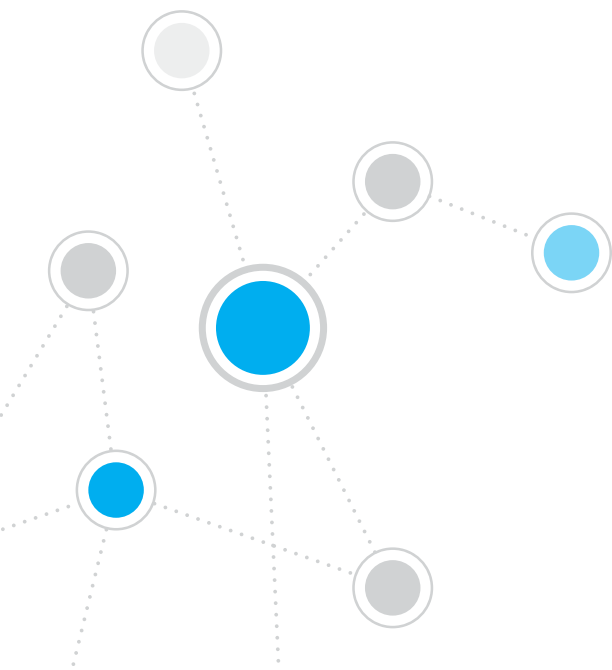




ForeScout CounterACT[®] 7

단일 CounterACT 기기

빠른 설치 안내서



목차

ForeScout CounterACT® 버전7 제품 소개	3
CounterACT 패키지에 포함된 내용물	3
개요	4
1. 배치 계획 수립	5
기기를 배치할 곳 선정	5
기기 인터페이스 연결	5
2. 스위치 설정	8
A. 스위치 연결 옵션	8
B. 스위치 설정 참고 사항	9
3. 네트워크 케이블을 연결하고 전원 켜기	10
A. 기기 포장을 풀고 케이블 연결	10
B. 인터페이스 할당 내역 기록	11
C. 기기 전원 켜기	11
4. 기기 구성하기	12
라이선스	14
네트워크 연결 요건	14
5. 원격 관리	15
iDRAC 설정	15
모듈을 네트워크에 연결	18
iDRAC 에 로그인	18
6. 연결 확인	19
관리 인터페이스의 연결 확인	19
스위치/기기 연결 확인	19
Ping 테스트 실시	20
7. CounterACT 콘솔 설정	21
CounterACT 콘솔 설치	21
로그인	22
초기 설정 실시	22
연락 정보	24

ForeScout CounterACT® 버전7 제품 소개

ForeScout CounterACT는 네트워크 장치 및 응용 프로그램이 네트워크에 연결되는 순간 동적으로 식별하고 평가하는 물리적 또는 가상 보안 기기입니다. CounterACT 는 에이전트를 필요로 하지 않기 때문에 관리형 또는 비관리형, 알려지거나 알려지지 않은 장치, PC 또는 모바일, 임베디드 또는 가상 장치 종류에 상관없이 모든 사용자의 장치와 작동됩니다. CounterACT는 빠르게 사용자, 소유자, 운영체제, 장치 구성, 소프트웨어, 서비스, 패치 상태와 보안 에이전트의 유무를 결정합니다. 그리고 그러한 장치들이 네트워크와 연결되거나 분리될 때 고정, 제어 및 지속적인 모니터링을 제공합니다. ForeScout CounterACT는 사용자의 기존 IT 인프라와 매끄럽게 통합이 되면서 이러한 작업을 수행해냅니다.



본 안내서는 독립형 단일CounterACT기기(이하 “기기”로언급) 의 설치 방법을 설명합니다.

보다 자세한 정보, 또는 기업용 네트워크 보호를 위해 다수의 기기를 배치하는 경우에 관한 정보는CounterACT 설치 안내서 및 콘솔 사용 설명서를 참고해 주십시오. 이 문서들은CounterACT CD의/docs 디렉토리에 있습니다.

또한 지원 웹사이트, <http://www.forescout.com/support> 에서 최신 문헌과 지식 데이터베이스 기사, 기기 업데이트 내용을 확인하실 수 있습니다.

CounterACT 패키지에 포함된 내용물

- CounterACT 기기
- 빠른 설치 안내서
- 콘솔 소프트웨어, CounterACT 콘솔 사용 설명서 및 설치 안내서가 있는 CounterACT CD
- 보증서
- 장착용브래킷
- 전력 케이블
- DB9 콘솔 연결 케이블(직 렬 연결 전용)

개요

CounterACT 설정을 위해 다음 단계를 실시하십시오.

1. 배치 계획 수립
2. 스위치 설정
3. 네트워크 케이블과 전원 연결
4. 기기 구성
5. 원격 관리
6. 연결 확인
7. CounterACT 콘솔 설정

1. 배치 계획 수립

설치를 하기 전에 기기를 어디에 설치해야 할지를 정하고 기기의 인터페이스 연결을 파악해야 합니다.

기기를 배치할 곳 선정

기기를 설치할 올바른 네트워크 위치를 정하는 일은 성공적 배치와 CounterACT 성능 최적화를 위해 매우 중요한 단계입니다. 사용자가 이루려는 목표와 네트워크 액세스 정책에 따라 적절한 위치가 정해집니다. 본 기기는 원하는 정책에 관련된 트래픽을 모니터링 할 수 있어야 합니다. 예를 들어 사용자의 정책이 엔드포인트로부터 기업 인증 서버로 가는 인증 이벤트를 모니터링하는 것이라면 본 기기는 인증 서버로 가는 엔드포인트 트래픽을 볼 수 있도록 설치가 되어야 합니다.

설치 및 배치에 관한 보다 자세한 정보는 본 패키지에 포함된 CounterACT CD 에서CounterACT 설치 안내서를 참고해 주십시오.

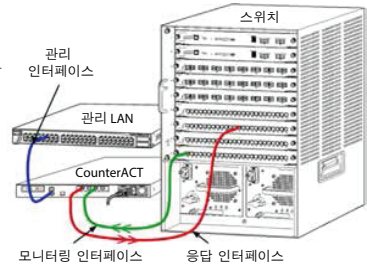
기기 인터페이스 연결

본 기기는 일반적으로 네트 워크 스위치의 세 가지 연결에 대해 구성이 되어 있습니다.

관리 인터페이스

이 인터페이스를 통해 CounterACT를 관리하고 쿼리를 주고 받으며 면밀한 엔드포인트 검사를 실시할 수 있습니다. 이 인터페이스는 모든 네트워크 엔드포인트에 액세스할 수 있는 스위치 포트로 반드시 연결되어 야합니다.

각 기기는 네트워크 관리를 위한 단일 연결을 필요로 합니다. 그러한 연결을 위해 로컬LAN 에서 IP 주소가 필요하며 CounterACT 콘솔 관리 응용프로그램을 실행할 장비에서 포트 13000/TCP 액세스를 하게 됩니다. 관리 인터페이스는 네트워크 상에서 다음과 같은 항목에 액세스할 수 있어야 합니다.



포트	서비스	CounterACT 에 대한 방향성	기능
22/TCP	SSH	CounterACT로 감	CounterACT 명령 라인 인터페이스에 액세스할 수 있습니다.
2222/TCP			(고가용성) 고가용성 클러스터의 부분인 물리적 CounterACT 장치에 액세스할 수 있습니다. 22/TCP를 이용하여 클러스터의 공유된 (가상) IP 주소에 액세스합니다.

포트	서비스	CounterACT 에 대한 방향성	기능
25/TCP	SMTP	CounterACT 에서 나옴	CounterACT에서 메일을 전송하기 위 해 사용됩니다
53/UDP	WMI	CounterACT 에서나옴	CounterACT가 내부 IP 주소를 확인할 수 있습니다
80/TCP	HTTP	CounterACT 로 감	HTTP 리디렉션을 할 수 있습니다.
123/UDP	NTP	CounterACT 에서 나옴	CounterACT가 NTP 시간 서버에 액세스할 수 있습니다. 기본값으로 CounterACT는 ntp.foreScout.net 를 사용합니다
135/TCP	MS-WMI	CounterACT 에서 나옴	Windows 엔드포인트의 원격 검사를 할 수 있습니다.
139/TCP	SMB, MS-RPP	CounterACT 에서 나옴	Windows 엔드포인트의 원격 검사를 할 수 있습니다(Windows 7 및 이전 버전을 실행하는 엔드포인트에 대해).
445/TCP			Windows 엔드포인트의 원격 검사를 할 수 있습니다.
161/UDP	SNMP	CounterACT 에서 나옴	CounterACT가 스위치나 라우터 같은 네트워크 인프라스트럭처 장비와 통신을 할 수 있게 됩니다. SNMP 구성에 관한 보다 자세한 정보는 <i>CounterACT 콘솔 사용 설명서</i> 를 참조하십시오.
162/UDP	SNMP	CounterACT 로 감	CounterACT가 스위치나 라우터 같은 네트워크 인프라스트럭처 장비로부터 SNMP 트랩을 수신할 수 있게 됩니다. SNMP 구성에 관한 보다 자세한 정보는 <i>CounterACT 콘솔 사용 설명서</i> 를 참조하십시오.
443/TCP	HTTPS	CounterACT 로 감	TLS를 통해 HTTP 리디렉션을 할 수 있습니다.
2200/TCP	Secure Connector	CounterACT 로 감	SecureConnector가 Macintosh/ Linux 장비와 본 기기 간에 보안(암호화 된 SSH) 연결을 만들 수 있습니다. <i>SecureConnector</i> 는 스크립트 기반 에이전트로서 Macintosh 및 Linux 엔드포인트가 네트워크에 연결되어 있는 동안 엔드포인트를 관리할 수 있게 해줍니다.
10003/TCP	Windows 용 SecureConnector	CounterACT 로 감	SecureConnector가 Windows 기기와 본 기기 간에 보안 연결을 만들 수 있습니다(암호화된 TLS). SecureConnector는 Windows 엔드포인트가 네트워크에 연결되어 있는 동안 엔드포인트를 관리해 주는 에이전트입니다. <i>SecureConnector</i> 에 대한 보다 자세한 정보는 <i>CounterACT 콘솔 사용 설명서</i> 를 참고해 주십시오. SecureConnector가 기기나 엔터프라이즈 관리자에 연결되면, 호스트가 할당되어 있는 기기로 리디렉션됩니다. 이 포트는 모든 기기와 엔터프라이즈 관리자에 대해 반드시 열려 있어야 조직 내에서 투명한 이동성을 보장할 수 있습니다.

13000/TCP	CounterACT	CounterACT 로 감	콘솔에서 본 기기로 연결이 가능해집니다 여러 대의 CounterACT 기기가 있는 시스템에서 콘솔과 엔터프라이즈 매니저(Enterprise Manager) 간 연결, 엔터프라이즈 매니저와 각 기기 간 연결을 만듭니다
-----------	------------	-------------------	---

모니터링 인터페이스

이 연결을 통해 본 기기가 네트워크 트래픽을 모니터링하고 추적할 수 있습니다.

트래픽이 스위치 포트에 미러링되고 본 기기에서 모니터링 합니다.

미러링된 VLAN 개수에 따라 802.1Q VLAN 태그 처리 여부가 결정됩니다.

- **단일 VLAN(태그 안 됨):** 모니터링 도는 트래픽이 단일 VLAN 에서 생성된 경우 미러링되는 트래픽은 VLAN 태그가 붙지 않습니다.
- **다중 VLAN(태그 됨):** 모니터링되는 트래픽이 한 개 이상의VLAN 에서 오는 경우 미러링되는 트래픽에는 반드시802.1QVLAN 태그가 붙어야 합니다.

두 개의 스위치가 중복 쌍으로서 연결된 경우 본 기기는 두 스위치 모두로부터 오는 트래픽을 모니터링해야 합니다.

인터페이스는 IP 주소가 필요하지 않습니다.

응답인터페이스

본 기기는 이 인터페이스를 통해 트래픽에 응답합니다. 응답 트래픽은 악성 활동을 차단하고 NAC 정책 조치를 실시하기 위해 사용됩니다. 정책 조치란 웹브라우저 리디렉션이나 방화벽 차단 등을 말합니다. 관련된 스위치 포트 구성은 모니터링되는 트래픽에 의해 결정됩니다.

- **단일 VLAN(태그 안 됨):** 모니터링되는 트래픽이 단일 VLAN 에서 생성된 경우 응답 인터페이스는 반드시 동일 VLAN의 한 부분으로서 구성되어야 합니다. 이 경우 본 기기는 해당 VLAN 상에서 IP 주소 하나를 필요로 합니다.
- **다중 VLAN(태그 됨):** 모니터링되는 트래픽이 두 개 이상의 VLAN 에서 오는 경우 응답 인터페이스는 반드시 같은 VLAN에 대해 802.1Q 태그를 붙여 구성해야 합니다.기기에 보호되는 VLAN 별로 각각의 IP 주소가 있어야 합니다.

2. 스위치 설정

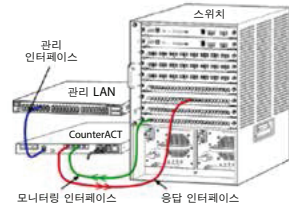
A. 스위치 연결 옵션

본 기기는 다양한 종류의 네트워크 환경에 완벽하게 통합될 수 있도록 설계되었습니다. 기기를 네트워크에 완벽하게 통합시키려면 사용하는 스위치가 모니터링이 필요한 트래픽을 잘 모니터링할 수 있도록 구성됐는지 확인해야 합니다.

본 기기를 스위치에 연결할 때 몇 가지 옵션이 가능합니다.

1. 표준 배치(별도 관리, 모니터링 및 응답 인터페이스)

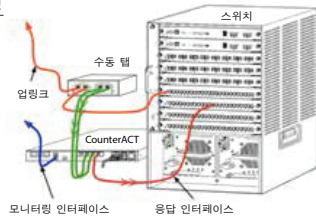
추천되는 배치는 세 개의 별도 포트를 사용하는 것입니다. 그러한 포트는 *기기 인터페이스 연결을 참조하십시오.*



2. 수동 인라인 랩

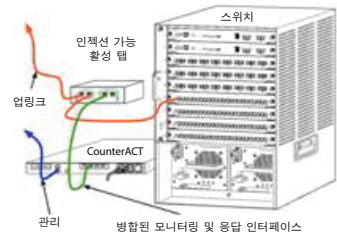
스위치 모니터링 포트에 연결하는 대신 본 기기는 수동 인라인 랩을 사용할 수 있습니다. 수동 랩은 두 개의 모니터링 포트를 필요로 합니다.

단, 두 개의 동시 스트림을 하나의 포트에 합치는 “재조합” 랩의 경우는 예외입니다. 랩 포트의 트래픽과 응답 인터페이스는 반드시 같은 방식으로 구성해야 합니다. 예를 들어 랩 포트의 트래픽이 VLAN 태그(802.1Q)가 붙은 경우 응답 인터페이스 또한 VLAN 태그가 붙은 포트여야 합니다.



3. 활성(인젝션 가능) 인라인 랩

본 기기가 *인젝션 가능* 인라인 랩을 사용하는 경우 모니터링 및 응답 인터페이스는 합쳐질 수 있습니다. 스위치에서 별도의 응답 포트를 구성하지 않아도 됩니다. 업스트림 또는 다운스트림 스위치 구성에 대해 본 옵션을 사용할 수 있습니다.



4. IP 레이어 응답 (레이어-3 스위치 설치의 경우)

본 기기는 트래픽에 응답하기 위해 자체적 관리 인터페이스를 사용할 수 있습니다. 이 옵션을 모니터링되는 어느 트래픽에 대해서나 사용할 수 있지만, 어느 VLAN에도 속해 있지 않은 포트를 본 기기가 모니터링할 때, 그래서 어느 다른 스위치 포트를 통해서도 모니터링되는 트래픽에 본 기기가 응답할 수 없는 경우 이 옵션이 추천됩니다. 두 개의 라우터를 연결한 링크를 모니터링할 때 이 방식이 일반적입니다.

이 옵션으로는 ARP(주소 확인 프로토콜) 요청에 응답할 수 없습니다. 이 프로토콜은 모니터링되는 서브넷에 포함된 IP 주소의 스캔 결과를 감지하려는 본 기기의 성능을 제한합니다. 두 개의 라우터 간 트래픽이 모니터링되는 경우에는 이러한 제약 사항이 적용되지 않습니다.

B. 스위치 설정 참고 사항

VLAN(802.1Q) 태그

- **단일 VLAN 모니터링 (트래픽에 태그 붙지 않음)** 모니터링되는 트래픽이 하나의 VLAN에서 오는 경우 트래픽은 802.1Q 태그를 필요로 하지 않습니다.
- **여러 VLAN 모니터링 (트래픽에 태그 붙음)** 모니터링되는 트래픽이 두 개 이상의 VLAN에서 오는 경우, 모니터링 인터페이스 및 응답 인터페이스는 모두 반드시 802.1Q 태그 적용이 가능 상태여야 합니다. 여러 개의 VLAN 모니터링하기는 미러링 포트 수는 줄여주는 반면 전반적으로 우수한 커버리지를 나타내므로 추천되는 옵션입니다.
- 스위치가 미러링 포트에서 802.1Q VLAN 태그를 할 수 없는 경우 다음 항목 중 하나를 실행해 보십시오:
 - 단일 VLAN만 미러링
 - 태그가 붙지 않은 한 개의 업링크 포트를 미러링
 - IP 레이어 응답 옵션 사용
- 스위치가 포트 한 개만 미러링할 수 있는 경우 업링크 포트 한 개만 미러링하십시오. 이 포트에 태그가 붙을 수 있습니다. 일반적으로 스위치가 802.1Q VLAN 태그를 제거하면 IP 레이어 응답 옵션이 사용되어야 합니다.

추가 사항

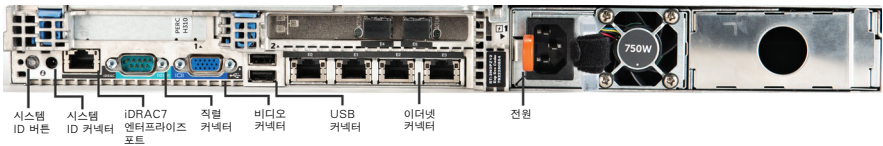
- 스위치가 트래픽을 전송하고 수신하지 못하면 전체 스위치, 모든 VLAN(전송/수신담당) 또는 (전송과 수신 이 가능한) 인터페이스 하나만 모니터링하십시오. 미러링 포트에 부하가 없는지 확인하십시오.
- 어떤 스위치의 경우(예, Cisco 6509), 새 설정을 하기 전에 이전 설정 내용을 완전히 지워야 할 수 있습니다. 이전의 구성 정보를 지우지 않아 생기는 일반적 결과는 스위치가 802.1Q 태그를 제거하는 현상입니다.

3. 네트워크 케이블을 연결하고 전원 켜기

A. 기기 포장을 풀고 케이블 연결

1. 배송 포장에서 본 기기와 전력 케이블을 꺼냅니다.
2. 기기와 함께 온 레일 키트를 꺼냅니다.
3. 기기에 레일 키트를 조립하고 기기를 랙에 장착합니다.
4. 네트워크 케이블로 기기 후면의 네트워크 인터페이스와 스위치 포트를 연결합니다.

후면에서_ CounterACT장치



B. 인터페이스 할당 내역 기록

데이터센터에서 기기 설치 및 CounterACT 콘솔 설치를 마치면 인터페이스 할당을 하라는 알림이 나타납니다. 이러한 할당 작업(채널 정의라고함)은 콘솔에 처음 로그인할 때 열리는 초기 설정 마법사에서 할 수 있습니다.

아래에 실제 인터페이스 할당 내역을 기록하고 콘솔에서 채널 설정을 마칠 때사용하십시오.

이더넷 인터페이스	인터페이스 할당 (예, 관리, 모니터링, 응답)
Eth0	
Eth1	
Eth2	
Eth3	
Eth4	
Eth5	
Eth6	
Eth7	
Eth8	

C. 기기 전원 켜기

1. 전력 케이블을 기기 후면의 전력 커넥터에 연결합니다.
2. 전력 케이블의 다른 한쪽을 접지 AC 콘센트에 연결합니다.
3. 키보드와 모니터를 기기에 연결하거나 기기의 직렬 연결을 구성합니다.
CounterACT CD에 있는 CounterACT 설치 안내서를 참고하십시오.
4. 기기 전면에서 전원을 켜십시오.

중요 정보: 전원 플러그를 뽑기 전에 장비를 끄십시오.

4. 기기 구성하기

기기를 구성하기 전에 다음 정보를 준비합니다.

□ 기기 호스트명	
□ CounterACT Admin 암호	암호는 안전하게 보관하십시오.
□ 관리 인터페이스	
□ 기기 IP 주소	
□ 네트워크 마스크	
□ 기본 게이트웨이 IP 주소	
□ DNS 도메인명	
□ DNS 서버 주소	

전원을 켜면 다음 메시지와 함께 구성을 시작하라고 나옵니다.

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

1. 다음 메뉴를 나타내기 위해 **Enter**를 누릅니다.

```
1) Configure CounterACT
2) Restore saved CounterACT configuration
3) Identify and renumber network interfaces
4) Configure keyboard layout
5) Turn machine off
6) Reboot the machine
Choice (1-6) :1
```

2. **1 - Configure CounterACT**(CounterACT 구성)을 선택합니다. 화면에 나오는 프롬프트는 다음과 같습니다:

```
Continue: (yes/no)?
```

Enter를 눌러 설정을 개시합니다.

3. **High Availability Mode**(고가용성 모드) 메뉴가 열립니다. **Enter**를 눌러 **Standard Installation**(표준 설치)를 선택합니다.

4. **CounterACT Initial Setup**(CounterACT 초기 설정) 프롬프트가 나타납니다. **Enter**를 눌러 진행합니다.

5. **Select CounterACT Installation Type**(CounterACT 설치 유형 선택)메뉴가 열립니다. **1**을 입력하고**Enter**를 눌러 표준 CounterACT 기기를 설치합니다. 설정이 초기화됩니다. 이 과정에 약간의 시간이 소요될 수 있습니다.

6. **Enter Machine Description**(장비 설명 입력) 프롬프트에서 이 장비를 알아볼 수 있는 짧은 설명을 입력한 후 **Enter**를 누릅니다. 다음 화면이 나타납니다.


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

This password is used to log in as 'root' to the machine Operating System and as 'admin' to the CounterACT Console.

The password should be between 6 and 15 characters long and should contain at least one non-alphabetic character.

Administrator password :

7. **Set Administrator Password**(관리자 암호 설정) 프롬프트에서 귀하의 암호로 사용할 문자열을 입력한 후(이때 문자열이 화면에 표시되지 않습니다) **Enter**. 암호를 재확인하라고 나옵니다. 암호는 6 자 내지 15자 길이어야 하고 알파벳이 아닌 문자가 반드시 1 자 이상 포함되어야 합니다.

 기기에는 root 로서 로그인하고 콘솔에는 admin.

8. **Set Host Name**(호스트명 설정) 프롬프트에서 호스트명을 입력한 후 **Enter**를 누릅니다. 호스트명은 콘솔에 로그인할 때 사용될 수 있고, 사용자가 보고 있는 **CounterACT** 기기가 무엇인지 식별할 수 있게 콘솔에서 표시됩니다.

9. **Configure Network Settings**(네트워크 설정 구성) 화면에서 구성 매개 변수들을 정하라고 나옵니다. 각 프롬프트별로 값을 입력한 후 **Enter**를 눌러 진행합니다.

- CounterACT 구성요소는 관리 인터페이스를 통해 통신을 합니다. 나타나는 관리 인터페이스 수는 기기 모델에 따라 다릅니다
- **Management IP address**(관리 IP 주소)는 CounterACT
- 구성요소가 통신할 때 매개체가 되는 인터페이스의 주소입니다. CounterACT 구성요소들 간에 통신을 담당하는 인터페이스가 태그 포트에 연결되는 경우에만 VLAN ID를 추가하십시오.
- 한 개 이상의 **DNS server address**(DNS 서버 주소)가 있는 경우
- 각 주소를 공란으로 띄우십시오. 대부분 DNS 서버는 외부 주소와 내부 주소를 확인하지만 외부 확인용 DNS 서버가 포함되어야 할 수 있습니다. 대부분 기기에서 만드는 모든 DNS 쿼리는 내부용일 것이므로 외부 DNS 서버는 마지막에 나열되어야 합니다.

10. **Setup Summary**(설정 요약) 화면이 표시됩니다. 일반 연결 테스트를 실시하거나 설정을 다시 구성하거나 아니면 설정을 마치라고 나옵니다. **D**를 입력하여 설정을 마칩니다.

라이선스

설치 후 CounterACT 업체 담당자가 제공한 초기 데모 라이선스를 반드시 설치해야 합니다. 라이선스는 초기 콘솔 설정 시에 설치됩니다. 이 초기 데모 라이선스는 일정 기간 동안만 유효합니다. 이 기간이 끝나기 전에 영구적 라이선스를 설치해야 합니다. 만료일과 관련하여 이메일로 연락을 받게 됩니다. 추가로 만료일 정보와 라이선스 상태가 콘솔의 Appliances/Devices(기기/장치) 창에 나타납니다.

영구적 라이선스를 받게 되면 라이선스는 매일 ForeScout 라이선스 서버로부터 유효성 검증을 받게 됩니다. 라이선스 경고나 문제가 있으면 Device Details(장치 세부 사항) 창에 표시됩니다.

한 달 동안 유효성 검증이 되지 않으면 라이선스는 취소됩니다. 라이선스에 관한 보다 자세한 사항은 CounterACT 설치 안내서를 참고해 주십시오.

네트워크 연결 요건

최소 하나의 CounterACT 장치 (기기 또는 엔터프라이즈 매니저)가 인터넷 액세스를 할 수 있어야 합니다. 이 연결은 CounterACT 라이선스를 ForeScout 라이선스 서버를 통해 유효성 검증을 하려 할 때 사용됩니다.

한 달 동안 유효성 검증이 되지 않으면 라이선스는 취소됩니다. CounterACT에서 서버와의 통신 오류가 있음을 알리는 이메일을 하루 한 번 보내오게 됩니다.

5. 원격 관리

iDRAC 설정

iDRAC(Integrated Dell Remote Access Controller)는 통합 서버 시스템 솔루션으로서 사용자 위치와 OS 종류에 관계없이 LAN이나 인터넷을 통해 CounterACT기기/엔터프라이즈 매니저에 접속을 가능하게 해줍니다. KVM 액세스, 전 원 ON/OFF, 리셋을 하기 위해서나 문제 해결, 유지보수 업무를 하기 위해 모듈을 사용할 수 있습니다.

iDRAC 모듈을 사용하기 위해 다음 항목을 실시하십시오.

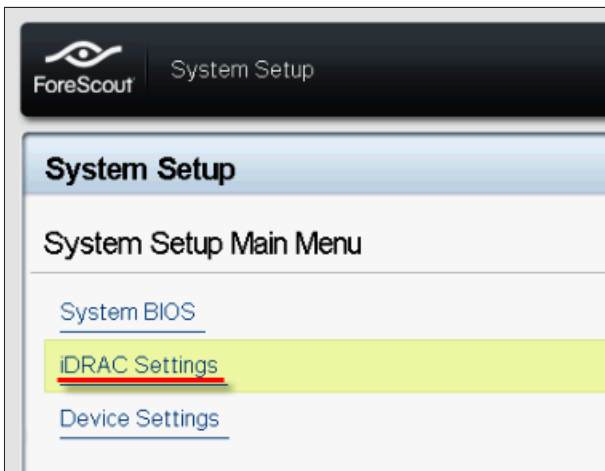
- iDRAC 모듈을 활성화시키고 구성
- 모듈을 네트워크에 연결
- iDRAC 에 로그인

iDRAC 모듈을 활성화시키고 구성

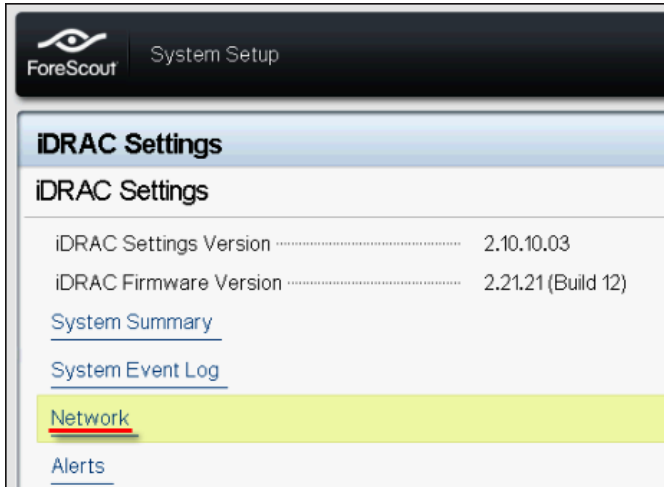
iDRAC 설정을 CounterACT 장치에서 원격 액세스가 가능하도록 변경합니다. 본 섹션에서는 CounterACT 작업에 필요한 기본적 통합 설정 내용을 설명합니다.

iDRAC 을 구성하려면:

1. 관리하고 있는 시스템의 전원을 켭니다.
2. 전원 자가점검(POST) 중에 F2를 선택합니다.
3. System Setup Main Menu(시스템 설정 주메뉴) 페이지에서 **iDRAC Settings** 을 선택합니다.

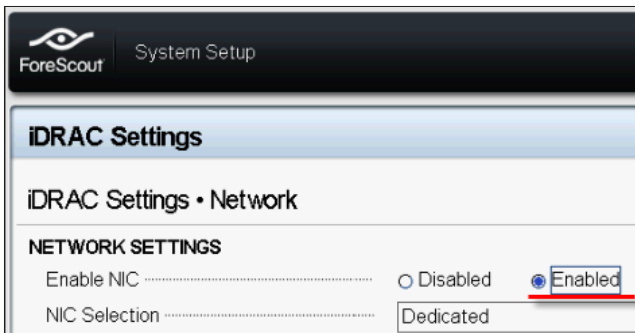


4. iDRAC Settings(iDRAC 설정) 페이지에서 **Network** (네트워크)를 선택합니다.



5. 다음과 같이 네트워크 설정을 구성합니다.

- **Network Settings (네트워크 설정).** Enable NIC(NIC 사용) 필드가 **Enabled**(사용함) 상태로 되어 있는지 확인합니다.



- **Common Settings(일반 설정).** DNS DRAC Name(DNS DRAC 이름) 필드에서 동적 DNS 를 업데이트 할 수 있습니다(선택 사항).

- **IPv4 Settings (IPv4 설정).** Enable IPv4(IPv4 사용) 필드가 Enabled(사용함) 상태로 되어 있는지 확인합니다. 동적 IP를 사용하기 위해서는 Enable DHCP(DHCP 사용) 필드를 Enabled(사용함) 상태로 놓고, 정적 IP를 사용하려면 Disabled(사용 안 함)로 설정 하십시오. 사용 상태로 하면 DHCP가 IP 주소, 게이트웨이, 서브넷 마스크를 자동으로 iDRAC 에 할당합니다. 사용 안 함 상태로 하면 **Static IP Address, Static Gateway, Static Subnet Mask**(정적IP 주소, 정적 게이트웨이, 정적 서브넷 마스크) 값을 수동으로 입력해야 합니다.

iDRAC Settings

iDRAC Settings • Network

IPv4 SETTINGS

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

6. **Back** (뒤로)를 선택합니다.

7. **User Configuration**(사용자 구성)을 선택합니다.

8. 사용자 구성 필드를 다음과 같이 구성합니다.

- **Enable User (사용자 활성화 /).** 이 필드가 Enabled(사용함) 상태로 되어 있는지 확인합니다.
- **User Name (사용자명).** 사용자명을 입력합니다.
- **LAN and Serial Port User Privileges (LAN 및 직렬 포트 사용자 권한).** 권한 수준을 Administrator(관리자)로 정합니다.
- **Change Password (암호 변경).** 사용자 로그인용 암호를 정합니다

iDRAC Settings

iDRAC Settings • User Configuration

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

9. **Back (뒤로)**를 선택한 다음 **Finish (마침)**을 선택합니다. 변경된 설정 내용을 확인합니다. 네트워크 설정이 저장되고 시스템이 다시 부팅됩니다.

모듈을 네트워크에 연결

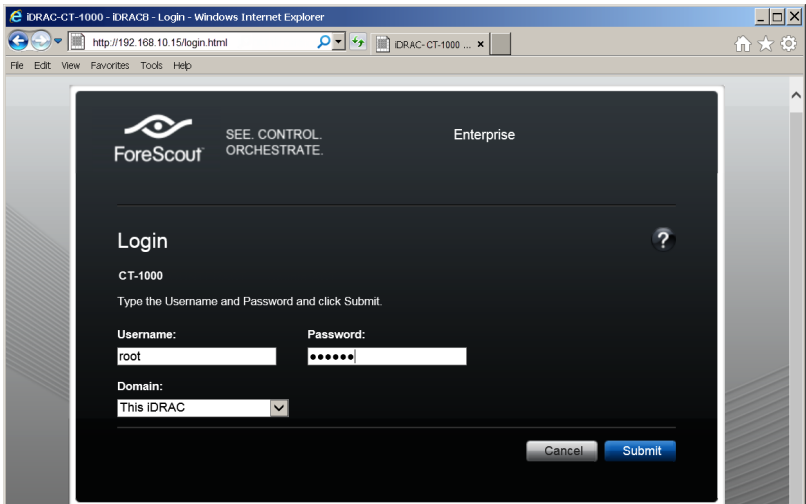
iDRAC은 이더넷 네트워크에 연결됩니다. 관리 네트워크에 연결하는 것이 일반적입니다. 다음 이미지는 CT-1000 기기의 후면 iDRAC 포트 위치를 보여줍니다.



iDRAC에 로그인

iDRAC에 로그인하려면:

1. **iDRACSettings(iDRAC 설정) > Network(네트워크)**



2. iDRAC 시스템 설정의 사용자 구성 페이지에서 정한 사용자명과 암호를 입력합니다.

3. **Submit(제출)**을 선택합니다.

iDRAC에 대한 자세한 정보는 iDRAC 사용 설명서를 참고해 주십시오. 기본 자격 증명 (로그인 정보)을 업데이트하는 것이 중요합니다.

6. 연결 확인

관리 인터페이스의 연결 확인

관리 인터페이스 연결을 테스트하려면 기기로 로그인한 후 다음 명령을 실행합니다.

```
fstool linktest
```

그러면 다음 정보 표시 됩니다.

```
Management Interface status  
Pinging default gateway information  
Ping statistics  
Performing Name Resolution Test  
Test summary
```

스위치/기기 연결 확인

데이터센터를 떠나기 전에 스위치가 기기에 올바르게 연결됐는지 확인하십시오. 이를 위해 **fstool ifcount** 명령을, 감지된 각 인터페이스의 기기에서 실행합니다.

```
fstool ifcount eth0 eth1 eth2  
(각 인터페이스를 공란으로 띄우십시오.)
```

이 틀은 지정된 인터페이스의 네트워크 트래픽을 지속적으로 표시합니다. 이 틀은 '인터페이스별' 또는 'VLAN 별' 두 가지 방식으로 작동합니다. 방식은 호스트명상에서 변경할 수 있습니다. 초당 총 비트수와 다음 각 트래픽 범주의 퍼센트가 표시됩니다.

- 모니터링 인터페이스는 미러링되는 트래픽을 90% 이상으로 주로 표시하게 됩니다.
- 응답 인터페이스는 브로드캐스팅 트래픽을 주로 표시하게 됩니다.
- 모니터링 인터페이스 및 응답 인터페이스 모두 예상되는 VLAN 을 표시하게 됩니다.

명령 옵션:

```
v - display in VLAN mode  
I - display in interface mode  
P - show previous  
N - show next  
q - quit displaying
```

VLAN 모드:

```
update=[4]      [eth3: 14 vlans]
Interface/Vlan  Total   Broadcast  Mirrored  *To my MAC  *From my MAC
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
```

인터페이스 모드:

```
update=[31]      [eth0: 32 vlans] [eth1: 1 vlans]
Interface         Total   Broadcast  Mirrored  *To my MAC  *From my MAC
eth0              3Kbps   42.3%     0.0%     14.1%      43.7%
eth1             475bps   0.0%     100.0%    0.0%       0.0%
```

*To my MAC은 목적지 MAC이며 기기의 MAC을 의미합니다.

*From my MAC은 기기에서 보내는 트래픽입니다(출발지 MAC은 기기의 MAC. 도착지는 브로드캐스팅 또는 유니캐스팅).

아무런 트래픽이 표시되지 않으면 인터페이스가 작동 중인지 확인하십시오.
기기에서 다음과 같은 명령을 실행시킵니다.

ifconfig [interface name] up

Ping 테스트 실시

연결을 확인하기 위해 기기에서 네트워크 데스크탑으로 ping 테스트를 실시합니다.

테스트를 실행하려면:

1. 기기로 로그인합니다.
2. 명령: **Ping [network desktop IP]**
를 실행합니다. 기본 설정상 기기는 ping 에 응답하지 않습니다.

7. CounterACT 콘솔 설정

CounterACT 콘솔 설치

CounterACT 콘솔은 기기에서 감지하는 활동을 보고, 추적하고 분석하는 데 이용되는 중앙 관리 응용프로그램입니다. NAC, 위협 감지, 방화벽 및 기타 정책을 콘솔에서 정의할 수 있습니다. 보다 자세한 정보는 *CounterACT 콘솔 사용 설명서*를 참조하십시오.

CounterACT 콘솔 응용 프로그램 소프트웨어를 호스팅할 수 있는 장치가 있어야 합니다. 최소 요건은 다음과 같습니다.

- 비전용 장치로서 다음 운영 체제를 실행:
 - Windows XP, Windows Vista 또는 Windows 7
 - Windows Server 2003 또는 Server 2008
 - Linux
- Pentium 3, 1GHz
- 2 GB 메모리
- 1 GB 디스크 공간

콘솔 설치를 위해 두 가지 방법을 이용할 수 있습니다.

기기에 있는 설치 소프트웨어를 이용합니다.

1. 콘솔 컴퓨터에서 브라우저 창을 엽니다.
2. 아래 주소를 브라우저 주소 표시줄에 입력합니다.

http://<Appliance_ip>/install

여기서 <Appliance_ip> 는 본 기기의 IP 주소입니다. 브라우저가 콘솔 설치 창을 표시합니다

3. 화면상의 지침을 따릅니다.

CounterACT CD-ROM을 이용한 설치

1. CounterACT CD ROM 을 DVD 드라이브에 넣습니다.
2. 브라우저로 **ManagementSetup.htm** 파일을 CD ROM 에서 엽니다.
3. 화면상의 지침을 따릅니다.

로그인

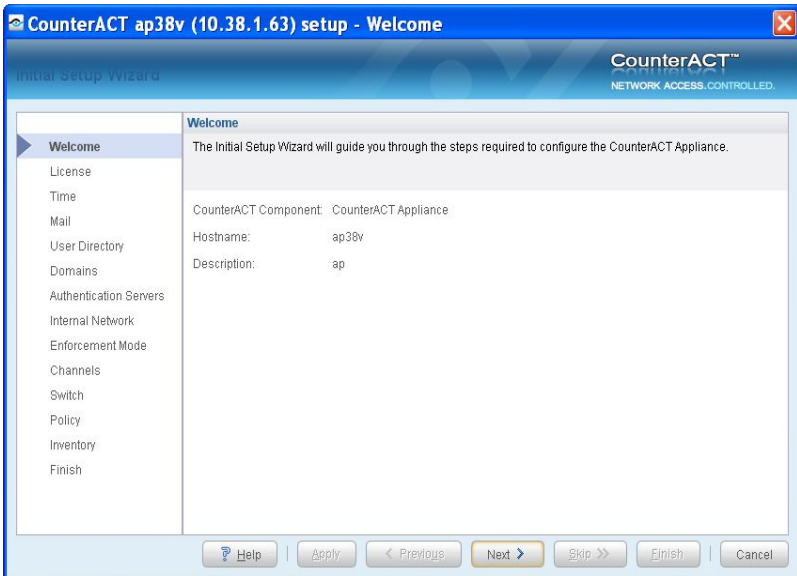
설치를 마친 후 CounterACT 콘솔에 로그인합니다.

1. 만들어 둔 바로 가기 위치에서 CounterACT 아이콘을 선택합니다
2. 기기의 호스트 이름이나 IP 주소를 **IP/Name (IP/이름)** 필드에 입력합니다.
3. **User Name (사용자이름)** 필드에 admin 이라고 입력합니다.
4. **Password (암호)** 필드에 기기 설치 중에 정했던 암호를 입력합니다.
5. 콘솔을 시작하기 위해 **Login (로그인)**을 선택합니다.



초기 설정 실시

처음으로로그인을 한 후 Initial Setup Wizard (초기 설정 마법사)가 나타납니다. 마법사가 CounterACT 가 신속하고 효과적으로 실행될 수 있도록 중요 구성 단계로 안내할 것입니다.



초기 설정을 시작하기 전에

마법사를 이용하기 전에 다음 정보를 준비합니다.

정보	값
□ 회사에서 사용하는 NTP 서버 주소 (선택 사항).	
□ 내부 메일 릴레이 IP 주소. 이를 통해, SMTP 트래픽이 기기로부터 허용되지 않는 경우 CounterACT의 이메일이 전달될 수 있습니다(선택 사항).	
□ CounterACT 관리자 이메일 주소.	
□ 데이터센터에서 정한 모니터링 인터페이스 및 응답 인터페이스 할당 내역.	
□ DHCP가 없는 VLAN이나 세그먼트의 경우 모니터링 인터페이스가 직접 연결된 VLAN 또는 네트워크 세그먼트와 그러한 VLAN에서 CounterACT가 사용할 영구적 IP 주소. 이 정보는 엔터프라이즈 매니저 설정에서는 필요하지 않습니다.	
□ 기기가 보호할 IP 주소 범위 (사용되지 않는 주소를 포함하여 모든 내부 주소).	
□ 사용자 디렉토리 계정 정보 및 사용자 디렉토리 서버 IP 주소.	
□ 도메인 자격 증명 (도메인 관리자 계정명 및 암호 포함).	
□ CounterACT가 어느 네트워크 호스트에서 성공적으로 인증했는지 분석할 수 있게 해주는 인증 서버.	
□ 핵심 스위치 IP 주소, 벤더 및 SNMP 매개변수.	

마법사 사용에 관한 정보는 *CounterACT 콘솔 사용 설명서* 또는 온라인 도움말을 참고해 주십시오.

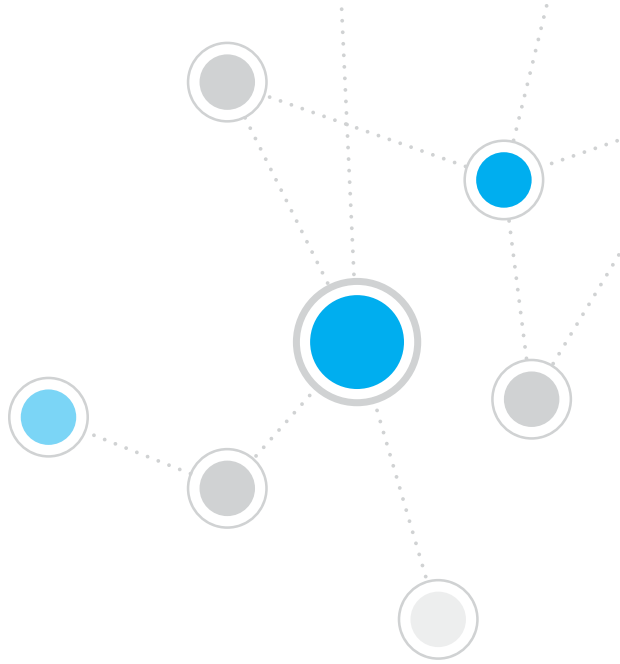
연락처정보

ForeScout 기술 지원을 받으시려면 support@forescout.com으로 이메일을 보내시거나 다음 번호로 전화해주십시오.

- 수신자부담(미국): 1.866.377.8771
- 전화(해외): 1.408.213.3191
- 지원: 1.708.237.6591
- 팩스: 1.408.371.2284

2016 ForeScout Technologies, Inc.의 제품은 미국 특허 #6,363,489, #8,254,286, #8,590,004 및 #8,639,800의 보호를 받습니다. 모든 권리 보유. ForeScout Technologies, ForeScout 로고는 ForeScout Technologies, Inc의 상표입니다. 다른 모든 상표는 해당 소유권자의 재산입니다.

ForeScout 제품의 사용은 ForeScout 최종 사용자 사용권 계약 (www.forescout.com/eula)의 적용을 받습니다.



ForeScout®

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

수신자부담(미국): 1.866.377.8771

전화(해외): 1.408.213.3191

지원: 1.708.237.6591

팩스: 1.408.371.2284

400-00020-01