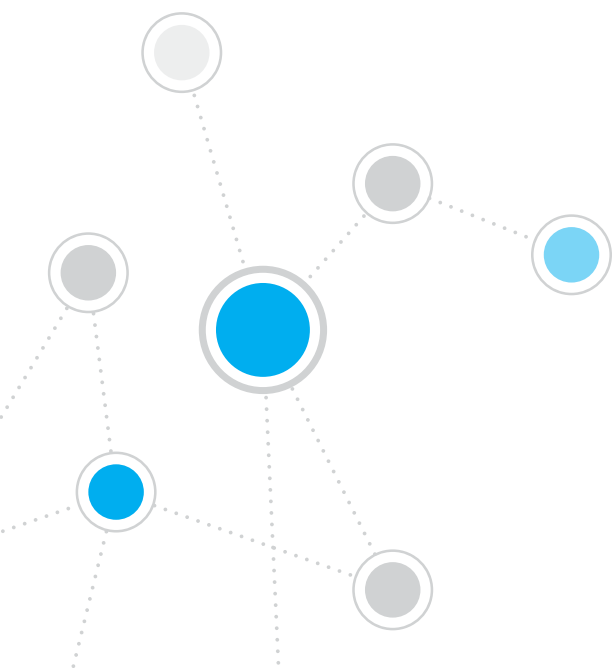




# ForeScout CounterACT<sup>®</sup> 7

Устройство CounterACT

**Краткое руководство по установке**



# Содержание

<b>Добро пожаловать в ForeScout CounterACT®, версия 7 .....</b>	<b>3</b>
В комплект CounterACT входит: .....	3
<b>Общие сведения.....</b>	<b>4</b>
<b>1. Разработка плана размещения .....</b>	<b>5</b>
Определить место размещения устройства.....	5
Подключение интерфейсов устройства .....	5
<b>2. Установка коммутатора .....</b>	<b>8</b>
А. Варианты подключения коммутатора .....	8
В. Примечания к установке коммутатора.....	9
<b>3. Подключение сетевых кабелей и включение питания.....</b>	<b>10</b>
А. Распаковка устройства и соединительных кабелей.....	10
В. Запись присваиваний интерфейса.....	11
С. Подача питания на устройство .....	11
<b>4. Конфигурирование устройства.....</b>	<b>12</b>
Лицензия .....	14
Требования к сетевым соединениям.....	14
<b>5. Дистанционное управление .....</b>	<b>15</b>
Настройка iDRAC.....	15
Подсоединить модуль к сети.....	18
Войти в iDRAC.....	18
<b>6. Проверка подключения и возможности сетевого взаимодействия.....</b>	<b>19</b>
Проверка соединения интерфейса управления.....	19
Проверка коммутатора/подключения и возможности сетевого взаимодействия устройства .....	19
Провести ping-тест .....	20
<b>7. Настройки консоли CounterACT .....</b>	<b>21</b>
Установка консоли CounterACT .....	21
Вход в систему .....	22
Начальные настройки .....	22
<b>Контактные данные:.....</b>	<b>24</b>

# Добро пожаловать в ForeScout CounterACT®, версия 7

ForeScout CounterACT — физическое и виртуальное устройство безопасности, обеспечивающее динамическое выявление и оценку сетевых устройств и приложений в момент их подключения к сети. Поскольку CounterACT не требует агентов, оно работает напрямую с вашими устройствами — управляемыми и неуправляемыми, известными и неизвестными, стационарными и мобильными, встроенными и виртуальными. CounterACT быстро распознает пользователя, владельца, операционную систему, конфигурацию устройства, программное обеспечение, услуги, состояние заплат и наличие средств защиты. И все это при бесшовной интеграции с вашей ИТ-инфраструктурой.



## ***В настоящем руководстве описывается установка одного автономного устройства CounterACT.***

Дополнительную информацию и сведения о размещении нескольких устройств для защиты сети в масштабе предприятия см. *“Руководство по установке CounterACT”* и *“Руководство пользователя консоли”*. Данные документы можно найти на компакт-диске CounterACT CD в директории /docs.

Кроме того, последние версии документов, статьи с базами знаний и обновления Вашего устройства можно найти на сайте поддержки по адресу: <https://www.forescout.com/support>.

## **В комплект CounterACT входит:**

- Устройство CounterACT
- Краткое руководство по установке
- Компакт-диск CounterACT с программным обеспечением консоли, руководством пользователя консоли и руководством по установке
- Гарантии
- Монтажный кронштейн
- Кабель питания
- Соединительный кабель консоли DB9 (только для последовательных соединений)

# Общие сведения

Для настройки CounterACT нужно выполнить следующие действия:

1. Разработать план размещения
2. Установить коммутатор
3. Подключить кабели сети и питание
4. Конфигурировать устройство
5. Дистанционное управление
6. Проверить подключения и возможности сетевого взаимодействия
7. Провести Начальную настройку консоли CounterACT

# 1. Разработка плана размещения

Перед установкой определить место размещения устройства и подключения интерфейса.

## Определить место размещения устройства

Правильный выбор места размещения устройства в сети имеет решающее значение для успешного разворачивания и оптимальной производительности CounterACT. Правильность расположения зависит от целей применения и политики контроля доступа к сети. Устройство также должно обеспечивать контроль трафика, установленного проводимой политикой контроля. Например, если ваша политика зависит от событий авторизации контроля от оконечных устройств до корпоративных серверов авторизации, устройство должно быть установлено так, чтобы оно “видело” трафик оконечных устройств, поступающий на серверы авторизации.

Дополнительную информацию об установке и размещении см. Руководстве по установке CounterACT на компакт- диске CounterACT, входящем в комплект устройства.

## Подключение интерфейсов устройства

Конфигурация устройства включает, как правило, три соединения с коммутатором сети.

### Интерфейс управления

Данный интерфейс обеспечивает управление устройством CounterACT, выполняет запросы и глубокую проверку оконечных устройств. Интерфейс должен быть подключен к порту коммутатора, имеющего доступ ко всем оконечным устройствам сети.

Каждое устройство подключается к сети через отдельное административное соединение. Для этого соединения в локальной сети LAN требуется IP-адрес и доступ через порт 13000/TCP от устройств, управляющих приложением управления консолью CounterACT. Интерфейс административного управления должен иметь в сети доступ к следующим элементам:



Порт	Услуга	На или от CounterACT	Назначение
22/TCP	SSH	На	Обеспечивает доступ к интерфейсу командной строки CounterACT.
2222/TCP			(Высокий уровень доступности) Обеспечивает доступ к физическим устройствам CounterACT, входящим в состав кластера высокого уровня доступности. Для доступа к (виртуальному) IP-адресу общего пользования кластера использовать 22/TCP.

Порт	Услуга	На или от CounterACT	Назначение
25/TCP	SMTP	От	Для отправки почты от CounterACT
53/UDP	DNS	От	Позволяет CounterACT преобразовывать внутренние IP-адреса.
80/TCP	HTTP	На	Осуществляет перенаправление HTTP.
123/UDP	NTP	От	Обеспечивает CounterACT доступ к серверу времени NTP. По умолчанию CounterACT использует ntp.foreScout.net
135	MS-WMI	От	Позволяет проводить удаленное исследование оконечных устройств Windows.
139/TCP	SMB, MS-RPP	От	Позволяет проводить удаленное исследование оконечных устройств Windows (для Windows 7 и более ранних версий).
445/TCP			Позволяет проводить удаленное исследование оконечных устройств Windows.
161/UDP	SNMP	От	Обеспечивает CounterACT связь с аппаратурой инфраструктуры сети, например переключателями и маршрутизаторами.  Информацию по конфигурированию SNMP см. в <i>Руководстве пользователя консолью CounterACT</i> .
162/UDP	SNMP	На	Обеспечивает CounterACT связь с аппаратным обеспечением инфраструктуры сети, например переключателями и маршрутизаторами.  Информацию по конфигурированию SNMP см. в <i>Руководстве пользователя консолью CounterACT</i> .
443/TCP	HTTPS	На	Осуществляет перенаправление HTTP с помощью TLS.
2200/TCP	Secure Connector	На	Позволяет SecureConnector (защищенному соединению) создать безопасное (зашифрованное SSH) соединение между устройством и устройствами Macintosh/Linux. <i>SecureConnector</i> — основанный на скрипте агент, позволяющий управлять оконечными устройствами Macintosh и Linux во время их подключения к сети.
10003/TCP	SecureConnector для Windows	На	Позволяет SecureConnector создавать защищенное (зашифрованное TLS) соединение между устройством и устройствами Windows. <i>SecureConnector</i> — агент, позволяющий управлять оконечными устройствами Windows во время их подключения к сети. Подробное описание SecureConnector см. в <i>Руководстве пользователя консолью CounterACT</i> .

			При подсоединении SecureConnector к устройству или компоненту Enterprise Manager он перенаправляется на то устройство, которому назначен его хост. Убедитесь, что этот порт открыт для всех устройств и Enterprise Manager, что позволит обеспечить прозрачную мобильность сети в рамках организации.
13000/TCP	CounterACT	На	Обеспечивает соединение от консоли к устройству. Для систем с несколькими устройствами CounterACT обеспечивает соединение от консоли с компонентом Enterprise Manager и от Enterprise Manager с каждым устройством.

## Интерфейс текущего контроля

Данное соединение обеспечивает наблюдение и контроль трафика сети.

Трафик отражается на порт на коммутаторе, и устройство осуществляет наблюдение.

В зависимости от количества отражаемых виртуальных локальных сетей (VLAN) трафик может или не может быть тегирован 802.1Q VLAN.

- **Отдельная виртуальная локальная сеть VLAN (нетегированная).** При генерации контролируемого трафика от отдельной виртуальной локальной сети VLAN, тегирование отражаемого трафика виртуальной локальной сетью VLAN не требуется.
- **Несколько виртуальных локальных сетей VLAN (тегированные).** При генерации контролируемого трафика более чем одной VLAN отражаемый трафик *должен быть тегирован 802.1Q VLAN.*

При двух коммутаторах, подключенных в качестве резервной пары, устройство должно контролировать трафик с обоих коммутаторов.

Для мониторинга текущего контроля IP-адреса, как правило, не требуется.

## Ответный интерфейс

Устройство отвечает на трафик с помощью данного интерфейса. Ответный трафик используется для защиты от вредоносной деятельности и выполняет функции политики контроля доступа к сети. К этим действиям могут относиться, например, перенаправление веб-браузеров или защита с помощью межсетевого экрана. Конфигурация порта соответствующего коммутатора зависит от контролируемого трафика.

- **Отдельная виртуальная локальная сеть VLAN (нетегированная).** При генерации контролируемого трафика отдельной виртуальной локальной сетью (VLAN) конфигурация ответного интерфейса должна входить в состав той же виртуальной локальной сети VLAN. В этом случае для устройства требуется отдельный IP-адрес в данной VLAN.
- **Несколько виртуальных локальных сетей VLAN (тегированные).** При генерации контролируемого трафика более чем одной виртуальной локальной сетью VLAN ответный интерфейс конфигурируется с тегированием 802.1Q в той же виртуальной локальной сети VLAN. Для устройства требуется IP-адрес для каждой защищаемой VLAN.

## 2. Установка коммутатора

### А. Варианты подключения коммутатора

Устройство разработано для бесшовной интеграции в самые разнообразные сетевые среды. Для успешной интеграции устройства в сеть необходимо проверить настройку коммутатора на контроль требуемого трафика.

Подключение устройства к Вашему коммутатору может осуществляться в нескольких вариантах.

#### 1. Стандартное размещение (раздельные интерфейсы управления, текущего контроля и ответа)

В рекомендуемом варианте используются три раздельных порта. Описание данных портов приведено в разделе *“Подключение интерфейсов устройства”*.



#### 2. Пассивный встраиваемый разветвитель

Вместо подключения к порту отслеживания коммутатора устройство может использовать пассивный встраиваемый разветвитель.

Для пассивного разветвителя требуется два порта текущего контроля, за исключением случая “рекомбинантных” разветвителей, объединяющих два вдвоенных потока в один порт. Трафик на разветвительном порту и ответный интерфейс должны конфигурироваться аналогичным образом. Например, трафик на разветвительном порту тегирован VLAN (802 1Q), и ответный интерфейс должен также быть VLAN-тегированным портом.



#### 3. Активный (способный к инъекции) встраиваемый разветвитель

При использовании в устройстве встраиваемого разветвителя, *способного к инъекции*, интерфейс монитора и ответный интерфейс можно объединить. Конфигурировать отдельный порт ответа на коммутаторе не требуется. Данный вариант можно применять для любого типа конфигурации коммутатора исходящего или входящего трафика.



#### 4. Ответ IP-уровня (для установки коммутатора уровня 3)

Для ответа на трафик устройство может использовать собственный интерфейс управления. Несмотря на то, что данный вариант пригоден для любого контролируемого трафика, его можно рекомендовать в том случае, когда устройство контролирует порты, не входящие в любую VLAN, и, таким образом, не может ответить на контролируемый трафик с использованием любого другого порта коммутаторов. Данная ситуация типична при отслеживании линка, соединяющего два маршрутизатора.

Данный вариант не способен ответить на запрос Протокола определения адреса (ARP), что ограничивает возможности устройства по обнаружению сканов, направленных на IP- адреса, включенные в контролируемую подсеть. Данное ограничение не применяется при контроле трафика между двумя маршрутизаторами.

## В. Примечания к установке коммутатора

### Теги VLAN (802.1Q)

- **Отслеживание отдельной VLAN (нетегированный трафик).** При генерации контролируемого трафика отдельной VLAN тегирование трафика 802.1Q не требуется.
- **Контроль нескольких VLAN (тегированный трафик).** При генерации контролируемого трафика двумя или более VLAN *на интерфейсах* текущего контроля и ответа тегирование 802.1Q должно быть активировано. Рекомендуется проводить контроль нескольких VLAN. При этом обеспечивается больший охват контроля при сокращении количества отражающих портов.
- При невозможности использования на коммутаторе тега 802.1Q VLAN необходимо выполнить одно из следующих действий:
  - Отразить только одну VLAN.
  - Отразить отдельный нетегированный восходящий порт.
  - Использовать вариант ответа IP уровня.
- Если коммутатор отражает только один порт, отразить отдельный восходящий порт. Это можно тегировать. В большинстве случаев, если коммутатор разделяет теги 802.1Q VLAN следует, использовать вариант ответа IP уровня.

### Дополнительно

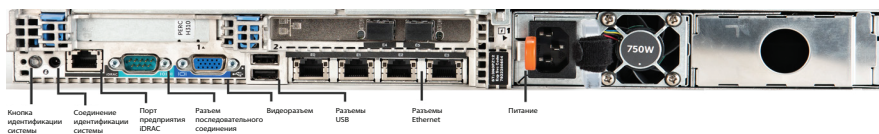
- При невозможности отражения коммутатором и передаваемого, и принимаемого трафика установить контроль над всем коммутатором, полными виртуальными локальными сетями (это обеспечит передачу/прием) или просто интерфейс (позволяет вести передачу/прием). Проверить отсутствие перегрузки на отражающем порте.
- На некоторых коммутаторах (например, Cisco 6509) перед вводом новой конфигурации необходимо произвести полную очистку конфигурации прежнего порта. Чаще всего удаление информации о прежнем порте приводит к разделению коммутатором тегов 802.1Q.

### 3. Подключение сетевых кабелей и включение питания

#### А. Распаковка устройства и соединительных кабелей

1. Вынуть устройство и кабель питания из упаковочной коробки.
2. Вынуть упоры, поставляемые в комплекте с устройством.
3. Собрать упоры на устройстве и установить устройство на стойку.
4. Подключить сетевые кабели между интерфейсами сети на задней панели устройства и портами коммутатора.

#### **Образец задней панели устройства CounterACT**



## В. Запись присваиваний интерфейса

АfПо завершении установки устройства в центре обработки и хранения данных и установки консоли CounterACT появляется подсказка о регистрации присваиваний интерфейса. Данные присваивания, называемые *Channel definitions (определения каналов)*, вводятся в Первоначальный мастер установки (Initial Setup Wizard), который открывается при первом входе в консоль.

Произвести запись присваиваний физического интерфейса ниже и использовать их по завершении настроек канала и консоли.

Интерфейс Ethernet	Присваивание интерфейса (например, Управление, Текущий контроль, Ответ)
Eth0	
Eth1	
Eth2	
Eth3	
Eth4	
Eth5	
Eth6	
Eth7	
Eth8	

## С. Подача питания на устройство

1. Подключить кабель питания к разъему питания на задней панели устройства.
2. Другой конец кабеля питания подключить к электрической розетке с заземлением.
3. Подключить клавиатуру и монитор к устройству или установить последовательное соединение устройства. См. *Руководство по установке CounterACT* на компакт-диске CounterACT.
4. Подать питание на устройство с передней панели.

**Внимание: Перед отсоединением разъема из розетки выключить устройство.**

## 4. Конфигурирование устройства

Перед конфигурированием устройства необходимо подготовить следующую информацию.

<input type="checkbox"/> Имя хоста устройства	
<input type="checkbox"/> Пароль администратора CounterACT	<b>Сохранить пароль в надежном месте</b>
<input type="checkbox"/> Интерфейс управления	
<input type="checkbox"/> IP-адрес устройства	
<input type="checkbox"/> Маска сети	
<input type="checkbox"/> IP-адрес шлюза по умолчанию.	
<input type="checkbox"/> DNS имя домена	
<input type="checkbox"/> DNS адреса сервера	

После включения питания о необходимости начать конфигурирование напоминает следующее сообщение:

**Самозагрузка CounterACT завершена.  
Нажать <Enter> (Ввод) и продолжить.**

1. Нажать **Enter (Ввод)** и вывести на экран следующее меню:

**1) Конфигурировать CounterACT  
2) Восстановить сохраненную конфигурацию CounterACT  
3) Идентифицировать и перенумеровать интерфейсы сети  
4) Конфигурировать расположение знаков на клавиатуре  
5) Выключить устройство  
6) Перезагрузить устройство  
Выбор (1-6) :1**

2. Выбрать **1** – Конфигурировать CounterACT. По подсказке:

**Продолжить: (yes/no) (да/нет) ?**

Нажать **Enter (Ввод)** и начать установку.

3. Открывается меню **Режим высокого уровня доступности (High Availability Mode)**. Нажать **Enter (Ввод)** и выбрать Standard Installation (Стандартная установка).
4. На экран выводится подсказка **CounterACT Initial Setup (Начальная настройка CounterACT)**. Для продолжения нажать **Enter (Ввод)**.
5. Открывается меню **Select CounterACT Installation Type (Выбрать тип установки CounterACT)**. Набрать **1**, нажать **Enter (Ввод)** и установить стандартное Приложение CounterACT. Установка инициализирована. Установка может занять некоторое время.


6. По подсказке **Enter Machine Description (Ввести описание устройства)**, ввести короткий текст идентификации устройства и нажать **Enter (Ввод)**.  
На экран выводится следующее сообщение:

>>>>> Set Administrator Password (Установить пароль администратора)<<<<<<

Пароль используется для входа в качестве "корня" в операционную систему устройства и в качестве "admin" ("админ") в консоль CounterACT.

Длина пароля должна составлять от 6 до 15 знаков, пароль должен содержать, по крайней мере, один знак, не являющийся алфавитным.

Пароль администратора:

7. По подсказке **Set Administrator Password (Установить пароль администратора)**, ввести строку, являющуюся Вашим паролем (строка не отображается на экране) и нажать **Enter (Ввод)**. Подсказка предлагает подтвердить пароль. Длина пароля должна составлять от 6 до 15 знаков, пароль должен содержать, по крайней мере, один знак, не являющийся алфавитным.
-  Войти в устройство в качестве корня, и войти в Консоль в качестве админ (admin).
8. По подсказке **Set Host Name (Установить имя хоста)**, набрать на клавиатуре имя хоста и нажать **Enter (Ввод)**. Имя хоста можно использовать при входе в консоль, имя хоста выводится на консоли для идентификации устройства CounterACT, находящегося у Вас перед глазами.
9. Экран **Configure Network Settings (Конфигурировать уставки сети)** подсказывает серию параметров конфигурации. Набрать на клавиатуре значение по каждой подсказке и нажать **Enter (Ввод)**:
- Компоненты CounterACT обмениваются данными через интерфейсы управления. Количество указанных в списке интерфейсов управления зависит от модели устройства.
  - **Management IP address (IP-адрес управления)** представляет собой адрес интерфейса, через который осуществляется обмен данными между компонентами CounterACT. Для данного интерфейса VLAN ID добавляется только в случае подключения интерфейса для обмена данными между компонентами CounterACT к тегированному порту.
  - При наличии более чем одного **адреса DNS-сервера**, отделить каждый адрес пробелом. —Как правило, внутренние DNS-серверы определяют внешние и внутренние адреса, но у Вас может возникнуть необходимость включения DNS- сервера, определяющего внешние адреса. Поскольку почти все DNS-запросы, выполненные устройством направлены на внутренние адреса, внешний DNS-сервер указывается последним.
10. На экран выводится подсказка **Setup Summary (Итоговые данные установки)**. Подсказка предлагает выполнить общую проверку целостности, реконфигурировать уставки или завершить установку. Для завершения установки набрать на клавиатуре **D**.

## Лицензия

По завершении установки необходимо установить начальную демонстрационную лицензию, предоставляемую Вашим представителем CounterACT. Лицензия устанавливается во время первоначальной установки консоли. Первоначальная демонстрационная лицензия действительна на срок в несколько дней. Постоянную лицензию необходимо установить до истечения этого срока. Уведомление о дате истечения срока действия демонстрационной лицензии будет отправлено Вам по электронной почте. Кроме того, информация о дате истечения срока действия и статусе лицензии выводится на дисплей консоли, панель Приложения/Устройства.

После получения постоянной лицензии она подтверждается ежедневно через лицензионный сервер ForeScout. Предупреждения и нарушения Лицензии выводятся на панель Характеристики устройства.

Лицензии, не подтверждаемые в течение одного месяца отзываются. Дополнительную информацию о лицензиях см. в Руководстве по установке CounterACT.

## Требования к сетевым соединениям

По крайней мере, одно устройство CounterACT (Приложение или Управление предметной областью) должны иметь доступ в Интернет. Данное соединение используется для подтверждения лицензий CounterACT по серверу Лицензий ForeScout.

Лицензии, не подтверждаемые в течение одного месяца отзываются. Ежедневно CounterACT отправляет электронные сообщения с предупреждением и уведомлением о наличии коммуникационной ошибки на сервере.

## 5. Дистанционное управление

### Настройка iDRAC

Встроенный контроллер удаленного доступа Dell (iDRAC) представляет собой встроенную серверную систему, обеспечивающую удаленный доступ, независимый от местонахождения/ОС, по локальной сети или через Интернет к Приложениям CounterACT/Управление предметными областями. Данный модуль используется для доступа к KVM, включения/выключения питания/сброса, проведения поиска и устранения неисправностей и технического обслуживания.

Для настройки модуля iDRAC необходимо выполнить следующие действия:

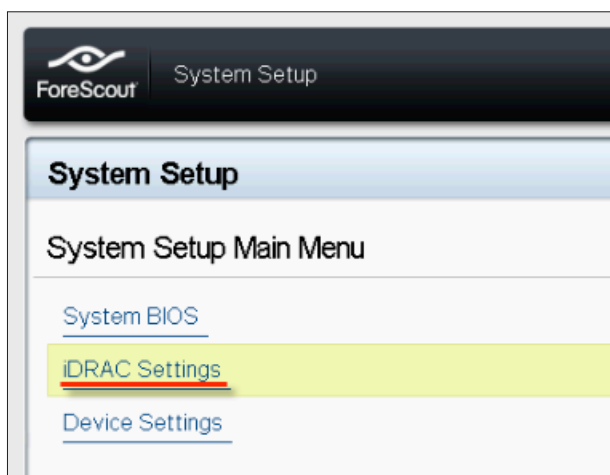
- *Активировать и сконфигурировать модуль iDRAC.*
- *Подсоединить модуль к сети.*
- *Войти в iDRAC.*

#### Активировать и сконфигурировать модуль iDRAC

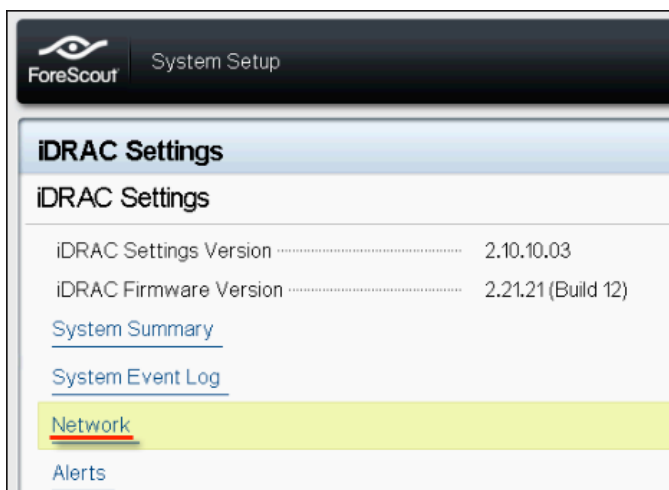
Изменить настройки iDRAC для активирования удаленного доступа на устройстве CounterACT. В настоящем разделе приведены основные параметры интеграции для работы с CounterACT.

#### Для установки конфигурации iDRAC:

1. Включить управляемую систему.
2. Во время самотестирования при включении питания (POST) выбрать F2.
3. На странице главного меню настроек системы выбрать **iDRAC Settings (Настройки iDRAC)**.

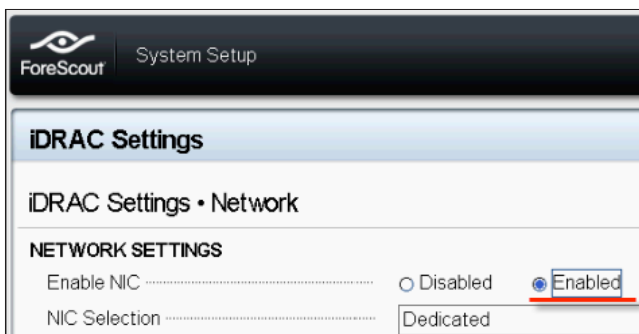


4. На странице iDRAC Settings (Настройки iDRAC) выбрать **Network (Сеть)**.



5. Сконфигурировать следующие настройки сети:

- **Настройки сети.** Проверить установку поля **Enable NIC (Активировать NIC)** на **Enabled (Активировано)**.



- **Общие настройки.** В поле имени DNS DRAC можно обновить динамический DNS (на усмотрение).
- **Настройки IPV4.** Проверить установку поля **Enable IPv4 (Активировать IPv4)** на **Enabled (Активировано)**. Установить поле **Enable DHCP (Активировать DHCP)** на **Enabled (Активировано)** и использовать динамическую IP-адресацию или деактивировать для использования статической IP-адресации. В случае активирования DHCP автоматически

присваивает IP-адрес, шлюз и маску подсети устройству iDRAC. В случае деактивирования ввести значения в поля **Static IP Address (Статический IP-адрес)**, **Static Gateway (Статический шлюз)** и **Static Subnet Mask (Статическая маска сети)**.

ForeScout System Setup

### iDRAC Settings

iDRAC Settings • Network

**IPv4 SETTINGS**

Enable IPv4	<input type="radio"/> Disabled	<input checked="" type="radio"/> <u>Enabled</u>
Enable DHCP	<input checked="" type="radio"/> Disabled	<input type="radio"/> Enabled
Static IP Address	<input type="text" value="192.168.1.103"/>	
Static Gateway	<input type="text" value="192.168.1.1"/>	
Static Subnet Mask	<input type="text" value="255.255.255.0"/>	
Use DHCP to obtain DNS server addresses	<input checked="" type="radio"/> Disabled	<input type="radio"/> Enabled
Static Preferred DNS Server	<input type="text" value="192.168.1.2"/>	
Static Alternate DNS Server	<input type="text" value="0.0.0.0"/>	

6. Выбрать **Back (Назад)**.
7. Выбрать **User Configuration (Конфигурация пользователя)**.
8. Сконфигурировать следующие поля User Configuration (Конфигурация пользователя):
  - **Активировать пользователя.** Проверить установку поля на Enabled (Активировано).
  - **Имя пользователя.** Ввести имя пользователя.
  - **Привилегии пользователя LAN и порта последовательного ввода-вывода.** Установить уровни привилегий на Администратора.
  - **Изменить пароль.** Установить пароль для логина пользователя.

ForeScout System Setup Help | About | E

### iDRAC Settings

iDRAC Settings • User Configuration

User ID	<input type="text" value="2"/>	
Enable User	<input type="radio"/> Disabled	<input checked="" type="radio"/> <u>Enabled</u>
User Name	<input type="text" value="root"/>	
LAN User Privilege	<input type="text" value="Administrator"/>	
Serial Port User Privilege	<input type="text" value="Administrator"/>	
Change Password	<input type="text"/>	

9. Выбрать **Back (Назад)**, затем выбрать **Finish (Закончить)**. Подтвердить измененные настройки. Настройки сети сохраняются, и система перезагружается.

## Подсоединить модуль к сети

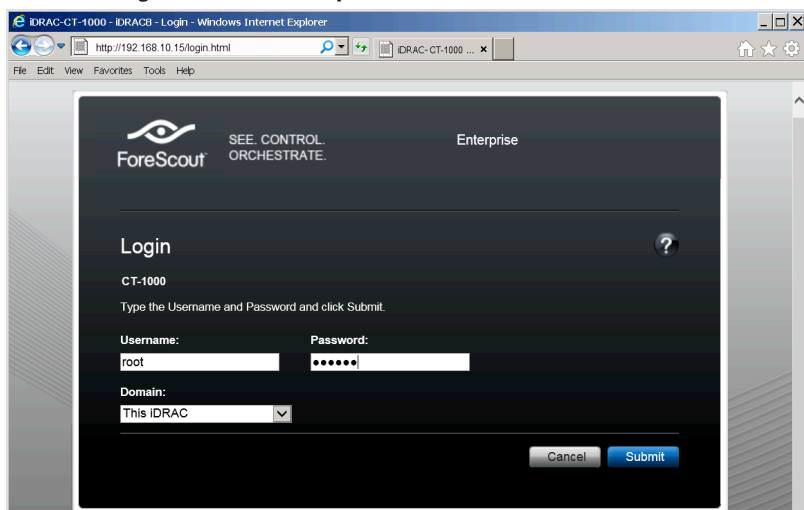
iDRAC подключается к сети Ethernet. Устройство принято подключать к сети управления. На изображении ниже показано расположение порта iDRAC на задней панели Приложения CT-1000:



## Войти в iDRAC

Для входа в iDRAC:

1. Перейти в IP-адрес или доменное имя, сконфигурированное в **iDRAC Settings > Network. (Настройки iDRAC > Сеть)**.



2. Ввести имя пользователя и пароль, сконфигурированные на странице Конфигурация пользователя установок системы iDRAC.
3. Выбрать **Submit (Отправить)**.

Дополнительную информацию по iDRAC см. в [Руководстве пользователя iDRAC](#).

Обновление регистрационных данных по умолчанию имеет большое значение.

## 6. Проверка подключения и возможности сетевого взаимодействия

### Проверка соединения интерфейса управления

Для проверки соединения интерфейса управления войти в устройство и выполнить следующую команду:

```
fstool linktest
```

На экран выводится следующая информация:

```
Management Interface status (Статус интерфейса  
управления)  
По умолчанию информация о проверке шлюза с  
помощью ping-команды  
Ping-статистика  
Тест на определение имен  
Краткое описание теста
```

### Проверка коммутатора/подключения и возможности сетевого взаимодействия устройства

Перед выходом из центра обработки данных проверить правильность подключения коммутатора к устройству. Для этого выполнить команду `fstool ifcount` на устройстве для каждого обнаруженного интерфейса.

```
fstool ifcount eth0 eth1 eth2
```

*(Каждый интерфейс отделяется пробелом)*

Данный инструмент непрерывно выводит на экран сетевой трафик по конкретным интерфейсам. Эти операции выполняются в двух режимах: по интерфейсам или по виртуальным локальным сетям (VLAN). Режим можно изменить с дисплея. Ниже приводится общее количество бит в секунду и процент каждой из нижеприведенных категорий трафика:

- Интерфейс текущего контроля должен в первую очередь видеть отраженный трафик — более 90%.
- Интерфейс ответа должен в первую очередь видеть широкоэвещательный трафик.
- И интерфейс текущего контроля, и интерфейс ответа должны видеть ожидаемые виртуальные локальные сети (VLAN).

#### Опции команд:

**v** – дисплей в режиме VLAN

**I** – дисплей в режиме интерфейса

**P** – показать предыдущий

**N** – показать следующий

**q** – прекратить вывод на экран

## Режим VLAN:

```
update=[4]      [eth3: 14 vlans]
Interface/Vlan  Total   Broadcast   Mirrored   *To my MAC   *From my MAC
(Интерфейс/Общая передача VLAN, отраженная *На мой MAC *С моего MACa.
eth3.untagged   4Mbps   0.2%        99.8%      0.0%        0.0%
eth3.1          9Mbps   0.0%        100.0%     0.0%        0.0%
eth3.2          3Mbps   0.1%        99.9%      0.0%        0.0%
eth3.4          542bps  100.0%      0.0%       0.0%        0.0%
eth3.20         1Kbps   100.0%      0.0%       0.0%        0.0%
Show [v]lans [i]nterfaces <-[p]rev [n]ext->      [q]uit
```

## Режим интерфейсов:

```
update=[31]     [eth0: 32 vlans] [eth1: 1 vlans]
Interface        Total   Broadcast   Mirrored   *To my MAC   *From my MAC
(Интерфейс/Общая передача, отраженная *На мой MAC *С моего MACa.
eth0             3Kbps   42.3%      0.0%       14.1%       43.7%
eth1             475bps  0.0%       100.0%     0.0%        0.0%
```

\*На мой MAC — Адресат MAC - это MAC устройства.

\*От моего MACa — трафик отправлен настоящим устройством (источником MAC является MAC устройства. Назначение может быть многоадресным или одноадресным.

Если трафик не наблюдается, проверить включение интерфейса. Использовать на устройстве следующую команду:

```
ifconfig [interface name] up
```

## Провести ping-тест

Провести ping-тест от устройства к рабочему столу сети и проверить подключение и взаимодействие.

### Для проведения теста:

1. Войти в устройство.
2. Выполнить следующую команду: **Ping [network desktop IP]**  
По умолчанию устройство само не отвечает на ping.

## 7. Настройки консоли CounterACT

### Установка консоли CounterACT

Консоль CounterACT представляет собой некое приложение управления предназначенное для просмотра, отслеживания и анализа деятельности, обнаруживаемой устройством.

С консоли можно определить NAC, Threat Protection, Firewall и другие политики.

Дополнительную информацию см. в *CounterACT Console User Manual (Руководство пользователя консолю CounterACT)*.

Для программного обеспечения консоли CounterACT необходим отдельный компьютер. Минимальные требования к аппаратному обеспечению:

- ПК общего назначения с ОС:
  - Windows XP, Windows Vista or Windows 7;
  - Windows Server 2003 or Server 2008;
  - Linux;
- Pentium 3, 1 ГГц;
- память 2 Гб;
- жесткий диск 1 Гб.

Установку консоли можно выполнять двумя способами:

#### **С использованием инсталляционного программного обеспечения, встроенного в устройство.**

1. Открыть окно браузера с компьютера консоли.
2. Ввести с клавиатуры следующую строку адреса браузера  
**http://<Appliance ip>/install**  
где <Appliance ip> - IP-адрес настоящего Приложения. На экран браузера выводится окно установки консоли.
3. Выполнить инструкции, выведенные на экран.

#### **Установка с компакт-диска CounterACT.**

1. Вставить компакт-диск CounterACT в привод DVD.
2. Открыть файл **ManagementSetup.htm** с CD ROM в браузере.
3. Выполнить инструкции, выведенные на экран.

## Вход в систему

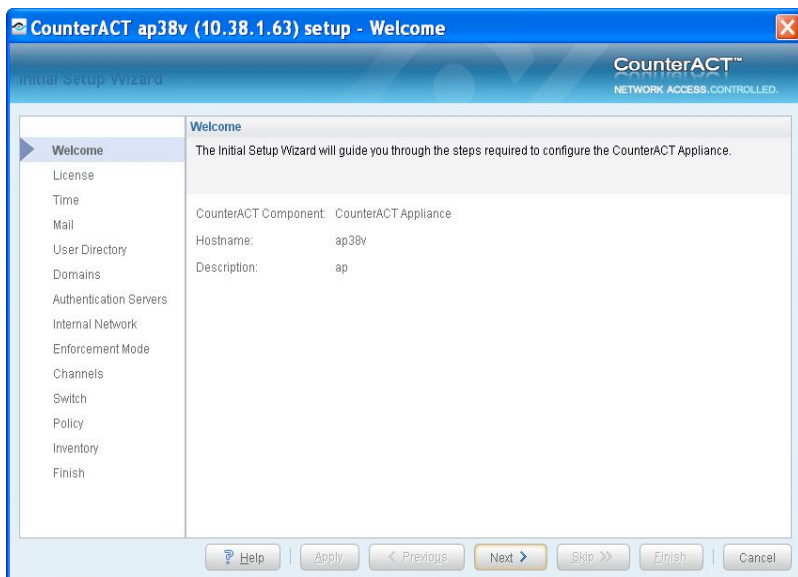
После завершения установки можно войти в консоль CounterACT.

1. Выбрать иконку CounterACT из созданного Вами места быстрого вызова.
2. Ввести в поле **IP/Name (IP/ Имя)** IP-адрес или имя хоста устройства.
3. В поле **User Name (Имя пользователя)** ввести **admin**.
4. В поле **Password (Пароль)** ввести пароль, созданный во время установки устройства.
5. Выбрать **Login** и запустить консоль.



## Начальные настройки

После первого входа появляется первоначальный мастер настроек. Мастер направляет по основным этапам конфигурирования и обеспечивает быструю и эффективную работу CounterACT.



## Перед тем, как установить первоначальные настройки:

Перед работой с Мастером подготовить следующую информацию:

Информация	Значения
<input type="checkbox"/> Адрес сервера NTP, используемый Вашей организацией (на усмотрение).	
<input type="checkbox"/> IP-адрес внутренней ретрансляции почты для доставки почты от CounterACT, если трафик SMTP от устройства не разрешается (на усмотрение).	
<input type="checkbox"/> Адрес электронной почты администратора CounterACT.	
<input type="checkbox"/> Присваивания интерфейсом текущего контроля и ответа, определенные в центре обработки данных.	
<input type="checkbox"/> Для сегментов VLAN без DHCP сегмент сети или виртуальные локальные сети (VLAN), с которыми интерфейс текущего контроля связан прямо, и постоянный IP-адрес, который будет использоваться CounterACT на каждой такой виртуальной локальной сети (VLAN). Для установки управления предметной областью данная информация не требуется.	
<input type="checkbox"/> Диапазон IP-адресов, который должно защищать устройство (все внутренние адреса, включая неиспользуемые адреса).	
<input type="checkbox"/> Сведения об учетной записи директории и IP-адрес сервера директории пользователя.	
<input type="checkbox"/> Регистрационные данные домена, включая административное имя данных домена и пароль.	
<input type="checkbox"/> Серверы идентификации для проведения CounterACT анализа и определения хоста сети с успешной авторизацией.	
<input type="checkbox"/> IP-адрес центрального коммутатора, параметры поставщика и SNMP.	

Работу с Мастером установки см. в *Руководстве пользователя консоли CounterACT* или интерактивную справку.

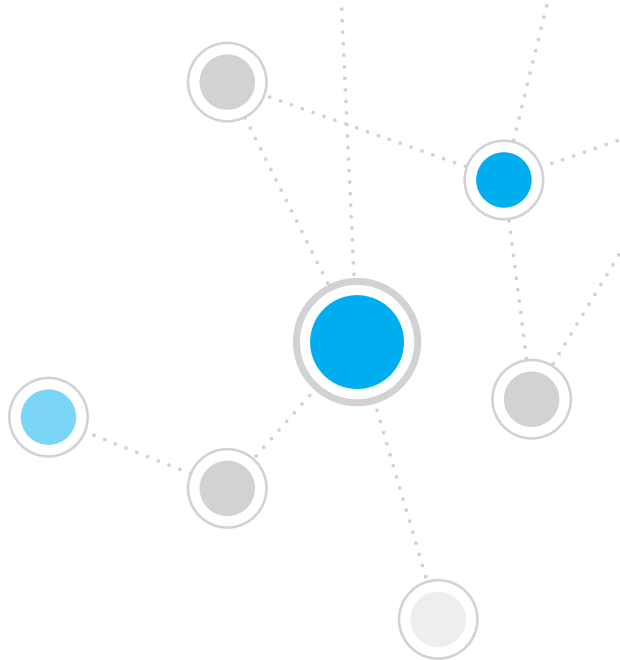
## Контактные данные:

По вопросам технической поддержки обращайтесь в ForeScout по адресу: [support@forescout.com](mailto:support@forescout.com) или по одному из следующих телефонов:

- Бесплатный (по США): 1.866.377.8771
- Телефон (международный): 1.408.213.3191
- Техническая поддержка: 1.708.237.6591
- Факс: 1.408.371.2284

©2016 ForeScout Technologies, Inc. Изделия защищены патентами США № 6,363,489, № 8,254,286, № 8,590,004 и № 8,639,800. Все права защищены. ForeScout Technologies, логотип ForeScout являются товарными знаками ForeScout Technologies, Inc.

Использование любой продукции ForeScout регламентируется условиями лицензионного соглашения для конечного пользователя, находящегося по адресу: [www.forescout.com/eula](http://www.forescout.com/eula).



# ForeScout®

ForeScout Technologies, Inc.  
900 E. Hamilton Avenue #300  
Campbell, CA 95008 USA

**Бесплатный (по США):** 1.866.377.8771

**Телефон (международный):** 1.408.213.3191

**Техническая поддержка:** 1.708.237.6591

**Факс** 1.408.371.2284

400-00020-01