FORESCOUT

Forescout®

단일 어플라이언스

빠른 설치 가이드

버전 8.2

연락처 정보

Forescout Technologies, Inc.

190 West Tasman Drive

San Jose, CA 95134 USA

https://www.forescout.com/support/

수신자부담 전화(미국): 1.866.377.8771

전화(국제): 1.408.213.3191

지원: 1.708.237.6591

문서 정보

- 추가적인 기술 문서는 Forescout 웹사이트의 리소스 페이지를 참조하십시오: https://www.forescout.com/company/resources/
- 의견이나 질문이 있으신가요? 다음으로 이메일을 보내주십시오: documentation@forescout.com

법적 고지 사항

2020-02-11 17:29

목차

버전 8.2 시작

Forescout 플랫폼은 네트워크 보안을 강화하기 위해 인프라와 기기의 가시성, 정책 관리, 조정, 워크플로 간소화 등을 지원합니다. 이 플랫폼을 통해 기업에서는 네트워크상에 있는 기기와 사용자의 상황별 정보를 실시간으로 볼 수 있습니다. 규정 준수, 문제 해결, 적절한 네트워크 액세스 및 서비스 운영 간소화를 지원하도록 이 상황별 정보를 사용하여 정책이 정의됩니다.

이 가이드에서는 버전 8.0 이 사전 설치된 독립형 CounterACT 단일 어플라이언스의 설치 방법에 대해 설명합니다. 일부 어플라이언스는 이후 버전으로 사전 설치되어 있을 수 있습니다. 버전 8.2 를 사용하려면 버전 출시 정보에 기술된 승인된 업그레이드 경로를 준수하십시오.

기업 전반에서 네트워크 보호를 구현하기 위해 여러 어플라이언스를 업그레이드 및 배포하는 방법을 자세히 알아보려면 *Forescout 설치 가이드* 및 *Forescout 관리 가이드*를 참조하십시오. 가이드 액세스 방법은 추가적인 Forescout 문서를 참조하십시오.

또한, 사용 중인 어플라이언스에 대한 최신 문서, 기술자료 및 업데이트는 다음 지원 웹사이트에서 찾을 수 있습니다: http://www.forescout.com/support

Forescout 패키지 구성요소

Forescout 패키지에는 다음 구성요소가 포함되어 있습니다.

- CounterACT 어플라이언스
- 프론트 베젤
- 레일 키트(장착 브래킷)
- 전원 코드
- DB9 콘솔 연결 케이블(직렬 연결 전용)
- 엔터프라이즈 제품 안전, 환경 및 규정 준수 정보
- 시작 문서(하드웨어 버전 5x 에 기반한 CT-xxxx 어플라이언스 및 Forescout 51xx 어플라이언스 전용)

개요

Forescout 를 설치하려면 다음을 수행하십시오.

1. 배포 계획 수립
2. 스위치 설정
3. 네트워크 케이블 연결 및 전원 켜기
4. 어플라이언스 구성
5. 원격 관리
6. 연결 확인
7. Forescout 콘솔 설정

1. 배포 계획 수립

설치를 수행하기 전에 어플라이언스 배포 위치를 결정하고 어플라이언스 인터페이스 연결에 대해 숙지해야 합니다.

어플라이언스 배포 위치 결정

Forescout 를 성공적으로 배포하고 최적의 성능을 실현하기 위해서는 어플라이언스가 설치되는 올바른 네트워크 위치를 선택하는 것이 중요합니다. 올바른 위치는 원하는 구현 목표와 네트워크 액세스 정책에 따라 달라집니다. 어플라이언스는 원하는 정책과 관련된 트래픽을 모니터링할 수 있어야 합니다. 예를 들어 정책이 기업 인증 서버에 대한 엔드포인트의 모니터링 권한 이벤트에 따라 달라지는 경우, 인증 서버로 유입되는 엔드포인트 트래픽을 파악할 수 있도록 어플라이언스를 설치해야 합니다.

설치 및 배포에 대한 자세한 내용은 *Forescout 설치 가이드*를 참조하십시오. 이 가이드 액세스 방법은 추가적인 Forescout 문서를 참조하십시오.

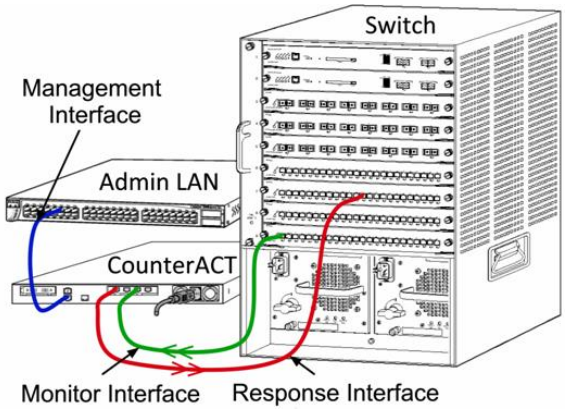
어플라이언스 인터페이스 연결

어플라이언스는 일반적으로 네트워크 스위치에 대한 세 가지 연결로 구성됩니다.

관리 인터페이스

관리 인터페이스를 통해 사용자는 Forescout 플랫폼을 관리하고 엔드포인트에 대한 쿼리와 심층 검사를 수행할 수 있습니다. 인터페이스는 모든 네트워크 엔드포인트에 대한 액세스 권한이 있는 스위치 포트에 연결해야 합니다.

각 어플라이언스는 네트워크에 대한 단일 관리 연결이 필요합니다. 이 연결을 위해서는 로컬 LAN 의 IP 주소가 필요하고 Forescout 콘솔 관리 애플리케이션을 실행하는 시스템에서 포트 13000/TCP 에 액세스할 수 있어야 합니다. 관리 포트는 추가 네트워크 서비스에 대한 액세스 권한이 있어야 합니다.



네트워크 액세스 요구 사항

포트	서비스	대상 또는 출처 **Forescout** 플랫폼	기능
22/TCP	SSH	송신	OS X 및 Linux 엔드포인트의 원격 검사를 허용합니다. Forescout 플랫폼이 네트워크 스위치 및 라우터와 통신하도록 허용합니다.
		수신	Forescout 플랫폼 명령줄 인터페이스에 대한 액세스를 허용합니다.
2222/TCP	SSH	수신	(고가용성) 고가용성 쌍의 일부인 물리적 어플라이언스에 대한 액세스를 허용합니다. 22/TCP 를 사용하여 쌍의 공유(가상) IP 주소에 액세스합니다.
25/TCP	SMTP	송신	Forescout 플랫폼이 엔터프라이즈 메일 릴레이에 액세스하도록 허용합니다.
53/UDP	DNS	송신	Forescout 플랫폼이 내부 IP 주소를 확인하도록 허용합니다.
80/TCP	HTTP	수신	HTTP 리디렉션을 허용합니다.
123/UDP	NTP	송신	Forescout 플랫폼이 로컬 타임 서버 또는 ntp.forescout.net 에 액세스하도록 허용합니다. 기본적으로, Forescout 플랫폼은 ntp.foreScout.net 을 액세스합니다.
135/TCP	MS-WMI	송신	Windows 엔드포인트의 원격 검사를 허용합니다.
139/TCP	SMB, MS-RPC	송신	Windows 엔드포인트(Windows 7 이하를 실행하는 엔드포인트)의 원격 검사를 허용합니다.
445/TCP			Windows 엔드포인트의 원격 검사를 허용합니다.

포트	서비스	대상 또는 출처 Forescout 플랫폼	기능
161/UDP	SNMP	송신	Forescout 플랫폼이 네트워크 스위치 및 라우터와 통신하도록 허용합니다. SNMP 구성에 대한 자세한 내용은 *Forescout 관리 가이드*를 참조하십시오.
162/UDP	SNMP	수신	Forescout 플랫폼이 네트워크 스위치 및 라우터에서 SNMP 트랩을 수신하도록 허용합니다. SNMP 구성에 대한 자세한 내용은 *Forescout 관리 가이드*를 참조하십시오.
389/TCP (636)	LDAP	송신	Forescout 플랫폼이 Active Directory 와 통신하도록 허용합니다. Forescout 플랫폼의 웹 기반 포털과 통신하도록 허용합니다.
443/TCP	HTTPS	수신	TLS 를 사용한 HTTP 리디렉션을 허용합니다.
2200/TCP	Linux 용 SecureConnector	수신	SecureConnector 가 Linux 시스템에서 어플라이언스에 대한 보안(암호화된 SSH) 연결을 생성하도록 허용합니다. *SecureConnector* 는 네트워크에 연결되어 있는 동안 Linux 엔드포인트를 관리할 수 있는 스크립트 기반 에이전트입니다.
10003/TCP	Windows 용 SecureConnector	수신	SecureConnector 가 Windows 시스템에서 어플라이언스에 대한 보안(암호화된 SSH) 연결을 생성하도록 허용합니다. *SecureConnector* 는 네트워크에 연결되어 있는 동안 Windows 엔드포인트를 관리할 수 있는 에이전트입니다. SecureConnector 에 대한 자세한 내용은 *Forescout 관리 가이드*를 참조하십시오. SecureConnector 가 어플라이언스 또는 엔터프라이즈 매니저에 연결되어 있는 경우 호스트가 할당된 어플라이언스로 리디렉션됩니다. 조직 내에서 투명한 모빌리티를 허용하도록 이 포트가 모든 어플라이언스 및 엔터프라이즈 매니저에 개방되어 있는지 확인하십시오.

포트	서비스	대상 또는 출처 Forescout 플랫폼	기능
10005/TCP	OS X 용 SecureConnector	수신	SecureConnector 가 OS X 시스템에서 어플라이언스에 대한 보안(암호화된 SSH) 연결을 생성하도록 허용합니다. *SecureConnector* 는 네트워크에 연결되어 있는 동안 OS X 엔드포인트를 관리할 수 있는 에이전트입니다. SecureConnector 에 대한 자세한 내용은 *Forescout 관리 가이드*를 참조하십시오. SecureConnector 가 어플라이언스 또는 엔터프라이즈 매니저에 연결되어 있는 경우 호스트가 할당된 어플라이언스로 리디렉션됩니다. 조직 내에서 투명한 모빌리티를 허용하도록 이 포트가 모든 어플라이언스 및 엔터프라이즈 매니저에 개방되어 있는지 확인하십시오.
13000/TCP	Forescout 플랫폼	송/수신	한 대의 어플라이언스만 있는 배포의 경우, 콘솔과 어플라이언스 간에 송수신합니다. 두 대 이상의 어플라이언스가 있는 배포의 경우, 콘솔과 어플라이언스 간에 또는 어플라이언스들 간에 송수신합니다. 어플라이언스 통신에는 TLS 를 사용한 엔터프라이즈 매니저 및 복구 엔터프라이즈 매니저와의 통신이 포함됩니다.

모니터링 인터페이스

모니터링 인터페이스를 사용하면 어플라이언스에서 네트워크 트래픽을 모니터링하고 추적할 수 있습니다. 이용 가능한 모든 인터페이스를 모니터링 인터페이스로 사용할 수 있습니다.

트래픽은 스위치의 포트에 미러링되고 어플라이언스에서 모니터링합니다. 802.1Q VLAN 태그 지정 기능의 사용 여부는 미러링되는 VLAN 의 수에 따라 달라집니다.

- ***단일 VLAN***: 모니터링 대상 트래픽이 단일 VLAN 에서 생성되는 경우 미러링된 트래픽에는 VLAN 태그를 지정할 필요가 없습니다.
- ***다중 VLAN***: 모니터링 대상 트래픽이 둘 이상의 VLAN 에서 생성되는 경우 미러링된 트래픽에는 802.1Q VLAN 태그를 지정해야 합니다.

두 스위치가 중복 쌍으로 연결되면 어플라이언스는 두 스위치 모두에서 보내는 트래픽을 모니터링해야 합니다.

모니터링 인터페이스에는 IP 주소가 필요하지 않습니다.

응답 인터페이스

어플라이언스는 응답 인터페이스를 사용하여 트래픽에 응답합니다. 응답 트래픽은 악성 활동으로부터 보호하고 정책 작업을 수행하는 데 사용됩니다. 이러한 작업에는 웹 브라우저

리디렉션 또는 세션 차단이 포함됩니다. 관련 스위치 포트의 구성은 모니터링하는 트래픽에 따라 달라집니다.

이용 가능한 모든 인터페이스를 응답 인터페이스로 사용할 수 있습니다.

- ***단일 VLAN***: 모니터링 대상 트래픽이 단일 VLAN 에서 생성되는 경우 응답 포트는 동일한 VLAN 에 속해야 합니다. 이 경우, 어플라이언스는 해당 VLAN 에 대한 단일 IP 주소가 필요합니다.
- ***다중 VLAN***: 모니터링 대상 트래픽이 둘 이상의 VLAN 에서 생성되는 경우 응답 포트는 해당 VLAN 에 대해 802.1Q VLAN 태그를 지정하여 구성해야 합니다. 어플라이언스는 각 모니터링 대상 VLAN 에 대한 IP 주소가 필요합니다.

2. 스위치 설정

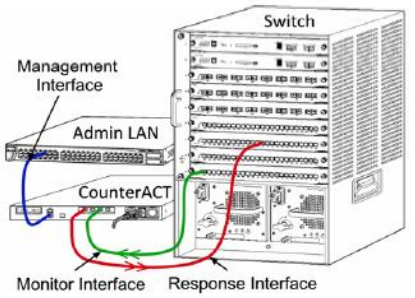
A. 스위치 연결 옵션

어플라이언스는 다양한 네트워크 환경을 원활하게 통합하기 위해 설계되었습니다. 어플라이언스를 네트워크에 성공적으로 통합하려면 스위치가 필요한 트래픽을 모니터링하도록 설정되어 있는지 확인하십시오.

여러 옵션을 이용하여 어플라이언스를 스위치에 연결할 수 있습니다.

1 표준 배포(별도의 관리, 모니터링 및 응답 인터페이스)

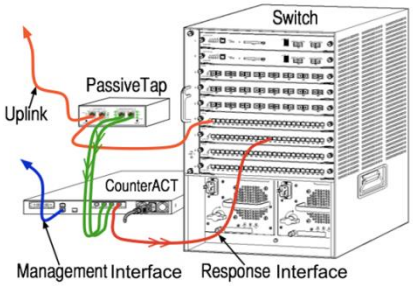
권장 배포는 3 개의 별도 포트를 사용합니다. 이러한 포트에 대해서는 어플라이언스 인터페이스 연결에서 설명합니다.



2 패시브 인라인 탭

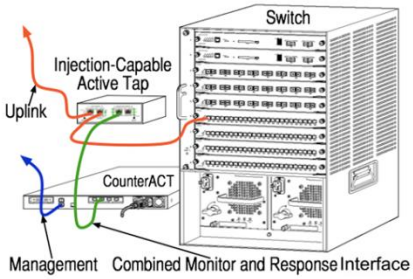
어플라이언스는 스위치 모니터 포트에 연결하는 대신 패시브 인라인 탭을 사용할 수 있습니다.

패시브 인라인 탭은 두 개의 모니터 포트가 필요합니다(각각 업스트림 트래픽용 및 다운스트림 트래픽용). 단, 두 개의 이중 통신 스트림을 단일 포트에 통합하는 *재조합* 탭은 예외입니다. 탭한 포트의 트래픽에 802.1Q VLAN 태그가 지정되는 경우 응답 포트에도 802.1Q VLAN 태그를 지정해야 합니다.



3 액티브(삽입 가능) 인라인 탭

어플라이언스는 액티브 인라인 탭을 사용할 수 있습니다. 탭이 삽입 가능한 경우 어플라이언스는 모니터 포트와 응답 포트를 통합하므로 스위치에서 별도의 응답 포트를 구성할 필요가 없습니다. 이 옵션은 업스트림 또는 다운스트림 스위치의 구성 유형에 상관없이 사용할 수 있습니다.



4 IP 레이어 응답(레이어-3 스위치 설치용)

어플라이언스는 자체 관리 인터페이스를 사용하여 트래픽에 응답할 수 있습니다. 이 옵션은 모든 모니터링 대상 트래픽에 대해 사용할 수 있지만, 어플라이언스가 VLAN 의 일부가 아닌 포트를 모니터링하므로 다른 스위치 포트를 사용하여 모니터링 대상 트래픽에 응답할 수 없는 경우에만 권장됩니다. 이는 두 라우터를 연결하는 링크를 모니터링할 때 일반적입니다. 이 옵션은 ARP(Address Resolution Protocol) 요청에 응답할 수 없으므로 어플라이언스가

모니터링 대상 서브넷에 포함된 IP 주소를 대상으로 하는 검색을 감지하는 기능이 제한됩니다. 두 라우터 간의 트래픽을 모니터링할 때는 이러한 제한이 적용되지 않습니다.

B. 스위치 설정 참고 사항

VLAN(802.1Q) 태그

- ***단일 VLAN 모니터링***: 모니터링 대상 트래픽이 단일 VLAN 에서 발생하는 경우 트래픽에는 802.1Q VLAN 태그를 지정할 필요가 없습니다.
- ***다중 VLAN 모니터링***: 모니터링 대상 트래픽이 둘 이상의 VLAN 에서 발생하는 경우 모니터 포트와 응답 포트 *모두* 802.1Q VLAN 태그를 지정해야 합니다. 다중 VLAN 모니터링은 미러링 포트의 수를 최소화하면서 최상의 전체 커버리지를 제공하므로 권장됩니다.
- 스위치가 미러링 포트에서 802.1Q VLAN 태그를 사용할 수 없는 경우 다음 중 하나를 수행하십시오.
- 단일 VLAN 만 미러링
- 태그가 지정되지 않은 단일 업링크 포트 미러링
- IP 레이어 응답 옵션 사용
- 스위치가 하나의 포트만 미러링할 수 있는 경우 단일 업링크 포트를 미러링하십시오. 해당 포트에는 태그를 지정할 수 있습니다. 일반적으로 스위치가 802.1Q VLAN 태그를 스트라이핑하는 경우 IP 레이어 응답 옵션을 사용해야 합니다.

추가 지침

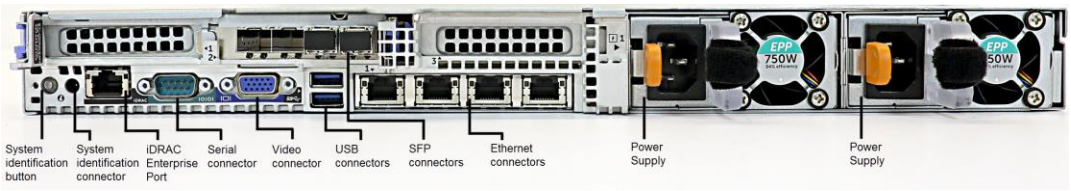
- 다음 경우 하나의 인터페이스(전송/수신 허용)만 미러링해야 합니다.
- 스위치가 전송된 트래픽과 수신된 트래픽을 모두 미러링할 수 없는 경우
- 스위치가 모든 스위치 트래픽을 미러링할 수 없는 경우
- 스위치가 VLAN 을 통한 모든 트래픽을 미러링할 수 없는 경우
- 미러링 포트에 과부하가 발생하지 않았는지 확인하십시오.
- 일부 스위치(예: Cisco 6509)에서는 새 구성을 입력하기 전에 현재 포트 구성을 완전히 삭제해야 할 수 있습니다. 오래된 포트 정보를 삭제하지 않으면 스위치가 종종 802.1Q 태그를 스트라이핑합니다.

3. 네트워크 케이블 연결 및 전원 켜기

A. 어플라이언스 패키지 해제 및 케이블 연결

1. 배송 상자에서 어플라이언스와 전원 케이블을 꺼냅니다.
2. 어플라이언스와 함께 받은 레일 키트를 꺼냅니다.
3. 레일 키트를 어플라이언스에 조립하고 어플라이언스를 랙에 장착합니다.
4. 어플라이언스 후면 패널의 네트워크 인터페이스와 스위치 포트 사이에 네트워크 케이블을 연결합니다.

*후면 패널 예제 – **Forescout** 어플라이언스*



Forescout 에서 공급한 SFP 를 Forescout 에서 테스트를 거쳐 승인한 Finisar SFP 로 교체할 수 있습니다. 자세한 내용은 *Forescout 설치 가이드*를 참조하십시오.

B. 인터페이스 할당 기록

데이터 센터에서 어플라이언스 설치를 완료하고 Forescout 콘솔을 설치하면 인터페이스 할당을 등록하라는 메시지가 표시됩니다. *채널 정의*라고도 하는 이러한 할당은 콘솔에 처음 로그인할 때 열리는 Initial Setup Wizard(초기 설정 마법사)에 입력됩니다.

물리적 인터페이스 할당을 아래에 기록한 후 콘솔에서 채널 설정을 완료할 때 사용하십시오.

Eth 인터페이스	**인터페이스 할당(예: 관리, 모니터, 응답)**
Eth0	
Eth1	
Eth2	
Eth3	
Eth4	
Eth5	
Eth6	
Eth7	

C. 어플라이언스 전원 켜기

1. 전원 케이블을 어플라이언스 후면 패널의 전원 커넥터에 연결합니다.
2. 전원 케이블의 다른 쪽을 접지된 AC 콘센트에 연결합니다.
3. 키보드와 모니터를 어플라이언스에 연결하거나 어플라이언스를 직렬 연결로 설정합니다. 자세한 내용은 *Forescout 설치 가이드*를 참조하십시오.
4. 전면 패널에서 어플라이언스의 전원을 켭니다.

4. 어플라이언스 구성

어플라이언스를 구성하기 전에 다음 정보를 준비하십시오.

어플라이언스 호스트 이름	
Forescout 관리자 비밀번호	비밀번호는 안전한 위치에 보관하십시오.
관리 인터페이스	
어플라이언스 IP 주소	
네트워크 마스크	
기본 게이트웨이 IP 주소	
DNS 도메인 이름	
DNS 서버 주소	

전원을 켜면 다음 메시지와 함께 구성을 시작하라는 메시지가 표시됩니다.

다음 메시지는 샘플입니다. 사전 설치된 일부 어플라이언스에서는 메시지가 약간 다를 수 있습니다.

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

1. **Enter** 를 누릅니다 Forescout 51xx 어플라이언스를 사용하는 경우 다음 메뉴가 표시됩니다.

```
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
```

CT-xxxx 어플라이언스를 사용하는 경우 CounterACT 7.0.0 또는 CounterACT 8.0.0 이 메뉴 상단에 버전으로 표시됩니다.

- CounterACT 7.0.0 이 표시되는 경우 버전 8.0.0 으로 업그레이드하거나 새로 설치할 수 있습니다. 자세한 내용은 *Forescout 설치 가이드*를 참조하십시오. 버전 8.0.0 으로 업그레이드하거나 설치하면 위에 나와 있는 메뉴가 표시됩니다.

- CounterACT 8.0.0 이 표시되는 경우 아래와 같이 7.0.0 을 설치하는 옵션이나 CounterACT 8.0.0 을 구성하는 옵션이 메뉴에 포함됩니다. 7.0.0 을 선택하는 경우에는 Configuration(구성) 메뉴를 통해 8.0.0 을 다시 설치할 수 없습니다. 버전 7.0.0 구성에 대한 자세한 내용은 *Forescout 설치 가이드 버전 7.0.0* 을 참조하십시오.

```
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) :
```

구성이 중단되거나 잘못된 버전을 선택한 경우 관련 버전의 ISO 파일을 사용하여 어플라이언스 이미지를 재생성해야 합니다. 어플라이언스 이미지 재생성에 관한 자세한 내용은 Forescout 설치 가이드를 참조하십시오.

2. **1** 을 입력하고 **Enter** 를 누릅니다.

```
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. **1**(Standard Installation[표준 설치])을 입력하고 **Enter** 를 누릅니다.

```
>>>>>> 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. **Yes** 를 입력하고 **Enter** 를 누릅니다.

새로 8.2 설치를 실행할 때 다음 프롬프트가 나타납니다.

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

5. 조직에서 Common Criteria(공통 기준) 및 DoDIN APL 인증을 준수해야 하는 경우가 아니라면, **No** 를 입력하고 **Enter** 를 누릅니다.

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

1) CounterACT Appliance
2) CounterACT Enterprise Manager

Choice (1-2) :
```

6. **1** 을 입력하고 **Enter** 를 누릅니다. 설정이 시작됩니다. 이 작업에는 약간의 시간이 소요될 수 있습니다.

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

1) Per Appliance licensing mode
2) Flexx licensing mode

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

7. 배포 시 사용하는 라이선싱 모드를 선택합니다. 라이선싱 모드는 구매 시 결정됩니다. ***배포 시 사용하는 라이선싱 모드를 확인할 때까지 값을 입력하지 마십시오***. 라이선싱 모드를 확인하려는 경우 또는 잘못된 모드를 입력하여 도움이 필요한 경우 Forescout 영업 담당자에게 문의하십시오.

   이 옵션은 Forescout 51xx 어플라이언스에 나타나지 않습니다.

8. Per-Appliance Licensing Mode(어플라이언별 라이선싱 모드)의 경우 **1** 을, Flexx Licensing Mode(유연 라이선싱 모드)의 경우 2 를 입력하고 **Enter** 를 누릅니다.

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

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

Description :
```

9. 설명을 입력하고 **Enter** 를 누릅니다.

   다음이 표시됩니다.

```
>>>>>> 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. Set Administrator Password(관리자 비밀번호 설정) 프롬프트에서 비밀번호로 사용할 문자열을 입력하고(문자열은 화면에 표시되지 않음) **Enter** 를 누릅니다. 비밀번호를 확인하라는 메시지가 표시됩니다. 비밀번호는 6~15 자여야 하며 알파벳이 아닌 문자를 하나 이상 포함해야 합니다.

> *어플라이언스에* cliadmin *으로 로그인하고 콘솔에 관리자로 로그인하십시오.*

11. Set Host Name(호스트 이름 설정) 프롬프트에서 호스트 이름을 입력하고 **Enter** 를 누릅니다. 호스트 이름은 콘솔에 로그인할 때 사용할 수 있으며 현재 보고 있는 CounterACT 어플라이언스를 식별하는 데 도움이 되도록 콘솔에 표시됩니다. 호스트 이름은 13 자를 초과하지 않아야 합니다.

12. Configure Network Settings(네트워크 설정 구성) 화면에 일련의 구성 매개변수가 표시됩니다. 각 프롬프트마다 값을 입력하고 **Enter** 를 눌러 다음 프롬프트를 표시합니다.

- Forescout 플랫폼 구성요소는 관리 인터페이스를 통해 통신합니다. 나열되는 관리 인터페이스의 수는 어플라이언스 모델에 따라 다릅니다.
- **Management IP address**(관리 IP 주소)는 Forescout 플랫폼 구성요소가 통신하는 인터페이스의 주소입니다. Forescout 플랫폼 구성요소 간 통신에 사용되는 인터페이스가 태그가 지정된 포트에 연결되는 경우에만 이 인터페이스에 대한 VLAN ID 를 추가하십시오.
- **DNS 서버 주소**가 둘 이상인 경우 각 주소를 공백으로 구분하십시오. 대부분의 내부 DNS 서버는 외부 주소와 내부 주소를 모두 확인하지만 외부 주소를 확인하는 DNS 서버를 포함해야 할 수 있습니다. 어플라이언스에서 수행하는 거의 모든 DNS 쿼리는 내부 주소에 대한 것이므로 외부 DNS 서버를 마지막에 나열해야 합니다.

13. Setup Summary(설정 요약) 화면이 표시됩니다. 일반 연결 테스트를 수행하거나 설정을 재구성하거나 설정을 완료하라는 메시지가 표시됩니다. **D** 를 입력하여 설정을 완료합니다.

라이선스

구성을 완료한 후 어플라이언스에 유효한 라이선스가 있는지 확인하십시오. 어플라이언스의 기본 라이선싱 상태는 배포 시 사용하는 라이선싱 모드에 따라 다릅니다.

- Forescout 배포가 ***Per-Appliance Licensing Mode***(어플라이언별 라이선싱 모드)에서 작동하는 경우 30 일 동안 유효한 데모 라이선스를 사용하여 작업을 시작할 수 있습니다. 이 기간 동안 Forescout 에서 영구 라이선스를 받아서 디스크 또는 네트워크상의 액세스 가능한 폴더에 배치해야 합니다. 30 일 데모 라이선스가 만료되기 전에 이 위치에서 라이선스를 설치하십시오. 필요 시 데모 라이선스 연장을 요청할 수 있습니다.

데모 라이선스가 곧 만료된다는 알림이 다양한 방법으로 표시됩니다. 데모 라이선스 알림에 대한 자세한 내용은 *Forescout 관리 가이드*를 참조하십시오.

Forescout 가상 시스템을 사용하여 작업하는 경우

- 이 단계에서는 데모 라이선스가 자동으로 설치되지 않습니다. Forescout 담당자가 이메일로 보내준 데모 라이선스를 설치해야 합니다.
- 최소 1 개 이상의 CounterACT 기기에서 인터넷에 액세스할 수 있어야 합니다. 이 연결은 Forescout 라이선스 서버에 대한 Forescout 라이선스의 유효성을 검사하는 데 사용됩니다. 한 달 동안 인증할 수 없는 라이선스는 해지됩니다. Forescout 플랫폼은 하루에 한 번씩 서버와의 통신 오류가 있음을 나타내는 경고 이메일을 보냅니다.

  자세한 내용은 *Forescout 설치 가이드*를 참조하십시오.

  어플라이언별 라이선싱 모드에서 라이선스 관리에 대한 자세한 내용은 *Forescout 관리 가이드*를 참조하십시오.

- Forescout 배포가 ***Flexx Licensing Mode***(유연 라이선싱 모드)에서 작동하는 경우 Forescout 고객 포털에서 라이선스 권한이 생성되어 사용 가능할 때 *Entitlement administrator*(권한 관리자)에게 이메일을 발송됩니다. 사용 가능한 경우, 콘솔에서 *Deployment administrator*(배포 관리자)를 사용하여 라이선스를 활성화할 수 있습니다. 라이선스가 활성화될 때까지, 라이선스 강제적용이 적용될 수 있으며, 특정 콘솔 구성 변경은 제한될 수도 있습니다. *데모 라이선스는 시스템 설치 중에 자동으로 설치되지 않습니다.*

  자세한 내용은 *Forescout 유연 라이선싱 방법가이드*를 참조하십시오.

5. 원격 관리

iDRAC 설정

iDRAC(Integrated Dell Remote Access Controller)는 위치/OS 에 상관없이 LAN 또는 인터넷을 통해 CounterACT 어플라이언스에 원격으로 액세스할 수 있도록 지원하는 통합 서버 시스템 솔루션입니다. 이 모듈을 사용하면 KVM 액세스, 전원 켜기/끄기/재설정, 문제 해결 및 유지 관리 작업을 수행할 수 있습니다.

iDRAC 모듈을 사용하여 작업하려면 다음을 수행하십시오.

- iDRAC 모듈 사용 및 구성
- 네트워크에 모듈 연결
- iDRAC 로그인

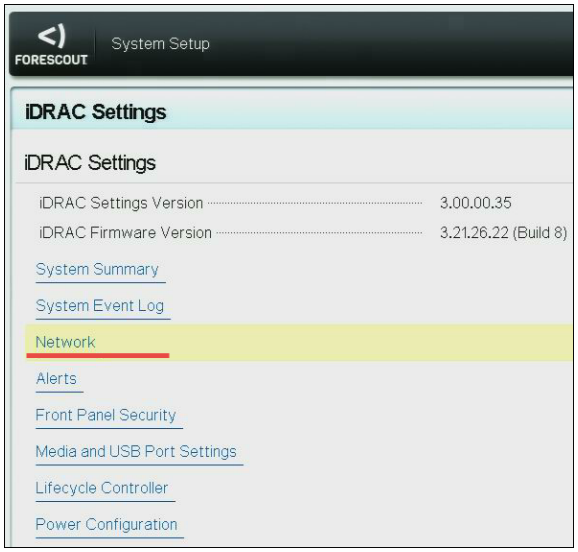
iDRAC 모듈 사용 및 구성

CounterACT 기기에서 원격 액세스를 사용하도록 iDRAC 설정을 변경하십시오. 이 섹션에서는 Forescout 플랫폼을 사용하여 작업할 때 필요한 기본 통합 설정에 대해 설명합니다.

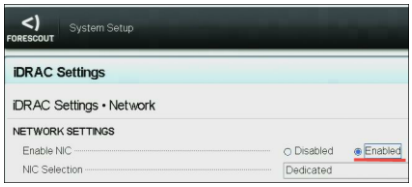
iDRAC 를 구성하려면 다음과 같이 하십시오.

1. 관리 대상 어플라이언스를 켭니다.
2. 부팅 프로세스 동안 F2 를 선택합니다.
3. System Setup Main Menu(시스템 설정 메인 메뉴) 페이지에서 **iDRAC Settings**(iDRAC 설정)을 선택합니다.

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



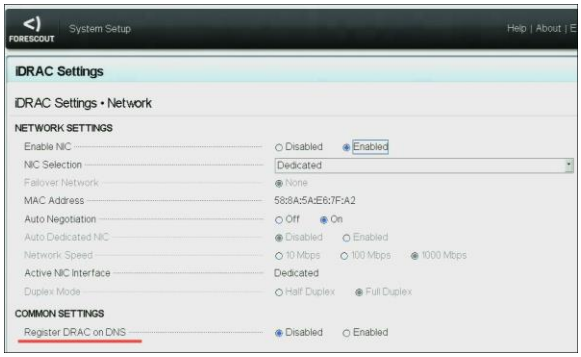
5. **iDRAC Settings** > **Network** > **Network Settings**(iDRAC 설정 > 네트워크 > 네트워크 설정)에서 *Enable NIC*(NIC 사용) 필드가 **Enabled**(사용)로 설정되어 있는지 확인합니다.



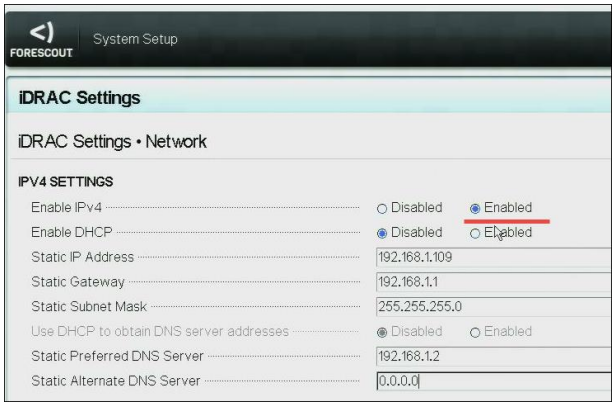
6. (옵션) **iDRAC Settings** > **Network** > **Common Settings**(iDRAC 설정 > 네트워크 > 일반 설정)에서 동적 DNS 를 업데이트하려는 경우:

   a. *Register iDRAC on DNS*(DNS 에 iDRAC 등록)을 **Enabled**(사용)로 설정합니다**.**

   b. *DNS iDRAC Name*(DNS iDRAC 이름) 필드에 동적 DNS 를 입력합니다.



7. **iDRAC Settings > Network > IPV4 Settings**(iDRAC 설정 > 네트워크 > IPV4 설정)에서:

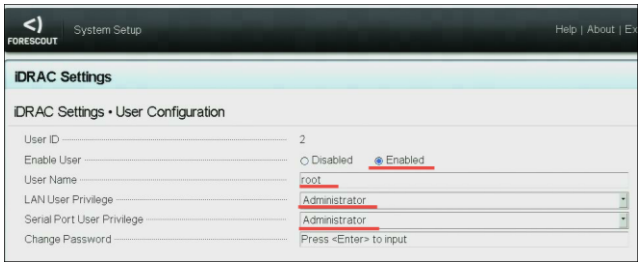


- **Enable IPv4**(IPv4 사용) 필드가 **Enabled**(사용)로 설정되어 있는지 확인합니다.
- 동적 IP 주소를 사용하려면 *Enable DHCP*(DHCP 사용) 필드를 **Enabled**(사용)로 설정합니다. DHCP 가 IP 주소, 게이트웨이, 서브넷 마스크를 iDRAC 에 자동으로 할당합니다.

  또는

  정적 IP 주소를 사용하려면 *Enable DHCP*(DHCP 사용) 필드를 Disabled(사용 안 함)로 설정하고 **Static IP Address**(정적 IP 주소), **Static Gateway**(정적 게이트웨이) 및 **Static Subnet Mask**(정적 서브넷 마스크) 필드에 값을 입력합니다.

8. **Back**(뒤로)을 선택합니다.
9. **iDRAC Settings** > **User Configuration**(iDRAC 설정 > 사용자 구성)에서**:**



'root' 사용자에 대해 다음 User Configuration(사용자 구성) 필드를 구성합니다.

- *Enable User*(사용자 활성화) 필드가 **Enabled**(활성화)로 설정되어 있는지 확인합니다.

  여기서 구성된 사용자 이름(root)는 Forescout 사용자 이름과 동일하지 않습니다.

- *LAN User Privilege(LAN 사용자 권한)*에 대해 **Administrator**(관리자)를 선택합니다.
- *Serial Port User Privilege(직렬 포트 사용자 권한)*에 대해 **Administrator**(관리자)를 선택합니다.
- *Change Password*(비밀번호 변경)에서 사용자 로그인에 필요한 비밀번호를 설정합니다

10. **Back**(뒤로)을 선택한 다음 **Finish**(마침)를 선택합니다. 변경된 설정을 확인합니다.

    구성된 설정이 저장되고 시스템이 재부팅됩니다.

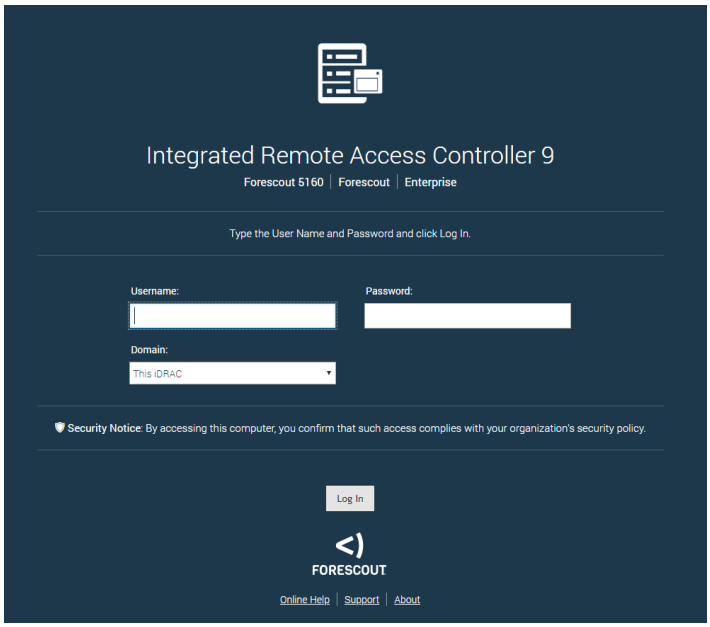
네트워크에 모듈 연결

iDRAC 가 이더넷 네트워크에 연결됩니다. 이는 관리 네트워크에 연결하는 것이 일반적입니다. 다음 이미지는 CT-1000 어플라이언스 후면 패널의 iDRAC 포트 위치를 보여줍니다.

iDRAC 로그인

iDRAC 에 로그인하려면 다음과 같이 하십시오.

1. **iDRAC Settings** > **Network**(iDRAC 설정 > 네트워크)에서 구성된 IP 주소 또는 도메인 이름으로 이동합니다.



2. iDRAC 시스템 설정의 User Configuration(사용자 구성) 페이지에 구성된 사용자 이름과 비밀번호를 입력합니다.
3. **Submit**(제출)를 선택합니다.

iDRAC 에 대한 자세한 내용은 *iDRAC 사용 설명서*를 참조하십시오. 이 가이드는 다음 위치에서 액세스할 수 있습니다:

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

사용 중인 라이선싱 모드를 확인하려면 다음과 같이 하십시오.

- 콘솔에서 **Help > About Forescout**(도움말 > Forescout 정보)를 선택합니다.

아직 수행하지 않은 경우 기본 root 비밀번호를 업데이트하는 것이 매우 중요합니다.

6. 연결 확인

관리 인터페이스 연결 확인

관리 인터페이스 연결을 테스트하려면 어플라이언스에 로그인하고 다음 명령을 실행하십시오.

fstool linktest

The following information is displayed:

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

핑 테스트 수행

어플라이언스에서 네트워크 데스크탑으로 다음 명령을 실행하여 연결을 확인하십시오.

Ping <network_desktop_IP_address>

7. Forescout 콘솔 설정

Forescout 콘솔 설치

콘솔은 엔드포인트에 대한 중요한 세부 정보를 확인하고 관리하는 데 사용되는 Forescout 관리 애플리케이션입니다. 이 정보는 CounterACT 기기에서 수집합니다. 자세한 내용은 *Forescout 관리 가이드*를 참조하십시오.

Forescout 콘솔 애플리케이션 소프트웨어를 호스팅할 시스템을 공급해야 합니다. 최소 하드웨어 요구 사항은 다음과 같습니다.

- 다음을 실행하는 비전용 시스템:
- Windows 7/8/8.1/10
- Windows Server 2008/2008 R2/2012/2012 R2/2016/2019
- Linux RHEL/CentOS 7
- 2GB RAM
- 1GB 디스크 공간

다음 방법을 사용하여 콘솔을 설치할 수 있습니다.

어플라이언스에 내장된 설치 소프트웨어를 사용하십시오.

1. 콘솔 컴퓨터에서 브라우저 창을 엽니다.
2. 다음을 브라우저 주소표시줄에 입력합니다.

   http://<Appliance_ip>/install

   여기서 Appliance_ip 는 이 어플라이언스의 IP 주소입니다. 브라우저에 콘솔 설치 창이 표시됩니다.
3. 화면에 표시되는 지침을 따릅니다.

로그인

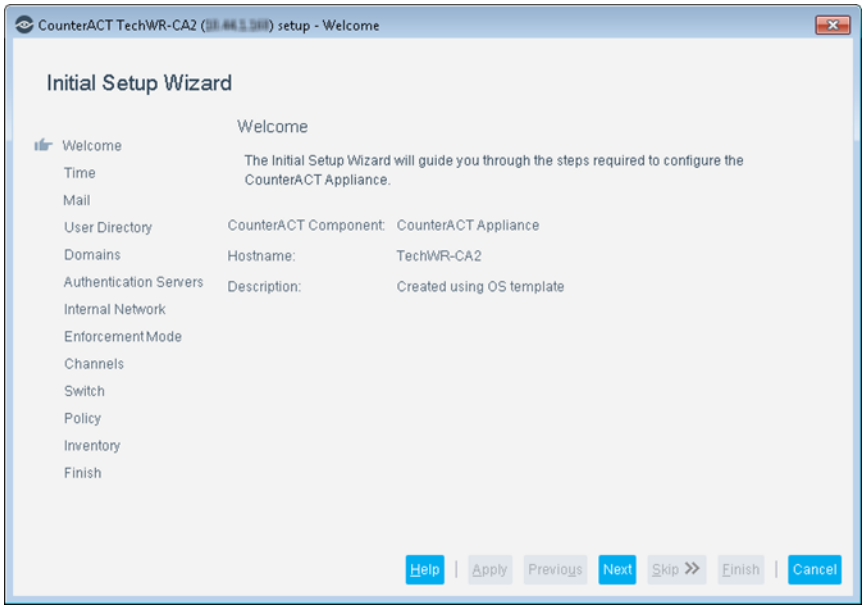
설치를 완료한 후 콘솔에 로그인할 수 있습니다.

1. 생성한 바로가기 위치에서 Forescout 아이콘을 선택합니다.

2. **IP/Name**(IP/이름) 필드에 어플라이언스의 IP 주소 또는 호스트 이름을 입력합니다.
3. **User Name**(사용자 이름) 필드에 관리자 이름을 입력합니다.
4. **Password**(비밀번호) 필드에 어플라이언스 설치 동안 생성한 비밀번호를 입력합니다.
5. **Login**(로그인)을 선택하여 콘솔을 실행합니다.

초기 설정 수행

처음 로그인할 때 Initial Setup Wizard(초기 설정 마법사)가 열립니다. 마법사는 Forescout 플랫폼을 빠르고 효율적으로 가동 및 실행하는 데 중요한 구성 단계를 안내합니다.



초기 설정을 시작하기 전에

마법사를 사용하여 작업하기 전에 다음 정보를 준비하십시오.

마법사에서 요구하는 정보	값
조직에서 사용하는 NTP 서버 주소(선택사항)	
어플라이언스에서 SMTP 트래픽이 허용되지 않는 경우 이메일 알림을 전송할 수 있는 내부 메일 릴레이 IP 주소(선택사항)	
Forescout 관리자 이메일 주소	
모니터링 인터페이스 및 응답 인터페이스	
DHCP 가 없는 세그먼트/VLAN 의 경우, 응답 인터페이스가 직접 연결되는 네트워크 세그먼트/VLAN 및 각 VLAN 에서 Forescout 플랫폼이사용할 영구 IP 주소	
이 어플라이언스가 모니터링하게 될 IP 주소 범위(미사용 주소를 포함한 모든 내부 주소)	
LDAP 사용자 계정 정보 및 LDAP 서버 IP 주소	
도메인 자격 증명(도메인 관리자 계정 이름 및 비밀번호 포함)	
Forescout 플랫폼이 성공적으로 인증된 네트워크 호스트를 분석할 수 있는 인증 서버	
스위치 IP 주소, 벤더 및 SNMP 매개변수	

마법사 사용에 대한 자세한 내용은 *Forescout 관리 가이드* 또는 온라인 도움말을 참조하십시오.

추가적인 Forescout 문서

기타 Forescout 기능 및 모듈에 대한 자세한 내용은 다음 리소스를 참조하십시오.

- 설명서 다운로드
- 설명서 포털
- Forescout 도움말 도구

설명서 다운로드

설명서는 배포 시 사용하는 라이선싱 모드에 따라 Forescout 기술 문서 페이지 또는 2 개의 Forescout 포털 중 하나에서 다운로드할 수 있습니다.

- ***Per-Appliance Licensing Mode***(어플라이언별 라이선싱 모드) - 제품 업데이트 포털
- ***Flexx Licensing Mode***(유연 라이선싱 모드) – 고객 포털

소프트웨어 다운로드도 해당 포털에서 이용할 수 있습니다.

사용 중인 라이선싱 모드를 확인하려면 다음과 같이 하십시오.

- 콘솔에서 **Help > About Forescout**(도움말 > Forescout 정보)를 선택합니다.

Forescout 기술 문서 페이지

Forescout 기술 문서 페이지에서는 검색 가능한 웹 기반 설명서 포털과 기술 문서 전반에 대한 PDF 링크를 제공합니다.

Forescout 기술 문서 페이지를 액세스하려면 다음과 같이 하십시오.

- https://www.Forescout.com/company/technical-documentation/으로 이동하여, **Technical Documentation**(기술 문서)을 선택하고 문서를 검색합니다.

제품 업데이트 포털

제품 업데이트 포털은 Forescout 버전 릴리즈, 기본 및 콘텐츠 모듈, eyeExtend 제품에 대한 링크뿐만 아니라 관련 문서에 대한 링크를 제공합니다. 또한 다양한 추가 문서도 이 포털에 나와 있습니다.

제품 업데이트 포털에 액세스하려면 다음과 같이 하십시오.

- https://updates.forescout.com/support/index.php?url=counteract 로 이동하여 찾을 버전을 선택합니다.

고객 포털

Forescout 고객 포털의 Downloads(다운로드) 페이지는 Forescout 버전 릴리즈, 기본 및 콘텐츠 모듈, eyeExtend 제품을 구매할 수 있는 링크뿐 아니라 관련 문서에 대한 링크를

제공합니다. 소프트웨어 및 관련 문서는 소프트웨어에 대한 라이선스 권한이 있는 경우에만 Downloads(다운로드) 페이지에 표시됩니다.

Forescout 고객 포털에서 설명서에 액세스하려면 다음과 같이 하십시오.

- https://Forescout.force.com/support/로 이동하여 **Downloads**(다운로드)를 선택합니다.

설명서 포털

Forescout 설명서 포털은 Forescout 도구, 특징, 기능 및 통합에 대한 정보가 포함되어 있는 검색 가능한 웹 기반 라이브러리입니다.

배포 시 Flexx Licensing Mode(유연 라이선싱 모드)를 사용하는 경우 이 포털에 액세스할 수 있는 자격 증명을 받지 않았을 수 있습니다.

설명서 포털에 액세스하려면 다음과 같이 하십시오.

- https://updates.forescout.com/support/files/counteract/docs_portal/로 이동하여 고객 지원 자격 증명을 사용하여 로그인합니다.

Forescout 도움말 도구

콘솔에서 직접 정보를 액세스합니다.

콘솔 도움말 버튼

진행 중인 작업과 주제에 대한 정보에 신속하게 액세스하려면 상황에 맞는 *Help*(도움말) 버튼을 사용합니다.

Forescout 관리 가이드

- **Help**(도움말) 메뉴에서 **Administration Guide**(관리 가이드)를 선택합니다.

플러그인 도움말 파일

- 플러그인을 설치한 후, **Tools** > **Options** > **Modules**(도구 > 옵션> 모듈)을 선택하고 플러그인을 선택한 후 **Help**(도움말)를 선택합니다.

설명서 포털

- **Help**(도움말) 메뉴에서 **Documentation Portal**(설명서 포털)을 선택하여 설명서 포털에 액세스할 수 있습니다.