



# Fore Scout

## Quick Installation Guide

Single Appliance

**Version 8.2.1**



## Contact Information

Forescout Technologies, Inc.

190 West Tasman Drive

San Jose, CA 95134 USA

<https://www.Forescout.com/support/>

Toll-Free (US): 1.866.377.8771

Tel (Intl): 1.408.213.3191

Support: 1.708.237.6591

## About the Documentation

- Refer to the Technical Documentation page on the Forescout website for additional documentation: <https://www.Forescout.com/company/technical-documentation/>
- Have feedback or questions? Write to us at [documentation@forescout.com](mailto:documentation@forescout.com)

## Legal Notice

© 2020 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.

2020-07-30 16:59

# Table of Contents

<b>Welcome to Version 8.2.1 .....</b>	<b>5</b>
Forescout Package Contents .....	5
<b>Overview .....</b>	<b>6</b>
<b>1. Create a Deployment Plan .....</b>	<b>6</b>
Decide Where to Deploy the Appliance .....	6
Appliance Interface Connections.....	6
Management Interface .....	6
Monitor Interface.....	9
Response Interface.....	9
<b>2. Set up your Switch .....</b>	<b>11</b>
A. Switch Connection Options .....	11
1. Standard Deployment (Separate Management, Monitor and Response Interfaces) .....	11
2. Passive Inline Tap.....	11
3 Active (Injection-Capable) Inline Tap .....	12
4 IP Layer Response (for Layer-3 Switch Installations) .....	12
B. Switch Setting Notes.....	12
VLAN (802.1Q) Tags .....	12
Additional Guidelines .....	13
<b>3. Connect Network Cables and Power On.....</b>	<b>14</b>
A. Unpack the Appliance and Connect Cables .....	14
B. Record the Interface Assignments .....	14
C. Power on the Appliance.....	15
<b>4. Configure the Appliance .....</b>	<b>16</b>
<b>5. Remote Management.....</b>	<b>20</b>
iDRAC Setup.....	20
Enable and Configure the iDRAC Module.....	20
Connect the Module to the Network .....	23
Login to iDRAC.....	23
<b>6. Verify Connectivity .....</b>	<b>24</b>
Verify the Management Interface Connection .....	24
Perform a Ping Test .....	24
<b>7. Set Up the Forescout Console.....</b>	<b>25</b>
Install the Console.....	25
Log In.....	25
Perform Initial Setup .....	26
Before You Start the Initial Setup .....	27

<b>8. Configure Inter-Enterprise Manager and Appliance Authentication.....</b>	<b>28</b>
Create a Certificate Sign Request .....	28
Import a Signed Certificate.....	28
Configure Certificate Verification Enforcement.....	28
 <b>Additional Forescout Documentation.....</b>	 <b>29</b>
Documentation Downloads .....	29
Documentation Portal .....	30
Forescout Help Tools.....	30

# Welcome to Version 8.2.1

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.

***This guide describes the installation for a single stand-alone CounterACT Appliance preinstalled with version 8.0. Some Appliances may come***

***preinstalled with a later version. To use version 8.2.1, follow an approved upgrade path, outlined in the upgrade path matrix, in the Installation Guide.***



■ Due to memory limitations, 5110 and CT-R series Appliances do not fully support version 8.2.1. However, you can install the Limited Appliance package (with limited plugin functionality) for version 8.2.1 on your 5110 and CT-R series Appliances. For more information, see the Installation Guide for this version.

For more detailed information or information about upgrade or about deploying multiple Appliances for enterprise-wide network protection, refer to the *Forescout Installation Guide* and *Forescout Administration Guide*. See [Additional Forescout Documentation](#) for information on how to access these guides.

Additionally, you can navigate to the support website located at: <http://www.forescout.com/support> for the latest documentation, knowledge base articles, and updates for your Appliance.

## Forescout Package Contents

Your Forescout package includes the following components:

- The CounterACT Appliance
- Front Bezel
- Rail Kits (Mounting brackets)
- Power cord(s)
- DB9 Console connecting cable (for serial connections only)
- Enterprise Products Safety, Environmental, and Regulatory Information
- Getting Started document (CT-xxxx Appliances based on hardware revision 5x and Forescout 51xx Appliances only)

# Overview

Perform the following to set up your Forescout deployment:

- [1. Create a Deployment Plan](#)
- [2. Set up your Switch](#)
- [3. Connect Network Cables and Power On](#)
- [4. Configure the Appliance](#)
- [5. Remote Management](#)
- [6. Verify Connectivity](#)
- [7. Set Up the Forescout Console](#)

## 1. Create a Deployment Plan

Before performing the installation, decide where to deploy the Appliance and learn about Appliance interface connections.

### Decide Where to Deploy the Appliance

Selecting the correct network location where the Appliance will be installed is crucial for a successful deployment and optimal performance. The correct location will depend on your implementation goals and network access policy. The Appliance needs to be able to monitor the traffic that is relevant to your policy. For example, if your policy depends on monitoring authorization events from endpoints to corporate authentication servers, the Appliance needs to be installed so that it sees endpoint traffic flowing into authentication server(s).

For more information about installation and deployment, refer to the *Forescout Installation Guide*. See [Additional Forescout Documentation](#) for information on how to access this guide.

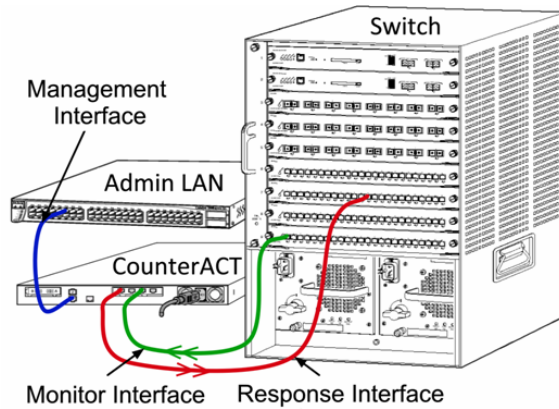
### Appliance Interface Connections

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

#### 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.



### Network Access Requirements

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.

Port	Service	To or From the Forescout Platform	Function
161/UDP	SNMP	From	Allows the Forescout platform to communicate with network switches and routers. For information about configuring SNMP, refer to the <i>Forescout Administration Guide</i> .
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 <i>Forescout Administration Guide</i> .
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. <i>SecureConnector</i> is a script-based agent that enables management of Linux endpoints while they are connected to the network.
10003/TCP	SecureConnector for Windows	To	Allows SecureConnector to create a secure (encrypted TLS) connection to the Appliance from Windows machines. <i>SecureConnector</i> is an agent that enables management of Windows endpoints while they are connected to the network. Refer to the <i>Forescout Administration Guide</i> for more information about SecureConnector. When SecureConnector connects to an Appliance or to the Enterprise Manager, it is redirected to the Appliance to which its host is assigned. Ensure this port is open to all Appliances and to the Enterprise Manager to allow transparent mobility within the organization.



Port	Service	To or From the Forescout Platform	Function
10005/TCP	SecureConnector for OS X	To	Allows SecureConnector to create a secure (encrypted TLS) connection to the Appliance from OS X machines. <i>SecureConnector</i> is an agent that enables management of OS X endpoints while they are connected to the network. Refer to the <i>Forescout Administration Guide</i> for more information about SecureConnector.  When SecureConnector connects to an Appliance or to the Enterprise Manager, it is redirected to the Appliance to which its host is assigned. Ensure this port is open to all Appliances and to the Enterprise Manager to allow transparent mobility within the organization.
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.

## 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.

When two switches are connected as a redundant pair, the Appliance must monitor traffic from both switches.

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.

## 2. Set up your Switch

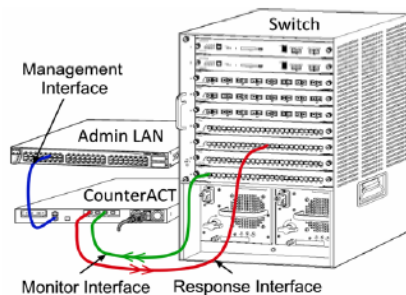
### A. Switch Connection Options

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.

Several options are available for connecting the Appliance to your switch.

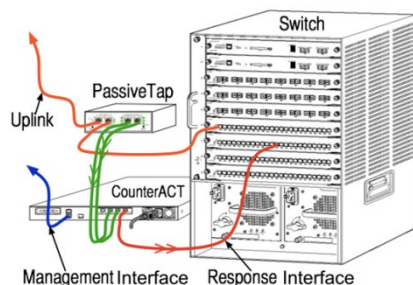
#### 1. Standard Deployment (Separate Management, Monitor and Response Interfaces)

The recommended deployment uses three separate ports. These ports are described in [Appliance Interface Connections](#).



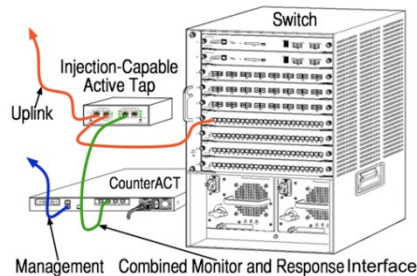
#### 2. Passive Inline Tap

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.



### 3 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.



### 4 IP Layer Response (for Layer-3 Switch Installations)

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.

## B. Switch Setting Notes

### 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

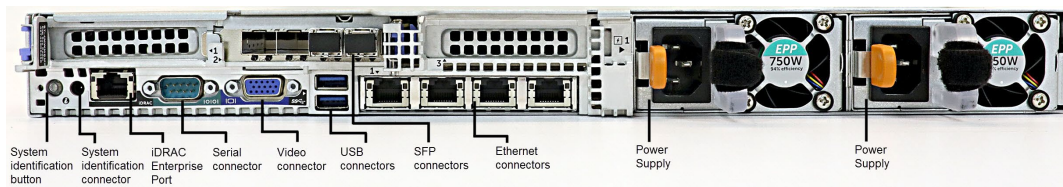
- In the following cases, you should mirror just one interface (that does allow transmit/receive):
  - If the switch cannot mirror both transmitted and received traffic
  - If the switch cannot mirror all the switch traffic
  - If the switch cannot mirror all the traffic over a VLAN
- Verify that you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

### 3. Connect Network Cables and Power On

#### A. Unpack the Appliance and Connect Cables

1. Remove the Appliance and power cable from the shipping container
2. Remove the rail kit you received with the Appliance.
3. Assemble the rail kit on the Appliance and mount the Appliance to the rack.
4. Connect the network cables between the network interfaces on the Appliance rear panel and the switch ports.

##### **Rear Panel Sample – CounterACT Device**



You can replace Forescout-supplied SFPs with Finisar SFPs that have been tested and approved by Forescout. Refer to the *Forescout Installation Guide* for more details.

#### B. Record the Interface Assignments

After completing the Appliance installation at the data center and installing the Forescout Console, you will be prompted to register interface assignments. These assignments, referred to as *Channel definitions*, are entered in the Initial Setup Wizard that opens when you first log on to the Console.

Record the physical interface assignments below and use them when completing the Channel setup at the Console.

Eth Interface	Interface Assignment (e.g. Management, Monitor, Response)
Eth0	
Eth1	
Eth2	
Eth3	
Eth4	
Eth5	
Eth6	
Eth7	

## C. Power on the Appliance


1. Connect the power cable to the power connector on the Appliance rear panel.
2. Connect the other end of the power cable to a grounded AC outlet.
3. Connect the keyboard and monitor to the Appliance or set up the Appliance for serial connection. Refer to the *Forescout Installation Guide* for more information.
4. Power on the Appliance from the front panel.

## 4. Configure the Appliance

Prepare the following information before you configure the Appliance.

Appliance host name	
Forescout Admin password	Keep the password in a secure location
Management interface	
Appliance IP address	
Network mask	
Default Gateway IP address	
DNS Domain Name	
DNS server addresses	

After power on, you will be prompted to start configuration with the following message:

 *The following prompts are samples. Some Appliances may be preinstalled with a version that has slightly different prompts.*

```
CounterACT Appliance boot is complete.
Press <Enter> to continue.
```

1. Press **Enter**. If you have a Forescout 51xx Appliance, the following menu appears:

```
CounterACT <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) :1
```

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


- If you see CounterACT 7.0.0, you can either upgrade to or perform a fresh installation of version 8.0.0. Refer to the *Forescout Installation Guide* for details. After upgrade or installation to version 8.0.0, you will see the menu listed above.
- If you see CounterACT 8.0.0, the menu offers an option to install 7.0.0 or to configure 8.0.0, as shown below. If you select 7.0.0, you will not be able to reinstall 8.0.0 through the Configuration menu. See the *Forescout Installation Guide version 7.0.0* for details on configuring version 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) :
```

 *If the configuration is interrupted or if you selected the wrong version, you will need to reimage the Appliance with the relevant version of the ISO file. Refer to the Forescout Installation Guide for more information on reimaging an Appliance.*

**2. 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] :
```

**3. Type 1 (Standard Installation) 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):
```

**4. Type Yes and press Enter.**

 *The following prompt appears when running a clean installation.*

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

**5. Unless your organization needs to comply with Common Criteria and DoDIN APL certification, type No and press Enter.**

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

1) CounterACT Appliance
2) CounterACT Enterprise Manager

Choice (1-2) :
```


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

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

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

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

- 7.** 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 for help if you entered the wrong mode.

 *This option does not appear on Forescout 51xx Appliances.*

- 8.** 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 :
```

- 9.** Type a description and press **Enter**.

The following is displayed:


```
>>>>> 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 15 characters long and should  
contain at least one non-alphabetic character.
```

```
Administrator password :
```

- 10.** At the Set Administrator Password prompt, type the string that is to be your password (the string is not echoed to the screen) and press **Enter**. You are prompted to confirm the password. The password must be between 6 and 15 characters long and contain at least one non-alphabetic character.

 *Log in to the Appliance as cliadmin, and log in to the Console as admin.*

- 11.** At the Set Host Name prompt, type a host name and press **Enter**. The host name can be used when logging in to the Console, and is displayed at the Console to help you identify the CounterACT Appliance that you are viewing. The hostname should not exceed 13 characters.

- 12.** The Configure Network Settings screen prompts you for a series of configuration parameters. Type a value at each prompt and press **Enter** to display the next prompt.
- Forescout platform components communicate through management interfaces. The number of management interfaces listed depends on the Appliance model.

- The **Management IP address** is the address of the interface through which Forescout platform components communicate. Add a VLAN ID for this interface only if the interface used to communicate between Forescout platform 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 and internal addresses, 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.

**13.** The Setup Summary screen is displayed. You are prompted to perform general connectivity tests, reconfigure settings or complete the setup. Type **D** to complete setup.

### **License**

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

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

You will be alerted that your demo license is about to expire. Refer to the *Forescout Administration Guide* for more information about demo license alerts.

If you are working with a Forescout virtual system:

- The demo license is not installed automatically at this stage. You must install the demo license you received from your Forescout representative by email.
- At least one CounterACT device must be able to access the Internet. This connection is used to validate Forescout licenses against the Forescout License server. Licenses that cannot be authenticated for one month will be revoked. The Forescout platform will send a warning email once a day indicating there is a communication error with the server.

Refer to the *Forescout Installation Guide* for more information.

Refer to the *Forescout Administration Guide* for more information about license management in Per-Appliance licensing mode.

- If your Forescout deployment is operating in **Flexx Licensing Mode**, the *Entitlement administrator* should receive an email when the license entitlement is created and available in the Forescout Customer Portal. Once available, the *Deployment administrator* can activate the license in the Console. Until the license is activated, license enforcement will apply, and certain Console configuration changes may be restricted. *No demo license is automatically installed during system installation.*

Refer to the *Forescout Flexx Licensing How-to Guide* for more information.

## 5. Remote Management

### iDRAC Setup

The Integrated Dell Remote Access Controller (iDRAC) is an integrated server system solution that gives you location-independent/OS-independent remote access over the LAN or Internet to CounterACT Appliances. Use the module to carry out KVM access, power on/off/reset and perform troubleshooting and maintenance tasks.

Perform the following to work with the iDRAC module:

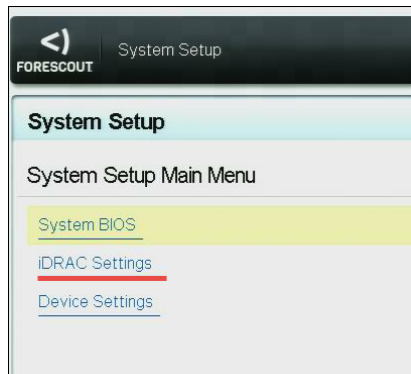
- [Enable and Configure the iDRAC Module](#)
- [Connect the Module to the Network](#)
- [Login to iDRAC](#)

### Enable and Configure the iDRAC Module

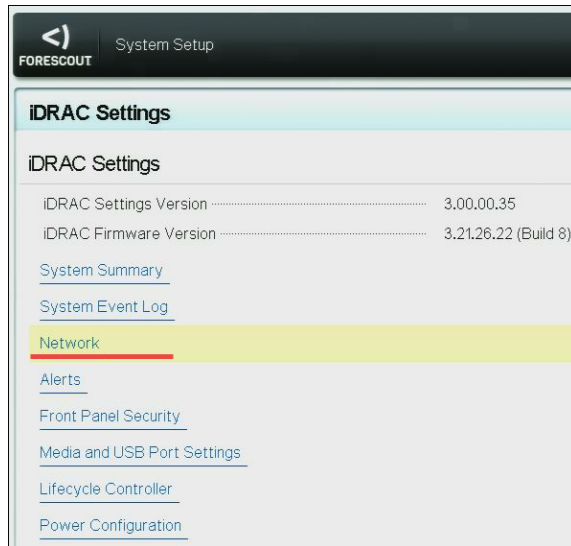
Change the iDRAC settings to enable remote access on the CounterACT device. This section describes basic integration settings required for working with the Forescout platform.

#### To configure iDRAC:

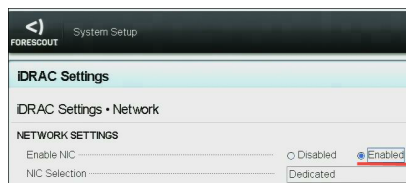
1. Turn on the managed Appliance.
2. Select F2 during the boot process.
3. In the System Setup Main Menu page, select **iDRAC Settings**.



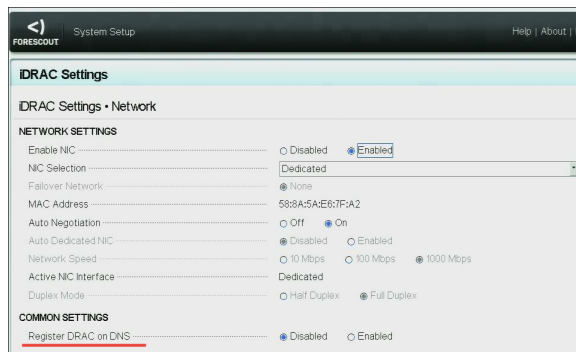
4. In the iDRAC Settings page, select **iDRAC Settings > Network**.



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:
- Set *Register iDRAC on DNS* to **Enabled**.
  - in the *DNS iDRAC Name* field, enter the dynamic DNS.



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

**iDRAC Settings**

iDRAC Settings • Network

**IPv4 SETTINGS**

Enable IPv4 .....	<input type="radio"/> Disabled <input checked="" type="radio"/> <b>Enabled</b>
Enable DHCP .....	<input checked="" type="radio"/> <b>Disabled</b> <input type="radio"/> Enabled
Static IP Address .....	192.168.1.109
Static Gateway .....	192.168.1.1
Static Subnet Mask .....	255.255.255.0
Use DHCP to obtain DNS server addresses .....	<input checked="" type="radio"/> <b>Disabled</b> <input type="radio"/> Enabled
Static Preferred DNS Server .....	192.168.1.2
Static Alternate DNS Server .....	0.0.0.0

- 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:**

**iDRAC Settings**

iDRAC Settings • User Configuration

User ID .....	2
Enable User .....	<input type="radio"/> Disabled <input checked="" type="radio"/> <b>Enabled</b>
User Name .....	root
LAN User Privilege .....	Administrator
Serial Port User Privilege .....	Administrator
Change Password .....	Press <Enter> to input

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:



## Login to iDRAC

**To log in to iDRAC:**

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

A screenshot of the iDRAC login web interface. The header shows 'Integrated Remote Access Controller 9' with sub-headers 'Forescout 5160 | Forescout | Enterprise'. Below this is a prompt: 'Type the User Name and Password and click Log In.' The login form contains fields for 'Username:', 'Password:', and 'Domain:' (with a dropdown menu currently showing 'This iDRAC'). A 'Log In' button is positioned below the fields. A security notice states: 'Security Notice: By accessing this computer, you confirm that such access complies with your organization's security policy.' At the bottom, there is a 'FORESCOUT' logo and links for 'Online Help | Support | About'.


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

For further information about iDRAC, refer to the *iDRAC User's Guide*. You can access this guide in the following location:

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

**To identify your licensing mode:**

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

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

## 6. Verify Connectivity

### 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>
```



## 7. Set Up the Forescout Console

### Install the Console

The Console is the Forescout management application used to view important detailed information about endpoints and control them. This information is collected by CounterACT devices. Refer to the *Forescout Administration Guide* for more information.

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
  - Linux RHEL/CentOS 7
  - macOS 10.12/10.13/10.14
- 2GB RAM
- 1GB disk space

The following method is available for performing the Console installation:

#### **Use the installation software built into your Appliance.**

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

After completing the installation, you can log in to the Console.

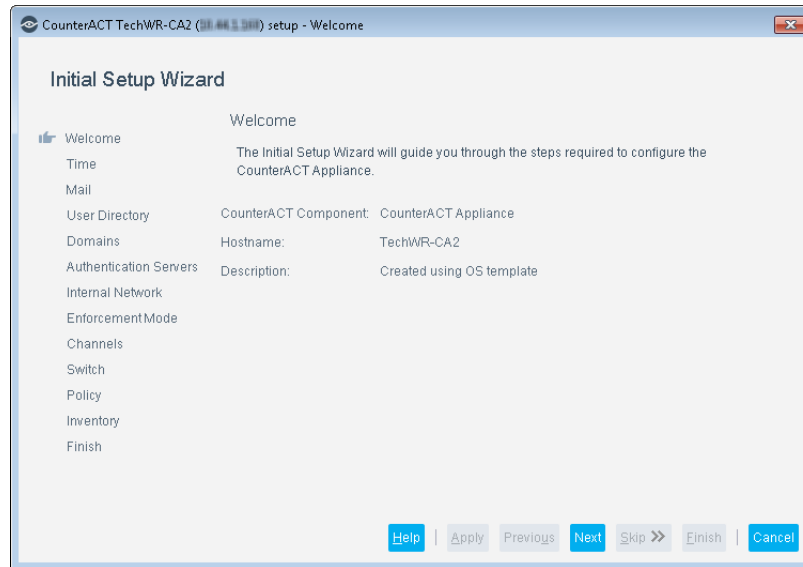
1. Select the Forescout icon from the shortcut location you created.

The image shows the login interface for ForeScout Version 8.2. It features a dark blue background with the ForeScout logo (a stylized white 'F' inside a circle) and the text 'FORESCOUT' and 'Version 8.2'. Below this, there are several input fields: 'IP/Name:' with a text box, 'Login Method:' with a dropdown menu currently showing 'Password', 'User Name:' with a text box containing 'admin', and 'Password:' with a text box. There is also a checkbox labeled 'Remember this address and user name' which is checked. At the bottom is a blue button labeled 'LOG IN'. A close button (X) is in the top right corner.

2. Enter the IP address or host name of the Appliance in the **IP/Name** field.
3. In the **User Name** field, enter admin.
4. In the **Password** field, enter the password you created during Appliance installation.
5. Select **Login** to launch the Console.

## Perform Initial Setup

When you log in for the first time, the Initial Setup Wizard opens. The Wizard guides you through essential configuration steps to get the ForeScout platform up and running quickly and efficiently.



## Before You Start the Initial Setup

Prepare the following information before you work with the Wizard:

---

### Information Required by Wizard

---

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

---

Refer to the *Forescout Administration Guide* or Online Help for information about working with the Wizard.

## 8. Configure 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
```

## Additional Forescout Documentation

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

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

### Documentation Downloads

Documentation downloads can be accessed from the [Technical Documentation Page](#), and from one of two Forescout portals, depending on which licensing mode your deployment is using.

- **Per-Appliance Licensing Mode** – [Product Updates Portal](#)
- **Flexx Licensing Mode** – [Customer Support Portal](#)

 *Software downloads are also available from these portals.*

**To identify your licensing mode:**

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

### Technical Documentation Page

The Forescout Technical Documentation page provides a link to the searchable, web-based [Documentation Portal](#), as well as links to a wide range of Forescout technical documentation in PDF format.

**To access the Technical Documentation page:**

- Go to <https://www.Forescout.com/company/technical-documentation/>

## Product Updates Portal

The Product Updates Portal provides product and documentation downloads for Forescout platform releases, Base Modules, Content Modules, and eyeExtend Modules. The portal also provides additional documentation.

### To access the Product Updates Portal:

- Go to <https://updates.forescout.com/support/index.php?url=counteract> and select the version you want to discover.

## Customer Support Portal

The Downloads page on the Forescout Customer Support Portal provides product and documentation downloads for Forescout platform releases, Base Modules, Content Modules, and eyeExtend Modules. Software and related documentation only appear on the Downloads page if you have a license entitlement for the software.

### To access documentation on the Customer Support Portal:

- Go to <https://Forescout.force.com/support/> and select **Downloads**.

## Documentation Portal

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

### To access the Documentation Portal:

- Go to [https://updates.forescout.com/support/files/counteract/docs\\_portal/](https://updates.forescout.com/support/files/counteract/docs_portal/)

## Forescout Help Tools

You can access individual documents, as well as the [Documentation Portal](#), directly from the Forescout Console.

### **Console Help Buttons**

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

### **Forescout Administration Guide**

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

### **Plugin Help Files**

- After the plugin is installed, select **Tools > Options > Modules**, select the plugin, and then select **Help**.

### **Content Module, eyeSegment Module, and eyeExtend Module Help Files**

- After the component is installed, select **Tools > Options > Modules**, select the component, and then select **Help**.

### **Documentation Portal**

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