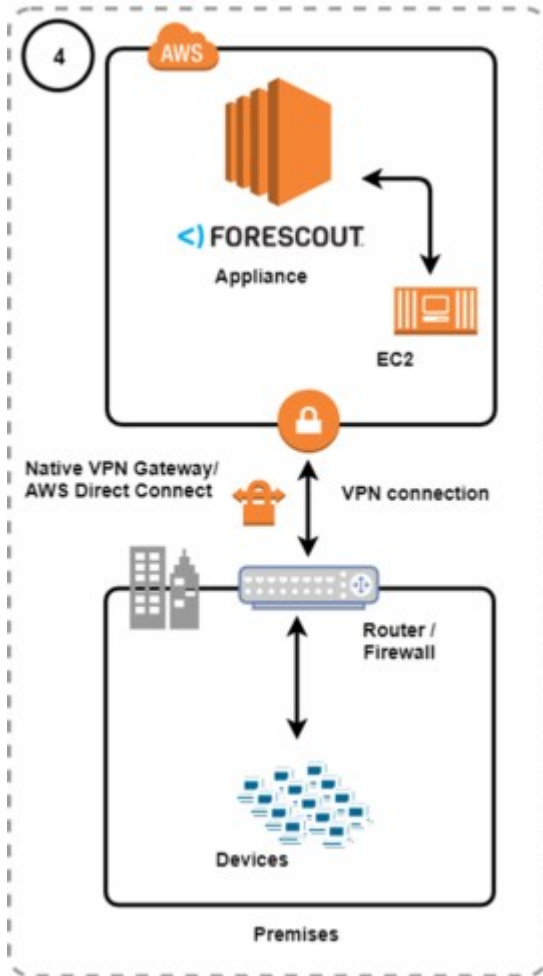
The table and diagrams below summarize several implementations (use cases).

 *These use cases are applicable to Amazon AWS and Microsoft Azure.*

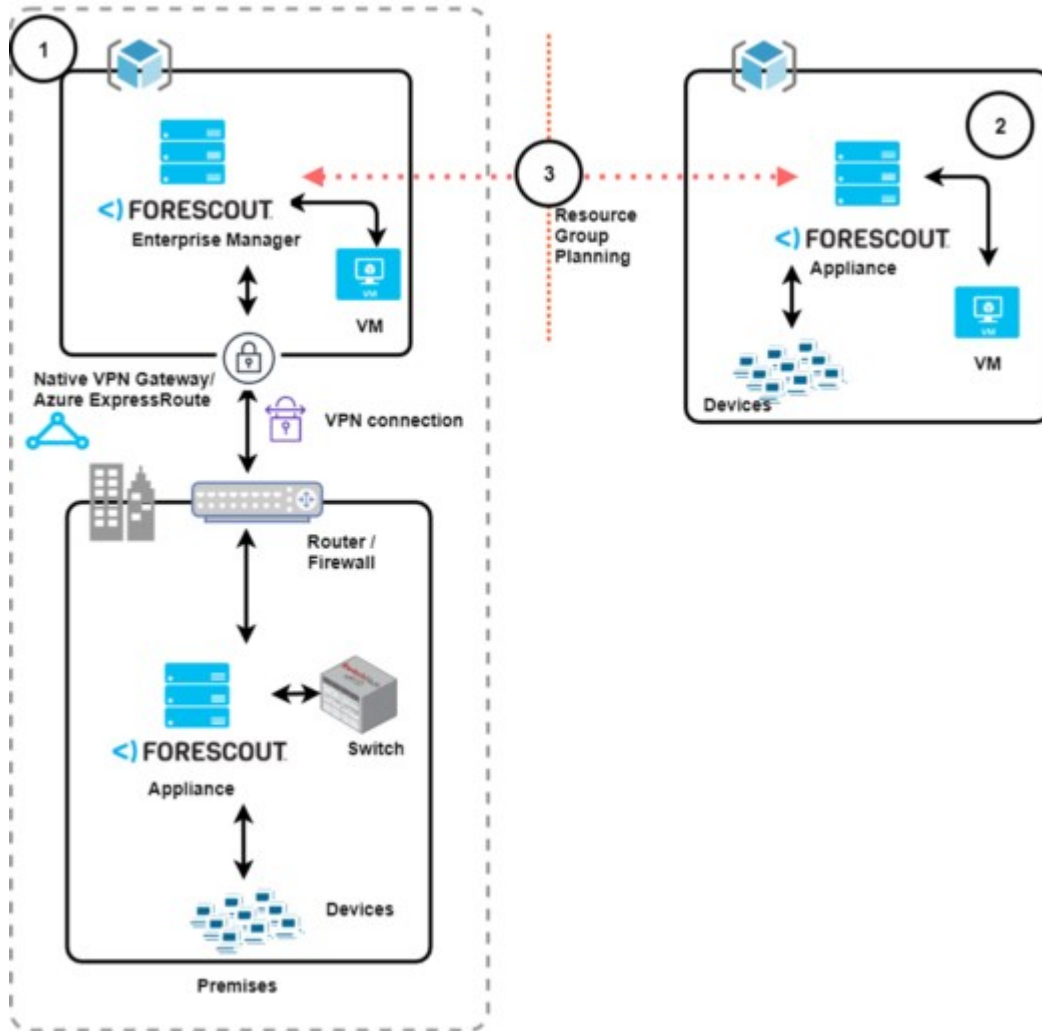
Use Case	Cloud Collateral	On-premises Collateral	Connectivity
1	Enterprise Manager	Appliance, switches, and devices	VPN connection (VPN Gateway and Router / Firewall)
2	Appliance and devices	N/A	N/A
3	Enterprise Manager, Appliance, and devices	Appliance, switches, and devices	AWS VPC / Azure Resource Group planning for connection
4	Appliance	Devices	VPN connection (VPN Gateway and Router / Firewall)

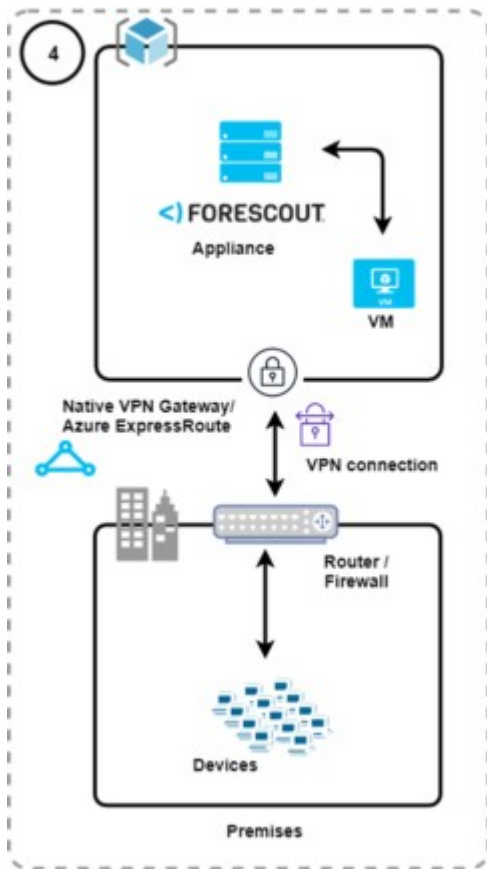
AWS Implementations





Azure Implementations





Limitations and Considerations

The same general considerations apply, whether the system is a purely cloud-based implementation, a centralized on-premises implementation, or a hybrid (cloud and on-premises) implementation.

Issues that specifically apply to cloud or hybrid implementations are noted in the following list:

- For communication between an Enterprise Manager and Appliances deployed over multiple regions, you need to ensure connectivity between them.
- If the Appliances are deployed in the cloud, SPAN traffic is not supported. There is no device discovery or classification via SPAN.
- If devices are deployed in the cloud, virtual firewall and hijacking (such as guest login) are not supported.
- Forescout supports 802.1x when an Appliance is deployed in the cloud, but the switch and the devices are deployed on- premises.
- Resiliency:
 - High Availability is not supported:

>	Between two cloud-based Appliances
>	Between a cloud-based Appliance and an on-premises Appliance.

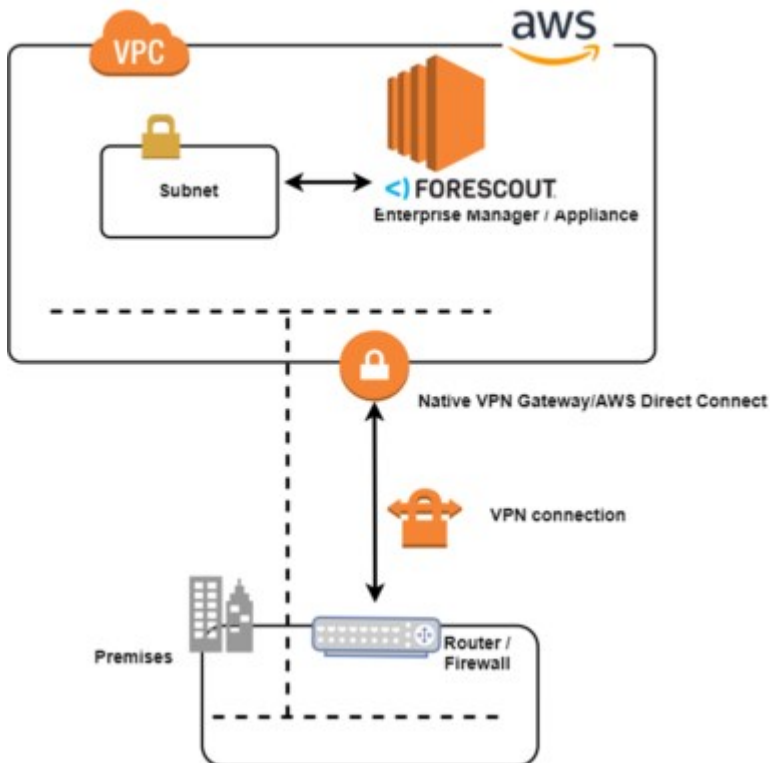
- Enterprise Manager Recovery is supported:
 - > Between two cloud-based Enterprise Managers.
 - > Between a cloud-based Enterprise Manager and an on-premises Enterprise Manager.
- Failover Clustering is not supported for cloud-based deployments.
- Bandwidth considerations: Certain Enterprise Manager and Appliance actions, together with data acquisition, can consume significant bandwidth, and incur high AWS maintenance costs:
 - If Appliances are deployed in the cloud, avoid the transfer of vulnerability updates to the devices.
 - If the Enterprise Manager is in the cloud, and the Appliance is on-premises:
 - > Forescout version upgrades from the cloud to premises can lead to relatively high traffic load.
- When Appliances are deployed in the cloud, take traffic communication between Appliances, switches, and devices, into account.

Performance Specifications

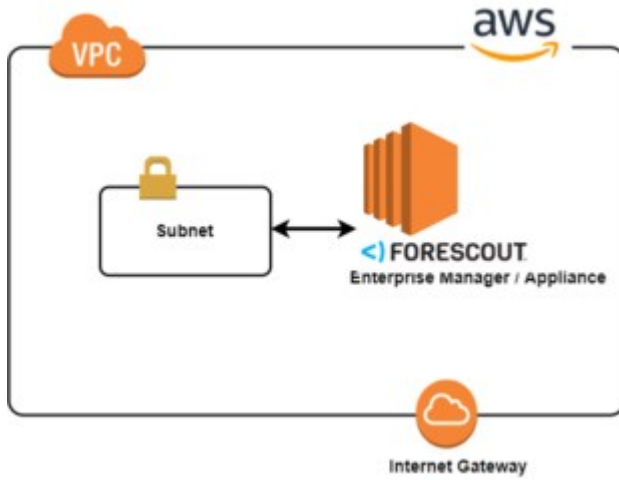
For the tested performance specifications for AWS / Azure small, medium, and large deployments, refer to the [Licensing and Sizing Guide](#).

AWS Solution Architecture

The following diagram presents the solution architecture for an existing Amazon AWS VPC:

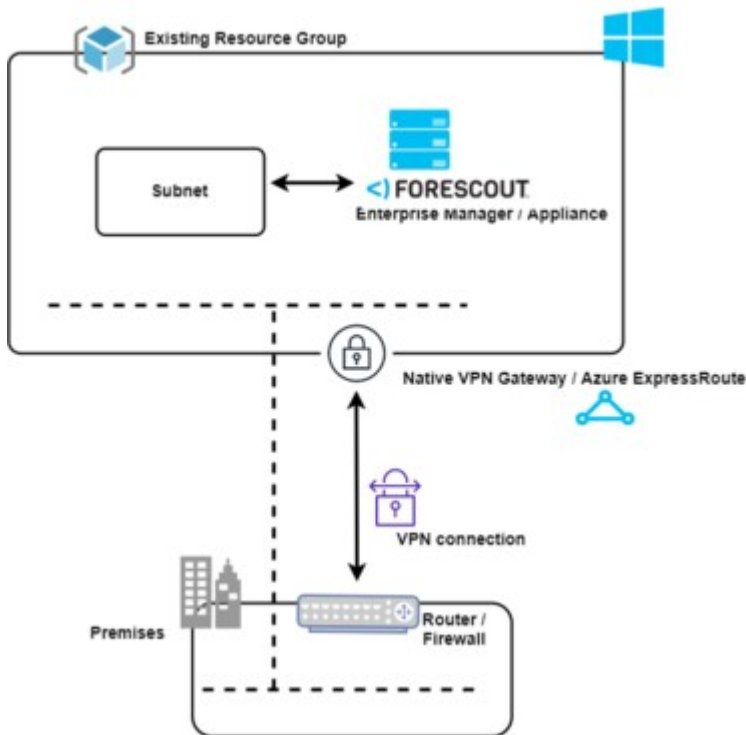


The following diagram presents the solution architecture for a new Amazon AWS VPC:

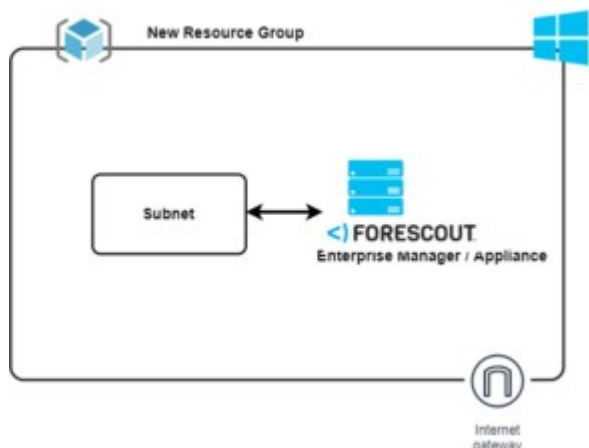


Azure Solution Architecture

The following diagram presents the solution architecture for an existing Microsoft Azure Resource Group:



The following diagram presents the solution architecture for a new Microsoft Azure Resource Group:



Install Forescout Platform in the AWS Cloud

Installation Pre-requisites and Important Information

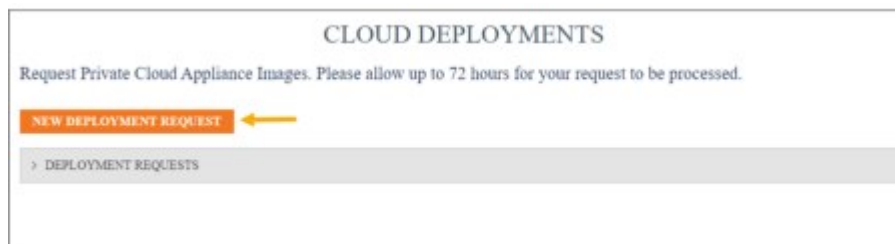
- Amazon AWS Account. Account ID (Number) from credentials file that you received from Amazon when you set up your user account
 - **Access to Forescout Customer Support Portal** <https://Forescout.force.com/support/>
- For an existing VPN in hybrid cloud solutions with managed on-premises Appliances / devices, verify that you have a site-to-site mesh between the on-premise terminator and the VPN gateway or AWS Direct Connect on the VPC. For more information, see the AWS Site-to-Site VPN User Guide at https://docs.aws.amazon.com/vpn/latest/s2svpn/VPC_VPN.html*
- The license policy for the site is BYOL. Additional EC2 billing depends on the instance type.*
- If you need to activate plugins that require ports other than HTTPS 443, SSH 22, HTTP 80 or Forescout Console 13000, you will need to make changes to the Security Group associated with the installed instance.*

Installation Procedure for AWS Customer Cloud

This section applies to AWS customers who need to install in their organization's cloud.

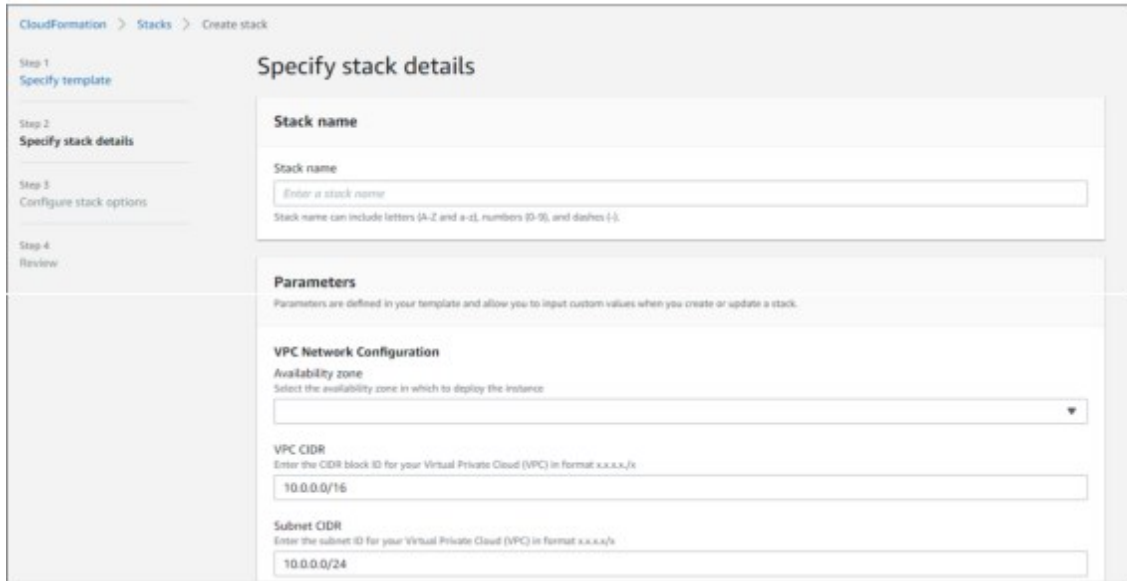
To install the Forescout platform in the AWS Customer Cloud:

1. Access the **Customer Support Portal** <https://Forescout.force.com/support/>
 - a. Navigate to the **Licenses** page.
 - b. **Scroll down to the Cloud Deployments** area.



2. Select **New Deployment Request**.

3. Enter your **AWS Account ID (Number)**, and select at least one **AWS Region**.
4. Select **Submit**. Your request is added to the **Deployment Requests** list.
5. You will receive an email from your Forescout Account Manager (this may take up to seventy-two hours) with the following attached AWS deployment templates:
 - **New VPC-deployment template**: Use to deploy Forescout platform on a new VPC
 - **Existing VPC-deployment template**: Use to deploy Forescout platform on an existing VPC.
6. Save the templates on your system.
7. In the AWS Management Console, open the required template (for **New VPC** or **Existing VPC**) in **All Services > Management & Governance > CloudFormation > Stacks > Create stack**.



8. Specify the stack details, which consist of VPC Network configuration parameters and Forescout-specific parameters.
- These are the VPC network configuration parameters you need to configure. The list contains information about using an existing VPC and setting up a new VPC.

Stack name	Enter a unique stack name. You can include letters (A-Z and a-z), numbers (0-9), and dashes (-).
VPC CIDR	Select an existing VPC ID in your Virtual Private Cloud (VPC) OR For a new VPC, enter a new CIDR block ID in format x.x.x.x/cidr
Availability zone	Select the availability zone in which to deploy the gateway.
Subnet CIDR	The eth0 interface receives the entered IP address. Select the subnet ID for your existing Virtual Private Cloud (VPC) OR For a new VPC, enter the subnet ID for your Virtual Private Cloud (VPC) in format x.x.x.x/x
Security Group ID	For existing VPC only: Select the list of security group IDs to use for accessing the EC2 instances.
Resources prefix name	(optional) Enter a prefix for the names of created resources.


- These are the Forescout-specific configuration parameters you need to configure. The list contains information about using an existing VPC and setting up a new VPC.

Enterprise Manager or Appliance	Select the type of Forescout deployment (Enterprise Manager or Appliance).
Hostname	Enter the hostname.
Appliance IP Address	The eth1 interface is static and requires manual IP configuration. Enter a valid IP address from the Subnet CIDR. Note: The selected IP address must be outside the range of the first three IP addresses: <ul style="list-style-type: none"> ▪ First IP reserved for the default gateway ▪ Second IP reserved for the DNS

	<ul style="list-style-type: none"> Third IP reserved for future use <p>For example, in subnet with CIDR block 10.0.0.0/24, you cannot use 10.0.0.1, 10.0.0.2, or 10.0.0.3</p>
Domain name	(optional) For a New VPC only: Enter a valid FQDN.
Admin password	Enter your Administrator password (16 characters, must include at least one upper-case letter (A-Z), one lower-case letter (a-z), one number (0-9) and one special character (#\$%^&*(!)).
DNS Server	(optional) For a New VPC only: The DNS configuration is received via DHCP, so that there is no DNS configuration via the console. Enter a valid FQDN or IP address. Note: If you do not enter information here, Amazon will use a default IP address.
Instance Model	Select the size of the instance model.
Admin Access IP	For a New VPC only: Enter the IP address range to use for SSH, HTTPS and console to the EC2 instances, in the format x.x.x.x/x

After entering all required values, click **Next**.

- Configure the stack options, and then select **Next**.

 Refer to the online AWS CloudFormation documentation for information about the stack options. https://docs.aws.amazon.com/cloudformation/?id=docs_gateway

Review the parameters you previously selected and/or entered, and then select **Create stack** to complete the procedure.

To verify successful installation:


- Verify that the EC2 displays the instance. You can connect to the Enterprise Manager/ Appliance from the instance.
Username is cliadmin

After configuring the Forescout virtual devices, enhance the security of your deployment by controlling users ability to perform a **root** user log in, via SSH, to Forescout devices (Enterprise Manager and Appliances), whether physical devices or virtual devices. See [Control Use of Root User Log In to Forescout Devices](#).



Install Forescout Platform in the Microsoft Azure Cloud

Installation Pre-requisites and Important Information

- Microsoft Azure Account. Account ID from credentials file that you received from Azure when you set up your user account
- Access to Forescout Customer Support Portal** (<https://Forescout.force.com/support/>)

 For an existing VPN in hybrid cloud solutions with managed on-premise appliances/ devices, verify that you have a site-to-site mesh between the on-premise terminator and the VPN gateway or Azure ExpressRoute on the Resource Group. For more information, see [Create a VPN Gateway and add a Site-to-Site connection using PowerShell at https://](#)

docs.microsoft.com/en-us/azure/vpn-gateway/scripts/vpn-gateway-sample-site-to-site-powershell

-  The license policy for the site is BYOL. Additional billing depends on the instance type.
-  If you need to activate plugins that require ports other than HTTPS 443, SSH 22, HTTP 80 or Forescout Console 13000, you will need to make changes to the resource group associated with the installed instance.


Installation Procedure for Azure Cloud

To install the Forescout Platform in the Azure cloud:

1. Access the **Customer Support Portal** <https://Forescout.force.com/support/>
 - a. Navigate to the **Licenses** page.
 - b. **Scroll down to the Cloud Deployments** area.

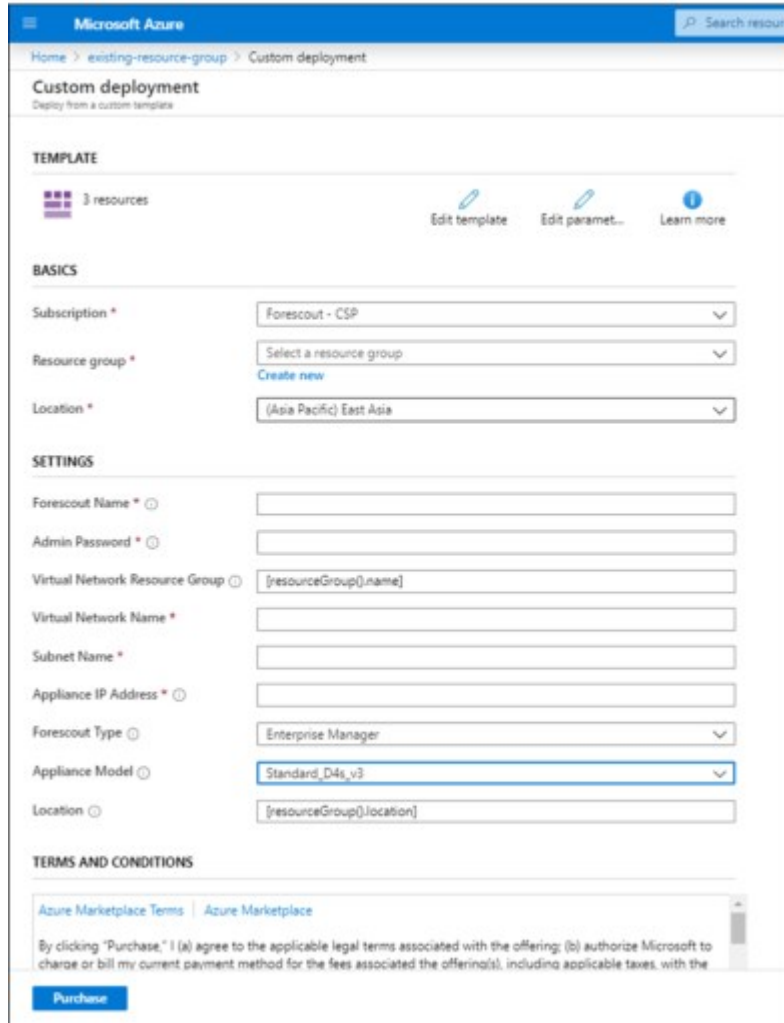


2. Select **New Deployment Request**.



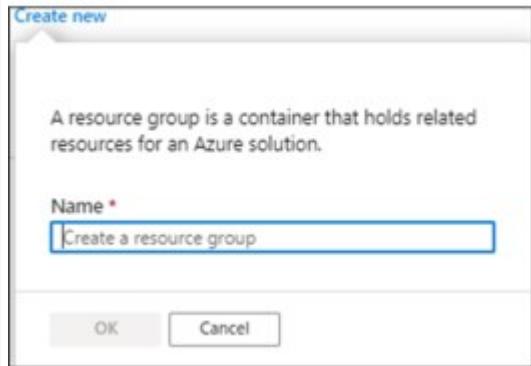
3. Enter your **Azure Subscription ID**.
4. Select **Submit**. Your request is added to the **Deployment Requests** List.
5. You will receive an email from your Forescout Account Manager (this may take up to seventy-two hours) with the following attached Azure deployment templates:
 - **New Resource Group-deployment template**: Use to deploy Forescout platform on a new Resource Group.
 - **Existing Resource Group-deployment template**: Use to deploy Forescout platform on an existing Resource Group.

6. Save the templates on your system.
7. In the Microsoft Azure Marketplace, open the required template (for **New Resource Group** or **Existing Resource Group**) in **Home > Templates > Existing / New Resource Group / Deploy / Custom deployment page**.



8. On the Custom deployment page: Specify details in the Basics and Forescout-specific (Settings) areas.
 - a. These are the basic deployment parameters you need to configure. The list contains information about using an existing resource and setting up a new resource.

Subscription	Enter a unique subscription name. You can include letters (A-Z and a-z), numbers (0-9), and dashes (-).
Resource group	Select an existing resource group, or to create a new one, select create new.



Enter the name for the new resource group, and then select OK.

Location	Select the location.
<p>b. These are the Forescout-specific configuration parameters (Settings) you need to configure. The list contains information about using an existing resource and setting up a new resource.</p>	
Forescout Name	Enter the Forescout machine name.
Admin Password	Enter your Admin password, same as for Forescout console and ssh login
Unique DNS Name	New template only: Enter a unique DNS name for the public IP address used to access the virtual machine.
Address Prefix	New template only: Enter the virtual network IP address in the format x.x.x.x/x
Subnet CIDR	New template only: Enter the internal subnet CIDR in format x.x.x.x/cidr
Virtual Network Resource Group	Existing template only: Enter the resource group in which the virtual network is deployed.
Virtual Network Name	Existing template only: Enter the name of the virtual network.
Subnet Name	Existing template only: Enter the name of the subnet.
Appliance IP Address	The eth1 interface is static and requires manual IP configuration. Enter a valid IP address from the subnet cidr.
Admin Access IP	New template only: enter the IP address range to use for SSH, HTTPS, and console, to the virtual machine instances, in the format x.x.x.x/x
DNS Servers	New template only (optional): Enter a valid list of FQDNs or IP addresses. Enter the IP addresses in format: ["DNS1","DNS2" ...] "x.x.x.x"
Forescout Type	Select the type of Forescout deployment (Enterprise Manager or Appliance).
Appliance Model	Select the Forescout machine type. For example, Standard_A4
Location	Enter the location for the resource group. The default location is identical to that selected in the Basics area of the template.

- Accept the Azure Marketplace terms and conditions, and then select **Purchase**. After configuring the Forescout virtual devices, enhance the security of your deployment by controlling users ability to perform a **root** user log in, via SSH, to

Forescout devices (Enterprise Manager and Appliances), whether physical devices or virtual devices. See [Control Use of Root User Log In to Forescout Devices](#).

Appendix A - Site Preparation Form

This appendix lists the Forescout 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	Forescout 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 Forescout Console or Forescout Enterprise Manager	
	Allowed addresses for Forescout Console or Forescout Enterprise Manager connectivity	
	Addresses of hosts allowed to control the Forescout platform through SSH	

Subject	Item	Possible Values
Communication Equipment	Communication equipment to which the Forescout platform 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	

Appendix B - Limited Appliance Mode

This appendix covers topics about Limited Appliances and Limited Appliance Mode.

About Limited Appliance Mode

Forescout interim release 8.2.1 introduced the Limited Appliance mode. Due to memory limitations, the 5110 and CT-R series Appliances do not fully support Forescout platform releases 8.2.x – 8.3. For customers owning CT-R or 5110 hardware, the Limited Appliance mode is available to enable on these Forescout hardware devices. Enabling this mode provides a subset of Forescout plugins that run on the Appliance and provide their Forescout eyeSight and eyeControl capabilities.

The enabled Limited Appliance mode for Forescout platform release 8.3 provides the following Forescout plugins:

- DHCP Classifier
- DNS Client
- Device Classification Engine
- Device Profile Library
- HPS Agent Manager
- HPS Inspection Engine
- Hardware Inventory
- Linux
- NBT Scanner
- NIC Vendor DB
- Packet Engine
- Syslog
- Switch
- User Directory
- VMware vSphere
- Wireless
- eyeExtend for ServiceNow

Install a Limited Appliance

To install a Limited Appliance:

1. Power on the Appliance. The Main menu appears.
Forescout <version number> Options:
 - 1) **Configure Forescout Lite Appliance**
 - 2) **Restore saved Forescout configuration**
 - 3) **Identify and renumber network interfaces**
 - 4) **Configure keyboard layout**
 - 5) **Turn machine off**

6) Reboot the machine

Choice (1-6) : 1

2. Type **1** to configure the Limited (Lite) Appliance. The setup process initializes.

```
>>>>> The Forescout platform Initial Setup <<<<<<
```

```
You are about to setup the Forescout platform. 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 continue the setup from the
Forescout Console.
```

```
Continue? (yes/no) [yes]
```

3. Type **Yes**.


 If you select No, the Limited Appliance installation process terminates.

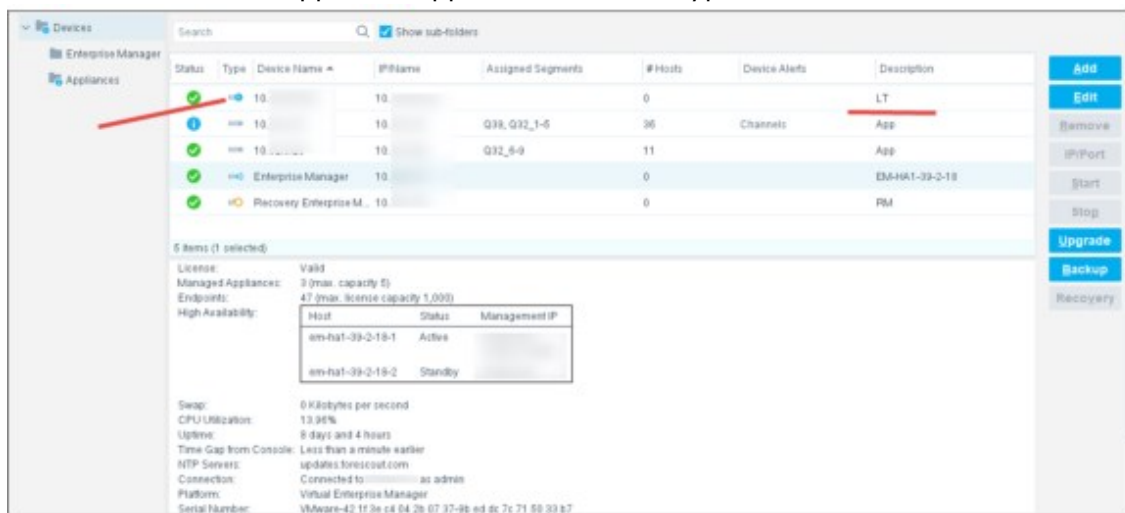
The rest of the installation process is identical to that for [Configure an Appliance](#).

Identify a Limited Appliance in the Console

To identify a Limited Appliance in the Console:

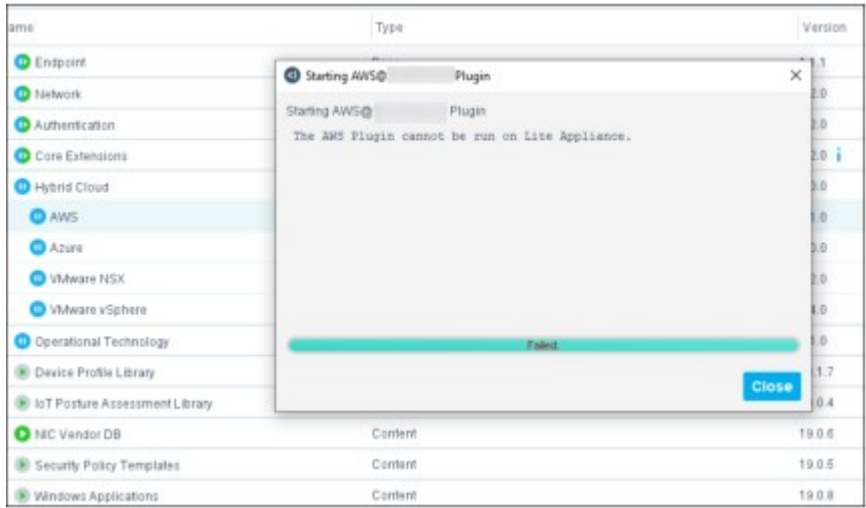
- Select **Tools > Options**.

A Limited Appliance appears with a  Type icon.



Plugin Incompatibility and Limited Appliance

If you attempt to run a plugin that is not provided by the Limited (Lite) Appliance mode, the following error message appears:



Appendix C - Inter-Enterprise Manager and Appliance Authentication

The Forescout platform ensures secure communication between Enterprise Managers and Appliances through customer issued CA certificates. Customers can generate certificate sign requests to a CA Service and import the signed certificate, and its certificate chains for each Enterprise Manager and Appliance.

This section describes how to:

- [Create a Certificate Sign Request](#)
- [Import a Signed Certificate](#)
- [Configure Certificate Verification Enforcement](#)

Create a Certificate Sign Request

Create a certificate sign request for each Enterprise Manager and Appliance.

To create a certificate sign request:

1. Per Enterprise Manager and Appliance, log in to its command-line interface (CLI).
2. Run the following command:

```
fstool replace_certificate --cert-req > <filename>
```

Send the request to the appropriate Certificate Authority to have it signed.

Import a Signed Certificate

After receiving the signed certificates, import them to their corresponding Enterprise Manager or Appliance.

To import a signed certificate

1. Per Enterprise Manager and Appliance, log in to its command-line interface (CLI).
2. Run the following command:

```
fstool replace_certificate --import --server-cert <certificate-file> --ca-cert-chain <ca-chain-file>
```

Configure Certificate Verification Enforcement

Disabled by default, certificate verification enforcement can be enabled using the `fs.enforce.cert.verify` property. Once enabled, the Forescout platform requires signed certificates of both existing and future Enterprise Managers and Appliances.

After importing a signed certificate on each Enterprise Manager and Appliance, enable certificate enforcement.

To enable certificate enforcement:

1. On the Enterprise Manager, log in to its command-line interface (CLI).
2. Run the following commands:

```
fstool set_property fs.enforce.cert.verify true  
fstool service restart
```

To disable certificate enforcement:

1. On the Enterprise Manager, log in to its command-line interface (CLI).
2. Run the following commands:

```
fstool set_property fs.enforce.cert.verify false  
fstool service restart
```