# FireSIGHT 사용자 에이전트 컨피그레이션 가이드

버전 2.2
2014년 6월 23일 화요일



**Cisco Systems, Inc.**
www.cisco.com
Cisco는 전 세계에 200개가 넘는 지사를 운영하고 있습니다.
각 지사의 주소, 전화번호 및 팩스 번호는 다음 Cisco 웹사이트에 나와 있습니다.
www.cisco.com/go/offices.

동봉된 제품의 소프트웨어 라이센스 및 제한 보증은 제품과 함께 제공되는 정보 패킷에 설명되어 있으며 본 참조 문서에 통합되어 있습니다. 소프트웨어 라이센스 또는 제한 보증을 찾을 수 없는 경우 CISCO 담당자에게 사본을 요청해 주십시오.

Cisco의 TCP 헤더 압축은 UNIX 운영 체제의 UCB 공개 도메인 버전의 일부로서 University of California, Berkeley(UCB)에서 개발된 프로그램을 적용하여 구현합니다. All rights reserved. Copyright © 1981, Regents of the University of California.

여기에 언급된 기타 모든 보증에도 불구하고 이러한 공급자의 모든 문서 및 소프트웨어는 모든 결함이 포함된 "있는 그대로" 제공됩니다. CISCO 및 위에 언급된 모든 공급업체는 상품성, 특정 목적에의 적합성, 타인의 권리 비침해 또는 처리, 사용, 거래 행위로 발생하는 문제에 대한 묵시적 보증을 포함하여(단, 이에 한하지 않음) 묵시적이든 명시적이든 모든 종류의 보증을 부인합니다.

Cisco 또는 해당 공급업체는 피해의 가능성에 대해 언급한 경우라도 이 설명서의 사용 또는 사용 불능으로 인해 발생하는 이익 손실, 데이터 손실 또는 손상을 포함하여(단, 이에 한하지 않음) 간접, 특별, 중대 또는 부수적 손해에 대해 어떠한 경우라도 책임을 지지 않습니다.

Cisco 및 Cisco 로고는 미국 및 기타 국가에서 Cisco Systems, Inc. 및/또는 계열사의 상표 또는 등록 상표입니다. Cisco 상표 목록을 확인하려면 www.cisco.com/go/trademarks로 이동하십시오. 언급된 서드파티 상표는 해당 소유주의 재산입니다. 파트너라는 용어의 사용이 Cisco와 다른 업체 사이의 제휴 관계를 의미하는 것은 아닙니다. (1110R)

이 문서에서 사용된 모든 IP(인터넷 프로토콜) 주소와 전화 번호는 실제 주소와 전화 번호가 아닙니다. 이 문서에 포함된 예제, 명령 표시 출력, 네트워크 토폴로지 다이어그램 및 다른 그림은 이해를 돕기 위한 자료일 뿐이며, 실제 IP 주소나 전화번호가 사용되었다면 이는 의도하지 않은 우연의 일치입니다.

# 목 차


1장 **소개** 1-1

사용자 에이전트 버전 2.2에 대한 주요 변경 사항 1-1

사용자 에이전트 이해 1-1

사용자 에이전트 기능 이해 1-2

레거시 에이전트 지원 이해 1-4

버전 5.x의 에이전트 및 액세스 제어 이해 1-4

사용자 데이터베이스 이해 1-4

사용자 활동 데이터베이스 이해 1-5

액세스 제어된 사용자 데이터베이스 이해 1-5

사용자 데이터 수집 제한 사항 1-6

2장 **사용자 에이전트 설정** 2-1

버전 4.x 방어 센터 연결 준비 2-2

버전 5.x 방어 센터 연결 준비 2-3

방어 센터에서 사용자 에이전트 설정 2-3

사용자 엑세스 제어를 허용하기 위한 LDAP 연결 설정 2-4

Active Directory 서버에 연결하는 권한 컨피그레이션 2-4

유휴 세션 시간 초과 활성화 2-5

사용자 에이전트 설치를 위한 컴퓨터 준비 2-7

사용자 에이전트 컨피그레이션 백업 2-7

사용자 에이전트 설치 2-8

사용자 에이전트 구성 2-9

사용자 에이전트 구성 Active Directory 서버 연결 2-10

사용자 에이전트 방어 센터연결 구성 2-13

사용자 이름이 제외된 사용자 에이전트 설정 구성 2-14

주소가 제외된 사용자 에이전트 설정 구성 2-16

사용자 에이전트 로깅 설정 구성 2-17

일반 사용자 에이전트 설정 구성 2-18

사용자 에이전트 유지 관리 설정 구성 2-19


# 소개

버전 2.2의 사용자 에이전트는 FireSIGHT 시스템 관리 디바이스와 함께 사용자 데이터를 수집합니다. 버전 5.x의 FireSIGHT 시스템이 포함된 에이전트를 사용하는 경우 사용자 에이전트가 사용자 액세스 컨트롤을 구현하는 데에도 필수적입니다.

사용자 에이전트는 LDAP를 통해 인증된 Microsoft Active Directory 서버 및 보고 로그인 및 로그오프를 모니터링합니다. FireSIGHT 시스템은 이러한 레코드를 관리되는 디바이스에 의한 직접 네트워크 트래픽 관찰을 통해 수집한 정보와 통합합니다.

자세한 내용은 다음 섹션을 참고하십시오.


- 사용자 에이전트 버전 2.2에 대한 주요 변경 사항, 1-1페이지
- 사용자 에이전트 이해, 1-1페이지


## 사용자 에이전트 버전 2.2에 대한 주요 변경 사항

사용자 에이전트를 버전 2.2로 업그레이드하는 경우 다음 변경 사항에 유의해 주십시오.

- 버전 2.0~버전 2.1.1의 에이전트를 제거하는 경우 컨피그레이션 설정을 유지하려면 데이터베이스를 백업해야 합니다. 자세한 내용은 사용자 에이전트 컨피그레이션 백업, 2-7페이지를 참조하십시오.

  그러나, 에이전트 버전 2.2는 향후 자동으로 업그레이드할 수 있도록 컨피그레이션 설정을 유지합니다. 에이전트 버전 2.2를 제거 및 재설치하는 경우 수동으로 데이터베이스를 백업할 필요가 없습니다.
- 에이전트는 구성된 Active Directory 서버에 대한 로그인을 탐지할 수 있습니다. 연결을 구성할 경우, **Local Login IP Address(로컬 로그인 IP 주소)** 필드에서 IP 주소를 선택합니다.
- 구성된 Active Directory 서버 연결은 최대 64자의 문자로 구성된 사용자 비밀번호를 지원합니다.
- 에이전트는 이제 1분 및 5분의 **활성 디렉터리 서버 최대 폴링 시간**을 지원합니다. 최대 폴링 시간이 짧을수록 실시간 모니터링 성능과 로그아웃 탐지 성능이 향상될 수 있습니다.

## 사용자 에이전트 이해

이 섹션에서는 FireSIGHT 시스템에서 사용자 검색을 구현하는 데 있어 사용자 에이전트의 역할에 초점을 맞추고 있습니다. 사용자 검색 및 네트워크 검색(또는 버전 4.x 문서의 RNA)과 관련된 모든 개념에 대한 더 자세한 내용은 장치에서 실행되는 FireSIGHT 시스템 버전의 *FireSIGHT 시스템 사용 설명서*를 참조하십시오.

자세한 내용은 다음 섹션을 참고하십시오.


- 사용자 에이전트 기능 이해, 1-2페이지
- 레거시 에이전트 지원 이해, 1-4페이지
- 버전 5.x의 에이전트 및 액세스 제어 이해, 1-4페이지
- 사용자 데이터베이스 이해, 1-4페이지
- 사용자 활동 데이터베이스 이해, 1-5페이지
- 액세스 제어된 사용자 데이터베이스 이해, 1-5페이지
- 사용자 데이터 수집 제한 사항, 1-6페이지


# 사용자 에이전트 기능 이해

FireSIGHT 시스템은 조직의 LDAP 서버에서 사용자 ID 및 사용자 활동 정보를 얻을 수 있습니다. 사용자 에이전트를 이용하면 Microsoft Active Directory 서버에 대한 Active Directory 자격 증명으로 인증하는 경우 사용자를 모니터링할 수 있습니다.

모니터링하려는 Microsoft Active Directory 서버에 대한 TCP/IP 액세스를 포함한 Microsoft Windows Vista, Microsoft Windows 7, Microsoft Windows 8, Microsoft Windows Server 2003, Microsoft Windows Server 2008 또는 Microsoft Windows Server 2012에 에이전트를 설치할 수 있습니다. 또한 지원되는 운영 체제 중 하나를 실행하는 Active Directory 서버에 설치할 수도 있습니다.

각 에이전트는 정기적으로 예약된 폴링 또는 실시간 모니터링을 사용해 암호화된 트래픽을 사용하여 로그인을 모니터링할 수 있습니다. 워크스테이션에서 또는 원격 데스크톱 로그인을 통해 사용자가 컴퓨터에 로그인하면 Active Directory 서버에 의해 로그인이 생성됩니다.

에이전트에서는 사용자 로그오프도 모니터링 및 보고할 수 있습니다. 사용자가 호스트 IP 주소에서 로그아웃할 때 에이전트 자체에 의해 로그오프가 생성됩니다. 호스트에 로그인한 사용자가 변경된 것을 에이전트에서 탐지하는 경우에도(Active Directory 서버에서 그러한 변경 사항을 보고하기 전에) 로그오프가 생성됩니다. 로그오프 데이터를 로그인 데이터와 결합하면 사용자의 네트워크 로그인에 대한 좀 더 완전한 상황을 파악할 수 있습니다.

Active Directory 서버 폴링을 통해 에이전트는 정의된 폴링 간격으로 일련의 사용자 활동 데이터를 검색할 수 있습니다. Active Directory 서버가 데이터를 받자마자 실시간 모니터링이 사용자 활동 데이터를 에이전트로 전송합니다.

특정 사용자 이름 또는 IP 주소와 연결된 모든 로그인 또는 로그오프는 보고에서 제외하도록 에이전트를 구성할 수 있습니다. 파일 공유와 인쇄 서버 등 공유 서버에 대한 반복적인 로그인 및 문제 해결 목적으로 컴퓨터에 로그인하는 사용자는 제외하는 것이 좋습니다.

최대 5개의 서버를 모니터링하고 암호화된 데이터를 최대 5개의 방어 센터로 전송하도록 각 에이전트를 구성할 수 있습니다.

에이전트는 제외된 사용자 이름 또는 IP 주소 외에 탐지된 모든 로그인 및 로그오프의 레코드를 방어 센터로 전송합니다. 그러면 해당 레코드는 사용자 활동으로 보고됩니다. 에이전트는 방어 센터 버전을 탐지하고, 적절한 데이터 형식으로 로그인 레코드를 전송합니다. 이는 관리되는 디바이스에 의해 직접 탐지되는 사용자 활동을 보완합니다. 액세스 컨트롤 수행을 위해 버전 5.x의 FireSIGHT 시스템을 사용하는 경우 사용자 에이전트가 보고한 로그인이 사용자와 IP 주소를 연결할 수 있으므로 사용자 조건으로 액세스 컨트롤 규칙이 트리거될 수 있습니다.

사용자 에이전트는 사용자가 네트워크에 로그인할 때 또는 기타 이유로 Active Directory 자격 증명에 대해 계정을 인증할 때 사용자를 모니터링합니다. 버전 2.2 사용자 에이전트 버전 2.2는 호스트에 대한 인터랙티브 사용자 로그인, 원격 데스크톱 로그인, 파일 공유 인증, 컴퓨터 계정 로그인은 물론 사용자 로그오프 및 사용자 로그오프 시 원격 데스크톱 세션도 탐지합니다.

탐지된 로그인 유형에 따라 에이전트가 로그인을 보고하는 방법 및 호스트 프로필에 로그인이 표시되는 방법이 결정됩니다. 호스트에 대한 *권한 있는 사용자 로그인*의 경우 새 로그인의 사용자로 변경되도록 현재 사용자가 호스트 IP 주소에 매핑됩니다. 호스트의 기존 사용자가 호스트에 대해 권한 있는 사용자 로그인을 가지고 있지 않으면, 다른 로그인은 현재 사용자를 변경하지 않거나 호스트에 대한 현재 사용자만 변경합니다. 이러한 경우 예상 사용자가 더 이상 로그인하지 않으면 에이전트는 해당 사용자에 대해 로그오프를 생성합니다. 호스트의 기존 사용자가 호스트에 대해 권한 있는 사용자 로그인을 가지고 있지 않으면, 네트워크 검색에 의해 탐지된 사용자 로그인은 호스트에 대한 현재 사용자만 변경합니다. 에이전트에서 탐지한 로그인은 네트워크 맵에 다음과 같은 영향을 미칩니다.

- 사용자 또는 원격 데스크톱 로그인의 호스트에 대한 인터랙티브 로그인을 탐지하면 에이전트는 호스트에 대해 권한 있는 사용자 로그인을 보고하고 호스트의 현재 사용자를 새 사용자로 변경합니다.
- 파일 공유 인증을 위한 로그인을 탐지하면 에이전트는 호스트에 대한 사용자 로그인을 보고하되, 호스트의 현재 사용자를 변경하지 않습니다.
- 호스트에 대한 컴퓨터 계정 로그인을 탐지하면 에이전트는 NetBIOS Name Change 검색 이벤트를 생성하며 호스트 프로필은 NetBIOS 이름에 대한 변경 사항을 반영합니다.
- 제외된 사용자 이름의 로그인을 탐지하면 에이전트는 방어 센터에 로그인을 보고하지 않습니다.

로그인 또는 기타 인증이 발생하면 에이전트는 다음 정보를 방어 센터에 전송합니다.

- 사용자의 LDAP 사용자 이름
- 로그인 및 기타 인증 시간
- 사용자 호스트의 IP 주소 및 링크 로컬 주소(에이전트가 컴퓨터 계정 로그인에 대해 IPv6 주소를 보고하는 경우)

**참고** 사용자가 Windows 컴퓨터에 로그인하는 데 원격 데스크톱을 사용하는 경우 에이전트가 로그인을 탐지하면 Linux 컴퓨터 IP 주소가 아닌 Windows 컴퓨터 IP 주소를 방어 센터에 보고합니다.

방어 센터는 로그인 및 로그오프 정보를 사용자 활동으로 기록합니다. User Agent가 사용자 로그인 또는 로그오프에서 사용자 데이터를 보고하면, 보고된 사용자가 사용자 목록을 기준으로 점검됩니다. 보고된 사용자가 에이전트에서 보고한 기존 사용자와 일치하면 보고된 데이터가 사용자에게 할당됩니다. 보고된 사용자가 기존 사용자와 일치하지 않으면 새 사용자가 생성됩니다.

제외된 사용자 이름과 연결된 사용자 활동이 보고되지 않더라도 관련 사용자 활동은 계속 보고될 수 있습니다. 컴퓨터에 대한 첫 번째 로그인에 이어 두 번째 로그인이 탐지된 상태에서 두 번째 사용자 로그인과 연결된 사용자 이름을 보고에서 제외한 경우, 에이전트는 원래 사용자에 대한 로그오프를 보고합니다. 그러나 두 번째 사용자에 대한 로그인은 보고되지 않습니다. 그 결과, 제외된 사용자가 호스트에 로그인한 경우에도 사용자가 IP 주소에 매핑되지 않습니다.

에이전트에서 탐지한 사용자 이름에 대한 다음 제한 사항을 참고하십시오.

- 버전 5.0.2 이상의 방어 센터로 보고된, 달러 기호 문자($)로 끝나는 사용자 이름은 네트워크 맵을 업데이트하지만 사용자 로그인으로 표시되지는 않습니다. 에이전트는 달러 표시($)로 끝나는 사용자 이름을 다른 버전의 방어 센터로 보고하지 않습니다.
- 방어 센터에서 유니코드 문자가 포함된 사용자 이름을 표시하는 데에는 제한 사항이 있을 수 있습니다.

방어 센터가 저장할 수 있는 탐지된 총 사용자 수는 RNA 또는 FireSIGHT 라이센스에 따라 다릅니다. 라이센스 사용자 제한에 도달하면 대부분의 경우 시스템은 데이터베이스에 대한 새 사용자 추가를 중지합니다. 새 사용자를 추가하려면 데이터베이스에서 오래된 사용자 또는 비활성 사용자를 수동으로 삭제하거나 모든 사용자를 삭제해야 합니다.

# 레거시 에이전트 지원 이해

Active Directory LDAP 서버에 설치된 버전 1.0(레거시) 사용자 에이전트는 Active Directory 서버에서 단일 방어 센터로 사용자 로그인 데이터를 계속해서 전송할 수 있습니다. 레거시 에이전트의 구축 요구 사항 및 탐지 기능은 변함 없습니다. Active Directory 서버에 이를 설치해야 정확히 하나의 방어 센터에 연결할 수 있습니다. 그러나 User Agent Status Monitor 상태 모듈은 레거시 에이전트를 지원하지 않으며 연결된 레거시 에이전트를 통해 방어 센터에서 활성화해서는 안 된다는 점에 유의하십시오. 레거시 에이전트에 대한 지원은 단계적으로 중단되므로 향후 릴리스 준비 차원으로 가능한 한 빨리 버전 2.2 사용자 에이전트를 사용하여 배포를 업그레이드하도록 계획해야 합니다.

# 버전 5.x의 에이전트 및 액세스 제어 이해

**라이센스:** 제어

조직에서 Microsoft Active Directory LDAP 서버를 사용할 경우, Cisco는 Active Directory 서버를 통해 사용자 활동을 모니터링하는 사용자 에이전트를 설치할 것을 권장합니다. 사용자 제어를 수행하려면 **반드시** 버전 5.x의 사용자 에이전트를 설치하여 사용해야 합니다. 이 에이전트는 사용자를 IP 주소와 연결하며, 이에 따라 사용자 조건이 있는 액세스 제어 규칙이 트리거될 수 있습니다. 에이전트 하나를 사용하면 최대 5개의 Active Directory 서버에서 사용자 활동을 모니터링할 수 있습니다.

에이전트를 사용하려면 에이전트에 연결된 각 방어 센터와 모니터링되는 LDAP 서버 간에 연결을 구성해야 합니다. 이러한 연결을 활용하면 User Agents에서 로그인 및 로그오프가 탐지된 사용자의 메타데이터를 검색할 수 있을 뿐만 아니라, 액세스 제어 규칙을 사용할 사용자 및 그룹을 지정할 수도 있습니다. 사용자 검색을 위해 LDAP 서버를 구성하는 방법에 대한 자세한 내용은 *FireSIGHT 시스템사용 설명서*를 참고하십시오.

**참고** Microsoft Active Directory 서버에 설치하는 레거시 에이전트도 Active Directory 자격 증명에 대한 인증 시 사용자를 모니터링합니다. 하지만, 향후 릴리스에서 레거시 에이전트에 대한 지원이 중단될 것을 대비해 가능한한 빨리 버전 2.2의 사용자 에이전트로 전환해야 합니다.

# 사용자 데이터베이스 이해

**라이센스:** FireSIGHT

사용자 데이터베이스에는 관리되는 디바이스 또는 사용자 에이전트에 의해 탐지된 각 사용자에 대한 레코드가 포함되어 있습니다. 방어 센터가 저장할 수 있는 탐지된 총 사용자 수는 FireSIGHT 라이센스에 따라 다릅니다. 라이센스 제한에 도달하면 대부분의 경우 시스템은 데이터베이스에 대한 새 사용자 추가를 중지합니다. 새 사용자를 추가하려면 데이터베이스에서 오래된 사용자 또는 비활성 사용자를 수동으로 삭제하거나 모든 사용자를 삭제해야 합니다.

그러나 시스템은 권한 있는 사용자 로그인을 선호합니다. 제한에 도달한 상태에서 시스템이 전에 탐지하지 못한 권한 있는 사용자의 로그인을 탐지하면, 오랫동안 비활성 상태를 유지한 사용자를 삭제하고 새로운 사용자를 대신 추가합니다.

사용자 데이터베이스의 내용은 방어 센터 웹 인터페이스를 통해 볼 수 있습니다. 탐지된 사용자를 보고 검색하고 삭제하는 방법에 대한 자세한 내용은 *FireSIGHT 시스템사용 설명서*를 참고하십시오.

# 사용자 활동 데이터베이스 이해

**라이센스:** FireSIGHT

사용자 활동 데이터베이스에는 Sourcefire 사용자 에이전트로 모니터링되는 Active Directory LDAP 서버에 대한 연결을 통한 또는 네트워크 검색을 통한 네트워크상의 사용자 활동 레코드가 포함되어 있습니다. 시스템에서는 다음과 같은 상황에서 이벤트를 기록합니다.

- 개별 로그인 또는 로그오프를 탐지한 경우
- 새 사용자를 탐지한 경우
- 수동으로 사용자를 삭제한 경우
- 데이터베이스에 없는 사용자를 탐지했으나 FireSIGHT 라이센스 제한 때문에 사용자를 추가할 수 없는 경우

시스템에서 탐지한 사용자 활동을 보려면 방어 센터 웹 인터페이스를 사용할 수 있습니다. 사용자 활동을 보고 검색하고 삭제하는 방법에 대한 자세한 내용은 *FireSIGHT 시스템사용 설명서*를 참고하십시오. FireSIGHT 시스템 사용자 에이전트 버전 2.2를 사용하여 LDAP 로그인 데이터를 버전 5.x 방어 센터에 전송하려는 경우, 에이전트가 연결할 각 방어 센터에서 각 에이전트에 대한 연결을 구성해야 합니다. 이렇게 하면 에이전트는 방어 센터와 안전한 연결을 설정하여 로그인 데이터를 전송할 수 있습니다. 특정 사용자 이름을 제외하도록 에이전트를 구성한 경우 해당 사용자 이름의 로그인 데이터는 방어 센터에 보고되지 않습니다.

또한 사용자 액세스 제어를 구현하려는 경우, 데이터를 수집할 각 Microsoft Active Directory 서버에 대해 사용자 인식 매개 변수를 구성하여 연결을 설정해야 합니다.

# 액세스 제어된 사용자 데이터베이스 이해

**라이센스:** 제어

액세스 제어된 사용자 데이터베이스에는 액세스 제어 규칙에 사용할 수 있는 사용자 및 그룹이 포함되므로, FireSIGHT 시스템을 통한 사용자 제어를 수행할 수 있습니다. 이러한 사용자는 다음의 두 유형 중 하나일 수 있습니다.

- *액세스 제어된 사용자* - 사용자 제어를 수행하기 위해 액세스 제어 규칙에 추가할 수 있는 사용자. 방어 센터-LDAP 서버 연결을 구성할 때 액세스 제어된 사용자가 소속될 그룹을 지정합니다.
- *액세스 제어되지 않은 사용자*는 기타 탐지된 사용자입니다.

방어 센터가 저장할 수 있는 액세스 제어된 총 사용자 수는 FireSIGHT 라이센스에 따라 다릅니다.

방어 센터-LDAP 서버 연결을 구성할 때 액세스 제어된 사용자가 소속될 그룹을 지정합니다 (*FireSIGHT 시스템사용 설명서* 설명 참고).

FireSIGHT 시스템 사용자 에이전트 버전 2.2를 사용하여 LDAP 로그인 및 로그오프 데이터를 버전 5.x 방어 센터에 전송하려는 경우, 에이전트가 연결할 각 방어 센터에서 각 에이전트에 대한 연결을 구성해야 합니다. 이렇게 하면 에이전트는 방어 센터와 안전한 연결을 설정하여 사용자 활동 데이터를 전송할 수 있습니다.

특정 사용자 이름을 제외하도록 에이전트를 구성한 경우 해당 사용자 이름의 사용자 활동 데이터는 방어 센터에 보고되지 않습니다. 이러한 제외된 사용자 이름은 데이터베이스에 남아 있지만 IP 주소와는 연결되지 않습니다.

또한 사용자 액세스 제어를 구현하려는 경우, 데이터를 수집할 각 Microsoft Active Directory 서버에 대해 사용자 인식 매개 변수를 구성하여 연결을 설정해야 합니다.

# 사용자 데이터 수집 제한 사항

**라이센스:** FireSIGHT

다음 표에서는 일반적이거나 에이전트와 특히 관련된 사용자 데이터 수집 제한 사항에 대해 설명합니다.

***표 1-1 사용자 데이터 수집 제한 사항***

| 제한 사항 | 설명 |
|---|---|
| 사용자 제어 | 사용자 제어를 수행하려면 조직에서 **반드시** Microsoft Active Directory LDAP 서버를 사용해야 합니다. 시스템은 액세스 제어 규칙에 사용할 수 있는 사용자 및 그룹을 Active Directory에서 가져오며, Active Directory 서버에 설치된 User Agents에서 보고하는 로그인 및 로그오프로 사용자를 IP 주소에 연결합니다. |
| 로그인 탐지 | 에이전트는 버전 5.2 이상을 실행하는 방어 센터로 IPv6 주소의 호스트에 대한 사용자 로그인을 보고합니다.<br>에이전트는 버전 5.0.1 이상을 실행하는 방어 센터에 무단 사용자 로그인 및 NetBIOS 로그인을 보고합니다.<br>에이전트는 버전 4.10.x 이상을 실행하는 방어 센터로 실제 사용자 이름의 권한 있는 로그인을 보고합니다.<br>Active Directory 서버에 대한 로그인을 탐지하려는 경우 Active Directory 서버 연결을 서버 IP 주소로 구성해야 합니다. 자세한 내용은 사용자 에이전트 구성 Active Directory 서버 연결, 2-10페이지를 참고하십시오.<br>여러 사용자가 원격 세션을 사용해서 한 호스트에 로그인하는 경우 에이전트는 해당 호스트의 로그인을 제대로 탐지하지 못할 수 있습니다. 이를 방지하는 방법에 대한 자세한 내용은 유휴 세션 시간 초과 활성화, 2-5페이지를 참고하십시오. |
| 로그오프 탐지 | 에이전트는 버전 5.2 이상의 방어 센터에 팀지된 로그오프를 보고합니다.<br>로그오프는 즉시 탐지되지 않을 수 있습니다. 로그오프와 연결된 타임스탬프는, 사용자가 더 이상 호스트 IP 주소에 매핑되지 않음을 에이전트가 탐지한 시간입니다. 이는 사용자가 호스트에서 로그오프한 실제 시간과 일치하지 않을 수 있습니다.<br>사용자가 호스트 IP 주소에서 로그아웃할 때 에이전트 자체에 의해 로그오프가 생성됩니다. 호스트에 로그인한 사용자가 변경된 것을 에이전트에서 탐지하는 경우에도(Active Directory 서버에서 그러한 변경 사항을 보고하기 전에) 로그오프가 생성됩니다. |
| 실시간 데이터 검색 | Active Directory 서버는 Windows Server 2008 또는 Windows Server 2012를 실행해야 합니다. |
| 서로 다른 사용자가 동일한 호스트에 다중 로그인 | 시스템은 특정 시점에 어느 한 호스트에 한 사용자만 로그인하며 호스트의 현재 사용자가 마지막 권한 있는 사용자 로그인이라고 가정합니다. 권한 없는 로그인만 호스트에 로그인한 경우 권한 없는 최근 로그인이 현재 사용자로 간주됩니다. 원격 세션을 통해 여러 사용자가 로그인한 경우 Active Directory 서버에서 보고한 마지막 사용자가 방어 센터에 보고된 사용자입니다. |

*표 1-1 사용자 데이터 수집 제한 사항 (계속)*

| 제한 사항 | 설명 |
|---|---|
| 동일한 사용자가 동일한 호스트에 다중 로그인 | 시스템은 특정 호스트에 대한 사용자의 첫 번째 로그인만 기록하고 이후의 로그인은 무시합니다. 개별 사용자가 특정 호스트에 로그인하는 유일한 사람인 경우, 시스템에서는 원래 로그인만 기록합니다.<br>그러나 또 다른 사용자가 해당 호스트에 로그인하면 시스템에서는 새 로그인을 기록합니다. 그런 다음 원래 사용자가 다시 로그인하면 새 로그인이 기록됩니다. |
| 유니코드 문자 | 유니코드 문자의 사용자 이름은 사용자 인터페이스에 정확하게 표시되지 않을 수 있습니다.<br>에이전트는 버전 4.10.x의 방어 센터로 유니코드 문자가 포함된 사용자 이름을 보고하지 않습니다. |
| 사용자 데이터베이스의 LDAP 사용자 계정 | 사용자 인식이나 RUA LDAP 서버에서 LDAP 사용자를 제거 또는 비활성화하거나 방어 센터에 대한 보고에서 사용자 이름을 제외하는 경우, 방어 센터는 해당 사용자를 사용자 데이터베이스에서 제거하지 않으며 해당 사용자는 데이터베이스에 나열된 사용자의 라이센스 제한에서 계속 계산됩니다. 사용자를 데이터베이스에서 직접 삭제해야 합니다. 버전 5.x의 경우 사용자 라이센스 제한은 액세스 제어된 사용자에 대해 병렬로 적용됩니다. 액세스 제어된 사용자에 대한 사용자 카운트는 LDAP 컨피그레이션에 의해 검색되는 사용자 수에 따라 달라집니다. |


# 사용자 에이전트 설정

Microsoft Active Directory 서버에서 사용자 로그인 데이터를 수집하고 이를 방어 센터로 보내는 데 사용자 에이전트 버전 2.2를 사용하려면 우선 설치한 후 이를 각 방어 센터 및 Microsoft Active Directory 서버에 연결하고 일반 설정을 구성해야 합니다.

**사용자 에이전트 설정 방법:**

**액세스:** Admin

**1단계** 에이전트를 설치할 컴퓨터의 IP 주소에서 에이전트 연결을 허용하기 위해서는 각 방어 센터를 구성하십시오. 자세한 내용은 다음을 참고하십시오.

- 버전 4.x 방어 센터 연결 준비, 2-2페이지
- 버전 5.x 방어 센터 연결 준비, 2-3페이지

**참고** 사용자 제어를 수행하는 데 버전 5.x 방어 센터를 사용하려는 경우 방어 센터의 Microsoft Active Directory 서버에 대한 사용자 인식 매개변수를 이용하여 LDAP 연결을 구성해야 합니다.

**2단계** 에이전트가 Active Directory 서버와 연결하도록 허용하는 데 필요한 Windows와 사용자 권한을 구성합니다. 자세한 내용은 Active Directory 서버에 연결하는 권한 컨피그레이션, 2-4페이지를 참고하십시오.

**3단계** 또는, 유휴 원격 세션에 대한 시간 초과를 활성화합니다. 자세한 내용은 유휴 세션 시간 초과 활성화, 2-5페이지를 참고하십시오.

**4단계** 에이전트를 설치할 컴퓨터에 필수 프로그램을 설치합니다. Active Directory 서버에 대한 컴퓨터의 TCP/IP 액세스를 설정합니다. 자세한 내용은 Active Directory 서버에 연결하는 권한 컨피그레이션, 2-4페이지를 참고하십시오.

**5단계** 또는, 이전 버전 사용자 에이전트의 컨피그레이션 설정을 유지하기 위해 에이전트 데이터베이스 백업을 수행할 수도 있습니다. 자세한 내용은 사용자 에이전트 컨피그레이션 백업, 2-7페이지를 참고하십시오.

**6단계** 컴퓨터에 에이전트를 설치합니다. 자세한 내용은 사용자 에이전트 설치, 2-8페이지를 참고하십시오.

**7단계** 최대 5대의 Microsoft Active Directory 서버에 대한 연결을 구성합니다. 또는, 에이전트에 대한 폴링 간격 및 최대 폴링 시간을 구성합니다. 자세한 내용은 사용자 에이전트 구성 Active Directory 서버 연결, 2-10페이지를 참고하십시오.

**8단계** 최대 5개의 방어 센터 연결을 구성합니다. 자세한 내용은 사용자 에이전트 방어 센터연결 구성, 2-13페이지를 참고하십시오.

**9단계** 또는, 로그인 및 로그오프 데이터에 대한 폴링에서 제외할 사용자 이름 및 IP 주소 목록을 구성합니다. 자세한 내용은 사용자 이름이 제외된 사용자 에이전트 설정 구성, 2-14페이지 및 주소가 제외된 사용자 에이전트 설정 구성, 2-16페이지를 참고하십시오.

**10단계** 또는, 에이전트 로깅 설정을 구성합니다. 자세한 내용은 사용자 에이전트 로깅 설정 구성, 2-17페이지를 참고하십시오.

**11단계** 또는, 에이전트 이름을 구성하고 서비스를 시작 및 중지하고 서비스의 현재 상태를 확인합니다. 자세한 내용은 일반 사용자 에이전트 설정 구성, 2-18페이지를 참고하십시오.

**12단계** **Save(저장)**를 클릭하여 에이전트 구성을 저장합니다.

**주의** 지원 담당자의 안내를 받은 경우를 제외하고 에이전트 관리 설정을 수정하지 **마십시오**.

# 버전 4.x 방어 센터 연결 준비

사용자 에이전트를 사용하여 LDAP 사용자 로그인 정보를 수집하는 첫 단계는 Active Directory 서버에 연결하려는 에이전트와의 연결을 허용하도록 각 방어 센터를 구성하는 것입니다. 이 섹션에서는 버전 4.x 방어 센터에 대한 에이전트 연결 인증 절차에 대해 설명합니다.

**User Agent에 연결하도록 방어 센터를 구성하려면**

**액세스:** Admin

**1단계** **Operations(작동) > Configuration(컨피그레이션) > RUA**를 선택합니다.

**2단계** **RUA Agent Add(에이전트 추가)**를 클릭합니다.

**3단계** **Name(이름)** 필드에 에이전트를 쉽게 이해할 수 있는 이름을 입력합니다.

**4단계** **Hostname or IP Address(호스트 이름 또는 IP 주소)** 필드에 사용자 에이전트가 상주하게 될 컴퓨터의 IP 주소나 호스트 이름을 입력합니다. 반드시 IPv4 주소를 사용해야 합니다. IPv6 주소를 사용하여 사용자 에이전트에 연결하는 데 방어 센터를 구성할 수 **없습니다**.

**참고** IPv6 주소를 포함한 사용자 에이전트나 IPv6 주소를 확인하는 호스트 이름을 추가할 수 없습니다.

**5단계** **RUA Agent Add(에이전트 추가)**를 클릭합니다.

방어 센터는 구성된 IP 주소의 에이전트에서 연결을 허용하도록 구성됩니다.

**팁** 방어 센터 에이전트 연결을 삭제하려면 삭제하려는 연결 옆에 있는 **Delete(삭제)**를 클릭합니다.

**6단계** Active Directory 서버에 연결하는 권한 컨피그레이션, 2-4페이지를 계속 진행합니다.

# 버전 5.x 방어 센터 연결 준비

사용자 에이전트 버전 2.2를 사용하여 LDAP 로그인 데이터를 버전 5.x 방어 센터에 전송하려는 경우, 에이전트가 연결할 각 방어 센터에서 각 에이전트에 대한 연결을 구성해야 합니다. 이렇게 하면 에이전트는 방어 센터와 안전한 연결을 설정하여 데이터를 전송할 수 있습니다.

또한 사용자 액세스 제어를 구현하려는 경우, 데이터를 수집할 각 Microsoft Active Directory 서버에 대해 사용자 인식 매개 변수를 구성하여 연결을 설정해야 합니다.

자세한 내용은 다음 섹션을 참고하십시오.


- 방어 센터에서 사용자 에이전트 설정, 2-3페이지
- 사용자 엑세스 제어를 허용하기 위한 LDAP 연결 설정, 2-4페이지


## 방어 센터에서 사용자 에이전트 설정

사용자 에이전트를 사용하여 LDAP 사용자 로그인 정보를 수집하는 첫 단계는 Active Directory 서버에 연결하려는 에이전트와의 연결을 허용하도록 각 방어 센터를 구성하는 것입니다. 이 장에서는 버전 5.x 방어 센터에 대한 에이전트 연결 인증 절차를 설명합니다.

**User Agent에 연결하도록 방어 센터를 구성하려면**

**액세스:** Admin/Discovery Admin

**1단계** **Policies(정책) > Users(사용자)**를 선택합니다.

**2단계** **Add User Agent(사용자 에이전트 추가)**를 클릭합니다.

**3단계** **Name(이름)** 필드에 에이전트를 쉽게 이해할 수 있는 이름을 입력합니다.

**4단계** **Hostname or IP Address(호스트 이름 또는 IP 주소)** 필드에 에이전트가 상주하게 될 컴퓨터의 IP 주소나 호스트 이름을 입력합니다. 반드시 IPv4 주소를 사용해야 합니다. IPv6 주소를 사용하여 사용자 에이전트에 연결하는 데 방어 센터를 구성할 수 **없습니다**.

**참고** IPv6 주소를 포함한 사용자 에이전트나 IPv6 주소를 확인하는 호스트 이름을 추가할 수 없습니다.

**5단계** **Add User Agent(사용자 에이전트 추가)**를 클릭합니다.

방어 센터는 이제 구성된 호스트에서 사용자 에이전트에 연결합니다.

**6단계** 다음 옵션을 이용할 수 있습니다.

- 사용자 제어를 수행하고자 한다면 사용자 엑세스 제어를 허용하기 위한 LDAP 연결 설정, 2-4페이지를 계속하십시오.
- 사용자 제어를 수행하지 않으려면 Active Directory 서버에 연결하는 권한 컨피그레이션, 2-4페이지를 계속하십시오.

# 사용자 엑세스 제어를 허용하기 위한 LDAP 연결 설정

사용자 제어를 수행(즉, 사용자 조건으로 액세스 제어 규칙 작성)하려면 방어 센터 및 조직의 Microsoft Active Directory 서버 중 하나 이상 사이에 연결을 구성하고 활성화해야 합니다. *LDAP 연결* 또는 *사용자 인식 인증 개체*라고 하는 이 컨피그레이션에는 서버에 대한 인증 필터 설정과 연결 설정이 포함되어 있습니다. 연결의 사용자 및 그룹 액세스 제어 매개 변수는 액세스 제어 규칙에서 사용할 수 있는 그룹과 사용자를 지정합니다.

**참고** 사용자 제어를 수행하려면 Microsoft Active Directory를 **반드시** 사용해야 합니다. 시스템은 Active Directory 서버에서 실행 중인 사용자 에이전트를 사용하여 사용자와 IP 주소를 연결하며, 이를 통해 액세스 제어 규칙이 트리거됩니다.

사용자 인식 컨피그레이션을 통한 LDAP 연결 설정에 대한 자세한 내용은 *FireSIGHT 시스템 사용 설명서*를 참고하십시오.

# Active Directory 서버에 연결하는 권한 컨피그레이션

모든 에이전트 전제조건을 충족하는 컴퓨터를 준비한 후 Active Directory 서버가 로그인 데이터를 이 로그에 기록할 수 있도록 Active Directory 보안 로그가 활성화되어 있는지 확인합니다. 그런 다음, 로그인 데이터나 선택적으로 로그오프 데이터를 검색하기 위해 에이전트가 Active Directory 서버와 통신하고 보안 로그에 액세스할 수 있도록 사용자 권한 및 Windows 보안 권한을 구성합니다.

**Active Directory 서버가 로그인 데이터를 기록하는지 확인하는 방법:**

**1단계** Active Directory 서버에서, **Start(시작) > All Programs(모든 프로그램) > Administrative Tools(관리 도구) > Event Viewer(이벤트 뷰어)**를 선택합니다.

**2단계** **Windows Logs(Windows 로그) > Security(보안)**를 선택합니다.

로깅이 활성화된 경우, 보안 로그가 표시됩니다. 로깅이 비활성화된 경우 보안 로깅 활성화에 대한 정보는 http://technet.microsoft.com/en-us/library/cc779487(v=ws.10).aspx를 참고하십시오.

**에이전트가 Active Directory 서버와 통신할 수 있게 하는 방법:**

**1단계** Active Directory 서버에서 원격 관리 방화벽 규칙을 활성화합니다. 다음 옵션을 이용할 수 있습니다.

- Active Directory 서버가 Windows Server 2003을 실행하는 경우, http://technet.microsoft.com/en-us/library/cc738900%28v=ws.10%29.aspx에서 자세한 내용을 참고하십시오.
- Active Directory 서버가 Windows Server 2008 또는 Windows Server 2012를 실행하는 경우, http://msdn.microsoft.com/en-us/library/aa822854%28VS.85%29.aspx에서 자세한 내용을 참고하십시오.

**로그인 데이터를 검색하기 위한 에이전트 권한을 부여하는 방법:**

**1단계** 에이전트를 설치한 컴퓨터에서 사용자를 생성합니다.

**참고** Active Directory 서버 연결을 구성할 때 이 지격 증명을 사용합니다. 자세한 내용은 사용자 에이전트 구성 Active Directory 서버 연결, 2-10페이지를 참조하십시오.

**2단계** 사용자의 Active Directory 서버에서 RPC를 활성화합니다. 다음 옵션을 이용할 수 있습니다.

- Active Directory 서버에서 Windows Server 2008 R2 또는 Windows Server 2012를 실행하며 사용자가 관리자 그룹의 구성원이 아닌 경우, 사용자에게 DCOM 원격 액세스, 원격 실행 및 활성화 권한을 부여합니다. 자세한 내용은 http://msdn.microsoft.com/en-us/library/Aa393266.aspx를 참고하십시오.
- Active Directory 서버가 지원되는 다른 버전의 Microsoft Windows를 실행하는 경우 RPC는 활성화되어 있습니다.

**로그오프 데이터를 검색하기 위한 에이전트 권한을 부여하는 방법:**

**1단계** Active Directory 서버에 대한 인증을 수행하는 모든 워크스테이션에 사용자가 로그인할 수 있도록 하기 위해 생성된 사용자 관리자 권한을 부여합니다.

**보안 로그에 액세스할 수 있는 에이전트 권한을 부여하는 방법:**

**1단계** Active Directory 서버의 WMI Root/CIMV2 네임 공간에 대해 생성된 사용자 전체 권한을 부여합니다. 자세한 내용은http://technet.microsoft.com/en-us/library/cc787533%28v=WS.10%29.aspx를 참고하십시오.

유휴 세션 시간 초과 활성화, 2-5페이지를 계속 진행합니다.

# 유휴 세션 시간 초과 활성화

Active Directory 서버에 연결할 수 있는 권한을 구성한 후 선택적으로 그룹 정책에서 유휴 세션 시간 초과를 활성화할 수도 있습니다. 이렇게 하면 에이전트가 호스트의 여러 세션으로 인해 관련 없는 로그인을 감지하고 보고하는 것을 방지할 수 있습니다.

터미널 서비스를 이용하면 여러 사용자가 동시에 서버에 로그인할 수 있습니다. 유휴 세션 시간 초과를 활성화하면 서버에 로그인된 여러 세션의 인스턴스를 줄일 수 있습니다.

원격 데스크톱을 이용하면 한 번에 한 사용자가 워크스테이션에 원격으로 로그인할 수 있습니다. 하지만 해당 사용자가 로그아웃하지 않고 원격 데스크톱 세션 연결을 취소하게 되면 세션이 활성 상태로 유지됩니다. 사용자 입력이 없을 경우 활성 세션은 결국 유휴 상태로 전환됩니다. 또 다른 사용자가 원격 데스크톱을 사용하여 해당 워크스테이션에 로그인하면 두 세션이 실행됩니다. 실행 세션이 여러 개인 경우 에이전트가 관련 없는 로그인을 보고할 수 있습니다. 유휴 세션 시간 초과를 활성화하면 정의된 유휴 시간 초과 시간이 경과하면 해당 세션이 종료되므로 호스트에서 여러 원격 세션이 실행되는 것을 방지할 수 있습니다.

Citrix 세션은 원격 데스크톱 세션과 유사하게 작동합니다. 여러 Citrix 사용자 세션이 동시에 한 컴퓨터에서 실행될 수 있습니다. 유휴 세션 시간 초과를 활성화하면 호스트에서 여러 Citrix 세션이 실행되는 것을 방지하여 관련 없는 로그인 보고를 줄일 수 있습니다.

구성된 세션 시간 초과에 따라 한 컴퓨터에 여러 세션이 로그인되는 경우도 있을 수 있다는 점에 유의하십시오.

**터미널 서비스 세션 시간 초과를 활성화하는 방법:**

**1단계** 유휴 터미널 서비스 세션 시간 초과 및 연결 해제된 터미널 서비스 세션 시간 초과의 그룹 정책 설정을 업데이트합니다. 다음 옵션을 이용할 수 있습니다.

- Active Directory 서버가 Windows Server 2008 또는 Windows Server 2012를 실행 하는 경우, http://technet.microsoft.com/en-us/library/cc754272(v=ws.10).aspx에서 세션 시간 초과를 활성화하는 방법에 대한 자세한 내용을 참고하십시오.
- Active Directory 서버가 Windows Server 2003을 실행하는 경우, http://technet.microsoft.com/en-us/library/cc758177(v=ws.10).aspx에서 세션 시간 초과를 활성화하는 방법에 대한 자세한 내용을 참고하십시오.

유휴 및 연결 해제된 세션이 다음 로그오프 확인 전에 시간 초과될 수 있도록 세션 시간 초과 시간을 구성된 로그오프 확인 빈도보다 짧게 설정합니다. 필수 유휴 세션 또는 연결 해제 세션 시간 초과가 있는 경우, 구성된 로그오프 확인 빈도를 세션 시간 초과보다 길게 설정합니다. 로그오프 확인 빈도 컨피그레이션에 대한 자세한 내용은 일반 사용자 에이전트 설정 구성, 2-18페이지를 참고하십시오.

**원격 데스크톱 세션 시간 초과를 활성화하는 방법:**

**1단계** 유휴 원격 세션 시간 초과 및 연결 해제된 세션 시간 초과의 그룹 정책 설정을 업데이트합니다. 세션 시간 초과 활성화에 대한 자세한 내용은 http://technet.microsoft.com/en-us/library/ee791886%28v=ws.10%29.aspx를 참고하십시오.

유휴 및 연결 해제된 세션이 다음 로그오프 확인 전에 시간 초과될 수 있도록 세션 시간 초과 시간을 구성된 로그오프 확인 빈도보다 짧게 설정합니다. 필수 유휴 세션 또는 연결 해제 세션 시간 초과가 있는 경우, 구성된 로그오프 확인 빈도를 세션 시간 초과보다 길게 설정합니다. 로그오프 확인 빈도 컨피그레이션에 대한 자세한 내용은 일반 사용자 에이전트 설정 구성, 2-18페이지를 참고하십시오.

**Citrix 세션 시간 초과를 활성화하는 방법:**

**1단계** http://support.citrix.com/에서 Citrix의 온라인 설명서를 참조하십시오.

사용자 에이전트 설치를 위한 컴퓨터 준비, 2-7페이지를 계속 진행합니다.

# 사용자 에이전트 설치를 위한 컴퓨터 준비

각 사용자 에이전트를 설치하려는 Windows 컴퓨터에 연결할 방어 센터를 구성한 후 다음 전제조건으로 Windows 컴퓨터를 설정합니다.

- 컴퓨터에서는 Windows Vista, Windows 7, Windows 8, Windows Server 2003, Windows Server 2008, Windows Server 2012 등이 실행됩니다. 컴퓨터는 Active Directory 서버일 필요가 없습니다.
- 컴퓨터에는 Microsoft .NET Framework 버전 4.0 Client Profile 및 Microsoft SQL CE(SQL Server Compact) 버전 3.5도 설치되어 있어야 합니다. 프레임워크는 Microsoft에서 .NET Framework 버전 4.0 클라이언트 프로파일 재배포 가능 패키지(`dotNetFx40_Client_x86_x64.exe`)로 제공됩니다. SQL CE는 Microsoft에서 실행 파일(`SSCERuntime-ENU.exe`)로 제공됩니다.

**참고** .NET Framework 및 SQL CE가 모두 설치되지는 않은 상태에서 에이전트 실행 파일(`Setup.exe`)을 열면 적합한 파일을 다운로드하라는 메시지가 표시됩니다. 자세한 내용은 사용자 에이전트 설치, 2-8페이지 항목을 참조하십시오.

- 컴퓨터에는 모니터링하려는 Active Directory 서버에 대한 TCP/IP 액세스가 있으며 Active Directory 서버와 동일한 버전의 인터넷 프로토콜을 사용합니다. 에이전트가 Active Directory 서버를 실시간으로 모니터링하는 경우, 로그인 데이터를 검색할 수 있도록 컴퓨터의 TCP/IP 액세스가 항상 켜져 있어야 합니다.
- 컴퓨터에는 데이터 및 IPv4 주소를 보고하고자 하는 방어 센터에 대한 TCP/IP 액세스가 있습니다.
- IPv6 주소로 호스트에서의 로그오프를 감지하고자 하는 경우, 컴퓨터에는 IPv6 주소가 있으며, IPv4 주소로 호스트에서의 로그오프를 감지하려는 경우 IPv4 주소가 있습니다.
- 컴퓨터에는 레거시 에이전트나 버전 2.x의 에이전트가 아직 설치되어 있지 않습니다. 이러한 에이전트는 자동으로 설치 제거되지 않으므로 기존 에이전트를 설치 제거하려면 제어판에서 **Add/Remove Programs(프로그램 추가/제거)**를 엽니다.

**주의** 이전 버전의 사용자 에이전트가 설치되어 있는 경우 컨피그레이션 설정을 유지하려면 반드시 데이터베이스 백업을 완료해야 합니다.

사용자 에이전트 컨피그레이션 백업, 2-7페이지를 계속 진행합니다.

# 사용자 에이전트 컨피그레이션 백업

이전 버전의 사용자 에이전트가 설치되어 있는 경우 새로운 버전의 사용자 에이전트를 설치하면 기존 컨피그레이션이 제거됩니다. 이 컨피그레이션 설정을 보존하려면 새로운 버전의 사용자 에이전트를 설치하기 전에 데이터베이스를 백업하십시오.

**참고** 버전 2.2 이상의 사용자 에이전트가 설치되어 있다면 데이터베이스를 백업할 필요가 없습니다. 새로운 버전의 사용자 에이전트를 설치할 때 컨피그레이션 설정을 자동으로 가져옵니다. 사용자 에이전트 설치, 2-8페이지를 계속 진행합니다.

**컨피그레이션 설정을 유지하는 방법:**

**1단계** 에이전트를 설치한 컴퓨터에서, **Start(시작) > Programs(프로그램) > Sourcefire > Configure User Agent(사용자 에이전트 구성)**를 선택합니다.

**2단계** 에이전트 서비스를 중지하려면 중지 버튼( )을 클릭합니다.

**3단계** 에이전트가 설치된 컴퓨터에서 `C:\SourcefireUserAgent.sdf`를 찾아 해당 파일을 로컬에 복사합니다.

**4단계** 제어판으로 이동하고 **Add/Remove Programs(이 프로그램 추가/제거)**를 열어 Sourcefire 사용자 에이전트를 설치 제거합니다. 에이전트를 제거합니다.

**5단계** 최신 버전의 사용자 에이전트를 설치합니다. 자세한 내용은 사용자 에이전트 설치, 2-8페이지 항목을 참조하십시오.

**6단계** 에이전트를 설치한 컴퓨터에서, **Start(시작) > Programs(프로그램) > Sourcefire > Configure User Agent(사용자 에이전트 구성)**를 선택합니다.

**7단계** 에이전트 서비스를 중지하려면 중지 버튼( )을 클릭합니다.

**8단계** 최신 버전의 에이전트가 설치된 컴퓨터에서 `C:\SourcefireUserAgent.sdf`를 찾습니다. 현재 파일을 이전 버전의 에이전트에서 만든 로컬 백업과 교체합니다.

**9단계** 최신 버전의 에이전트를 설치한 컴퓨터에서, **Start(시작) > Programs(프로그램) > Sourcefire > Configure User Agent(사용자 에이전트 구성)**를 선택합니다.

**10단계** 시작하려면 재생 버튼( )을 클릭합니다. 에이전트 서비스가 시작됩니다.

사용자 에이전트 구성, 2-9페이지를 계속 진행합니다.

# 사용자 에이전트 설치

**라이센스:** FireSIGHT

Active Directory 서버에 연결할 권한을 구성하고 유휴 원격 세션 시간 초과 구성 여부를 결정한 후 에이전트를 설치합니다.

**주의** 이전 버전의 사용자 에이전트가 설치되어 있는 경우 컨피그레이션 설정을 유지하려면 설치하기 전에 데이터베이스를 백업해야 합니다. 자세한 내용은 사용자 에이전트 컨피그레이션 백업, 2-7페이지 항목을 참조하십시오.

에이전트는 **로컬 시스템** 계정을 사용하는 서비스로 실행됩니다. 에이전트가 실행되고 있는 Windows 컴퓨터가 네트워크에 연결되어 있다면 사용자가 해당 컴퓨터에 활성 로그인 상태가 아닌 경우에도 서비스가 사용자 데이터를 폴링하고 전송하는 작업을 계속 진행합니다.

**참고** 서비스 컨피그레이션을 변경하지 마십시오. 에이전트는 다른 계정을 사용하여 제대로 작동하지 않습니다.

각 에이전트에 대해 Active Directory 서버 및 5개의 방어 센터에 대한 연결을 구성할 수 있습니다. 방어 센터 연결을 추가하기 전에, 방어 센터 컨피그레이션에 에이전트를 추가하십시오. 자세한 내용은 버전 4.x 방어 센터 연결 준비, 2-2페이지 또는 버전 5.x 방어 센터 연결 준비, 2-3페이지를 참조하십시오.

고가용성 컨피그레이션에서는 기본 및 보조 데이터 센터에 데이터가 남아 있을 수 있도록 양쪽에 대한 사용자 로그인 데이터 업데이트를 활성화하기 위해 에이전트에 두 방어 센터를 추가합니다.

**사용자 에이전트를 설치하는 방법:**

**액세스:** 모두

**1단계** 지원 사이트에서 사용자 에이전트 설치 파일(`Sourcefire_User_Agent_2.2-9_Setup.zip`)을 다운로드합니다.

**참고** 지원 사이트에서 설치 파일을 직접 다운로드하고 이메일을 통해 이를 전달하지 마십시오. 설치 파일을 이메일로 전송하는 경우 손상될 수 있습니다.

**2단계** 설치 파일을 에이전트를 설치하려는 Windows 컴퓨터에 복사하고 파일의 압축을 풉니다.

에이전트를 설치하는 데에는 3MB의 하드 드라이브 공간이 필요합니다. Cisco는 에이전트 로컬 데이터베이스를 위해 하드 드라이브에 4GB의 공간을 할당할 것을 권장합니다.

**3단계** 설치 실행 파일(`Setup.exe`)을 엽니다.

**팁** 관리자 그룹의 구성원이 아닌 계정을 사용하고 Windows 컴퓨터에 새 애플리케이션을 설치하는 데 필요한 권한을 보유하지 않은 경우 설치를 시작하는 데 적합한 권한을 보유한 그룹에 속해 있는 사용자에게 인계해야 합니다. 에스컬레이션 옵션에 액세스하려면, `Setup.exe` 파일을 마우스 오른쪽 버튼으로 클릭하고 **Run As(다음 자격으로 실행)**를 선택합니다. 적합한 사용자를 선택하고 해당 사용자의 비밀번호를 입력합니다.

**4단계** 에이전트를 설치하려는 Windows 컴퓨터에 Microsoft .NET Framework 버전 4.0 Client Profile 및 SQL CE 버전 3.5가 설치되어 있지 않다면 적합한 파일을 다운로드하라는 메시지가 표시됩니다. 파일을 다운로드하고 설치합니다.

**5단계** 마법사의 지시를 따라 에이전트를 설치합니다.

**6단계** 에이전트 구성을 시작하려면 사용자 에이전트 구성, 2-9페이지를 참고하십시오.

# 사용자 에이전트 구성

**라이센스:** FireSIGHT

에이전트가 설치되면 Active Directory 서버에서 데이터를 수신하고 방어 센터로 정보를 보고하며 보고에서 특정 사용자 이름 및 IP 주소를 제외하고 로컬 이벤트 로그나 Windows 애플리케이션 로그에 상태 메시지를 기록하도록 구성할 수 있습니다.

**에이전트를 구성하는 방법:**

**액세스:** 모두

**1단계** 에이전트를 설치한 컴퓨터에서, **Start(시작) > Programs(프로그램) > Sourcefire > Configure Sourcefire User Agent(Sourcefire 사용자 에이전트 구성)**를 선택합니다.

다음 표는 에이전트 구성 시 수행해야 할 작업과 이를 구성할 수 있는 위치를 설명해 줍니다.

*표 2-1 사용자 에이전트 컨피그레이션 작업*

| 목적 | 방법 |
|---|---|
| 에이전트 이름을 변경하고 로그오프 확인 빈도를 변경하며 서비스를 시작 및 중지하고 우선순위 일정을 설정할 수 있습니다. | **General(일반)** 탭을 선택합니다. 자세한 내용은 일반 사용자 에이전트 설정 구성, 2-18페이지를 참고하십시오. |
| Active Directory 서버를 추가, 수정 또는 제거하고 실시간 Active Directory 서버 데이터 검색을 활성화하고 Active Directory 서버 폴링 간격 및 최대 폴링 시간을 수정합니다. | **Active Directory Servers(Active Directory 서버)** 탭을 선택합니다. 자세한 내용은 사용자 에이전트 구성 Active Directory 서버 연결, 2-10페이지를 참고하십시오. |
| 방어 센터를 추가 또는 제거 | **Sourcefire DC** 탭을 선택합니다. 자세한 내용은 사용자 에이전트 방어 센터연결 구성, 2-13페이지을/를 참조하십시오. |
| 보고에서 제외된 사용자 이름을 추가, 수정 또는 제거합니다. | **Excluded Usernames(제외된 사용자 이름)** 탭을 선택합니다. 자세한 내용은 사용자 이름이 제외된 사용자 에이전트 설정 구성, 2-14페이지를 참고하십시오. |
| 보고에서 제외된 IP 주소를 추가, 수정 또는 제거합니다. | **Excluded Addresses(제외된 주소)** 탭을 선택합니다. 자세한 내용은 주소가 제외된 사용자 에이전트 설정 구성, 2-16페이지를 참조하십시오. |
| 이벤트 로그를 확인, 내보내기 및 삭제하고 Windows 애플리케이션 로그에 로깅하며 얼마나 오랫동안 메시지를 보존할 것인지를 수정합니다. | **Logs(로그)** 탭을 선택합니다. 자세한 내용은 사용자 에이전트 로깅 설정 구성, 2-17페이지를 참고하십시오. |
| 지원 담당자의 지시에 따라 문제 해결 및 유지보수 작업을 수행합니다. | **Logs(로그)** 탭을 선택하고 **Show Debug Messages in Log(로그에서 디버그 메시지 보기)**를 활성화한 다음 **Maintenance(유지 관리)** 탭을 선택합니다. 자세한 내용은 사용자 에이전트 유지 관리 설정 구성, 2-19페이지를 참고하십시오. |
| 에이전트 설정 변경 사항 저장 | **Save(저장)**를 클릭합니다. 변경 사항이 저장되지 않았음을 알려주는 메시지가 **Save(저장)** 아래에 표시됩니다. |
| 에이전트 설정에 대한 변경 사항을 저장하지 않고 에이전트를 닫습니다. | **Cancel(취소)**을 클릭합니다. |

# 사용자 에이전트 구성 Active Directory 서버 연결

**라이센스:** FireSIGHT

에이전트에서 Active Directory 서버에 대한 연결을 최대 5개 추가하여 다음에 대해 구성할 수 있습니다.

- 에이전트가 로그인 및 로그오프 데이터를 실시간으로 검색할 수 있게 할 것인지 주기적으로 Active Directory 서버에서 데이터를 풀링할 수 있게 할 것인지 여부
- 에이전트가 얼마나 자주 사용자 활동 데이터를 폴링하게 할 것인지, 또는 연결이 끊어진 경우 Active Directory 서버와의 실시간 연결을 설정 또는 다시 설정하려는 시도를 얼마나 자주 할 것인지 여부

- 에이전트가 로그인에 대해 Active Directory 서버 자체에 보고하는 IP 주소
- 에이전트에서 Active Directory 서버와의 연결을 설정 또는 재설정할 경우 검색할 수 있는 로그인 및 로그오프 데이터의 양

에이전트가 실시간으로 데이터를 검색하도록 구성되어 있고 실시간 모니터링을 사용할 수 없을 경우 대신 에이전트가 실시간 모니터링이 다시 제공될 때까지 데이터를 위해 Active Directory 서버의 폴링을 시도합니다.

**팁** 사용자 에이전트가 검색한 사용자 활동량이 상당할 경우, Cisco는 실시간 데이터 검색 대신 폴링을 구성할 것을 권장합니다. 활동이 많은 환경에서는 1분의 폴링 간격을 구성하고 최대 폴링 길이는 10분을 넘지 않게 구성합니다.

Windows Server 2003을 실행하는 경우 에이전트가 Active Directory 서버를 실시간으로 모니터링하도록 구성할 수 없다는 점에 유의하십시오. 실시간 모니터링에는 Windows Server 2008 이상을 실행하는 Active Directory 서버가 필요합니다.

에이전트에서 탭이 선택되면 해당 시점의 현재 Active Directory 서버 폴링 상태, 에이전트에 보고된 최종 로그인, 에이전트가 Active Directory 서버를 폴링한 최근 시간을 확인할 수 있습니다. 또한 에이전트가 실시간으로 Active Directory 서버를 폴링하고 있는지 여부와 탭이 선택된 시점의 실시간 데이터 검색 상태를 확인할 수도 있습니다. 서버 상태에 대한 자세한 내용은 다음 표를 참고하십시오.

*표 2-2 Active Directory 서버 상태*

| Active Directory 서버 상태 | 폴링 가용성 | 실시간 가용성 |
|---|---|---|
| 사용 가능 | 서버는 폴링할 수 있습니다. | 서버는 실시간 데이터 검색을 사용할 수 있습니다. |
| 사용 불가능 | 서버는 폴링할 수 없습니다. | 서버는 실시간 데이터 검색을 사용할 수 없거나 폴링을 하도록 구성되었습니다. |
| 대기 중 | 서버 컨피그레이션이 추가되었으나 아직 저장되지 않았습니다. | 서버 컨피그레이션이 추가되었으나 아직 저장되지 않았습니다. |
| 알 수 없음 | 에이전트가 시작되었지만 상태는 아직 사용할 수 없거나 에이전트가 아직 Active Directory 서버를 확인하지 않았습니다. | 에이전트가 시작되었지만 상태는 아직 사용할 수 없거나 에이전트가 아직 Active Directory 서버를 확인하지 않았습니다. |

**참고** 각 에이전트가 다른 연결을 감지하여 관련이 없는 로그인을 보고할 수 있으므로 동일한 Active Directory 서버에 둘 이상의 에이전트를 연결하지 않아야 합니다. 연결할 경우, 각 에이전트가 동일한 Active Directory 서버를 폴링하는 에이전트를 실행하는 다른 모든 호스트의 주소와 해당 에이전트가 로그인하는 데 사용하는 사용자 이름을 제외하도록 구성해야 합니다. 자세한 내용은 주소가 제외된 사용자 에이전트 설정 구성, 2-16페이지를 참고하십시오.

**Active Directory 서버 연결을 구성하는 방법:**

**액세스:** 모두

**1단계** **Active Directory Servers(Active Directory 서버)** 탭을 선택합니다.

**2단계** 다음 2가지 옵션을 사용할 수 있습니다.

- 서버에 새 연결을 추가하려면, **Add(추가)**를 클릭합니다.
- 기존 연결을 수정하려면, 서버 이름을 두 번 클릭합니다.

**팁** 기존 연결을 제거하려면, 서버 이름을 선택하고 **Remove(제거)**를 클릭합니다.

**3단계** **Server Name/IP Address(서버 이름/IP 주소)** 필드에, 정식 고유 서버 이름이나 해당 Active Directory 서버의 IP 주소를 입력합니다. Active Directory 서버에 대한 로그인을 감지할 경우, IP 주소를 입력합니다.

**참고** 에이전트가 Active Directory 서버에 설치되어 있는 경우, 에이전트를 설치한 위치에 에이전트를 추가하려면 서버 이름으로 `localhost`를 입력합니다. 선택적으로 사용자 이름 및 비밀번호를 추가할 수 있습니다. 해당 정보를 생략할 경우, 해당 Active Directory 서버에 대한 로그오프는 감지할 수 없습니다. 사용자 이름 및 비밀번호 입력 여부와 관계없이 서버를 폴링할 수 있습니다.

**4단계** Active Directory 서버에 사용자 로그인 및 로그오프 데이터를 쿼리할 권한이 있는 사용자 이름 및 비밀번호를 입력합니다. 프록시를 통해 사용자를 인증하려면 정규화된 사용자 이름을 입력합니다.

기본적으로, 에이전트를 설치한 컴퓨터에 로그인하는 데 사용한 계정의 도메인이 **Domain(도메인)** 필드에 자동으로 채워집니다.

**참고** 사용자 비밀번호가 65자 이상의 문자로 구성된다면 새로운 서버 연결을 구성할 수 없습니다. 이 기능을 다시 사용하려면 비밀번호의 길이를 줄이십시오.

**5단계** Domain(도메인) 필드에 도메인이 Active Directory 서버인 도메인을 입력합니다.

**6단계** Active Directory 서버에 대한 로그인을 검색하려면, **Local Login IP Address(로컬 로그인 IP 주소)**를 선택합니다. 에이전트는 이 필드를 **Server Name/IP Address(서버 이름/IP 주소)** 필드에 지정된 서버와 관련된 모든 IP 주소로 자동으로 채웁니다.

**Server Name/IP Address(서버 이름/IP 주소)** 필드가 비어 있거나 `localhost`를 포함하는 경우, 이 필드는 로컬 호스트와 관련된 모든 IP 주소로 채워집니다.

**7단계** **Process real-time events(실시간 이벤트 진행)**를 선택하여 사용자 에이전트가 이 Active Directory 서버에서 실시간으로 로그인 이벤트를 검색할 수 있도록 합니다.

**8단계** **Add(추가)**를 클릭합니다.

서버 연결 정의가 Active Directory 서버 목록에 나타납니다. 2개 이상의 서버 연결이 구성된 경우 각 열의 헤더를 클릭하여 **Host(호스트)**, **Last Reported(최종 보고)**, **Polling Status(폴링 상태)**, **Last Polled(최종 폴링)**, **Real-time Status(실시간 상태)** 또는 **Real-time(실시간)**에 따라 정렬할 수 있습니다.

**참고** 컨피그레이션 시간 이내에 에이전트가 Active Directory 서버에 연결할 수 없는 경우, 서버를 추가할 수 없습니다. 에이전트가 서버에 대한 TCP/IP 액세스 권한이 있는지, 사용한 자격 증명이 연결 가능한지, 그리고 Active Directory 서버에 대한 연결을 올바르게 구성했는지 확인하십시오. 자세한 내용은 Active Directory 서버에 연결하는 권한 컨피그레이션, 2-4페이지를 참고하십시오.

**9단계** 선택적으로, 에이전트가 사용자 로그인 데이터를 위해 Active Directory 서버를 자동으로 폴링하는 간격을 변경하려면 **Active Directory Server Polling Interval(Active Directory 서버 폴링 간격)**에서 시간을 선택합니다.

설정을 저장한 후, 다음 폴링은 선택한 시간(분)이 경과한 후 발생하며 해당 간격에 따라 반복됩니다. 선택한 간격보다 폴링이 더 오래 걸리는 경우 다음 폴링은 해당 폴링이 종료된 후 다음 간격에서 다시 시작됩니다. Active Directory 서버에 대한 실시간 데이터 검색이 활성화되어 있으며 에이전트와 서버 간의 연결이 해제된 경우 에이전트는 응답을 받고 실시간 데이터 검색을 사용할 수 있을 때까지 지속적으로 폴링을 시도합니다. 일단 연결이 설정되면, 실시간 데이터 검색이 다시 시작됩니다.

**10단계** 선택적으로 에이전트가 사용자 로그인 데이터를 위해 Active Directory 서버를 폴링하기 위한 연결을 처음으로 설정하거나 재설정할 때 폴링된 최대 시간 범위를 변경하려면 **Active Directory Server Max Poll Length(Active Directory 서버 최대 폴링 시간)** 드롭다운 목록에서 시간을 선택합니다.

**참고** **Active Directory Server Max Poll Length(Active Directory 서버 최대 폴링 시간)**에는 **Active Directory Server Polling Interval(Active Directory 서버 폴링 간격)** 드롭다운 목록에서 선택한 값보다 크거나 같은 값을 저장할 수 있습니다. 에이전트는 각 폴링에 사용자 활동 데이터를 건너뛸 컨피그레이션을 저장하는 것을 허용하지 않습니다.

**11단계** 에이전트에 대한 컨피그레이션 변경 사항을 저장 및 적용하려면 **Save(저장)**를 클릭합니다.

**12단계** 다음 옵션을 이용할 수 있습니다.

- 방어 센터 연결을 추가하거나 제거하려면, **Sourcefire DC** 탭을 선택합니다. 자세한 내용은 사용자 에이전트 방어 센터연결 구성, 2-13페이지를 참고하십시오.

  최소한 1개의 방어 센터를 에이전트에 추가해야 사용자 로그인과 로그오프 데이터를 보고할 수 있습니다.
- 표 2-1 2-10페이지에 설명된 작업 중 하나를 수행하여 에이전트를 구성할 수 있습니다.

# 사용자 에이전트 방어 센터연결 구성

**라이센스:** FireSIGHT

에이전트에서 최대 5개의 방어 센터에 대한 연결을 추가할 수 있습니다. 에이전트에서는 탭이 선택된 시점의 방어 센터 상태(사용 가능, 사용 불가능, 또는 에이전트를 처음 시작하는 경우 알 수 없음)를 확인하거나 에이전트가 보고한 최종 로그인을 확인할 수 있습니다. 연결을 추가하기 전에, 방어 센터 컨피그레이션에 에이전트를 추가하십시오. 자세한 내용은 버전 4.x 방어 센터 연결 준비, 2-2페이지 또는 버전 5.x 방어 센터 연결 준비, 2-3페이지를 참조하십시오.

고가용성 컨피그레이션에서는 기본 및 보조 데이터 센터에 데이터가 남아 있을 수 있도록 양쪽에 대한 사용자 로그인 및 로그오프 데이터 업데이트를 활성화하기 위해 에이전트에 두 방어 센터를 추가합니다.

**방어 센터 연결을 구성하는 방법:**

**액세스:** 모두

**1단계** **Sourcefire DC** 탭을 선택합니다.

**2단계** **Add(추가)**를 클릭합니다.

**3단계** 추가하려는 방어 센터의 호스트 이름 및 IP 주소를 입력합니다.

**4단계** **Add(추가)**를 클릭합니다.

방어 센터 연결 컨피그레이션이 추가됩니다. 호스트 이름 또는 IP 주소를 여러 번 추가할 수 없습니다. 호스트 이름 및 IP 주소로 방어 센터를 추가해서는 안 됩니다. 방어 센터가 멀티홈 상태일 경우 서로 다른 IP 주소를 사용하여 이를 여러 번 추가해서는 안 됩니다.

2개 이상의 방어 센터 연결이 구성된 경우 각 열 헤더를 클릭하여 **Host(호스트)**, **Status(상태)** 또는 **Last Reported(최종 보고)**에 따라 정렬할 수 있습니다.

**참고** 컨피그레이션 시간 이내에 에이전트가 방어 센터에 연결할 수 없는 경우에는 이를 해당 방어 센터에 추가할 수 없습니다. 에이전트에 방어 센터에 대한 TCP/IP 액세스가 있는지 확인합니다.

**5단계** 에이전트에 대한 컨피그레이션 변경 사항을 저장 및 적용하려면 **Save(저장)**를 클릭합니다. 업데이트된 설정이 에이전트에 적용됩니다.

**6단계** 다음 옵션을 이용할 수 있습니다.

- 또는, 제외된 사용자 이름 목록에 사용자 이름을 추가하거나 제거하려면 **Excluded Usernames(제외된 사용자 이름)** 탭을 선택하십시오. 자세한 내용은 사용자 이름이 제외된 사용자 에이전트 설정 구성, 2-14페이지를 참고하십시오.
- 또는, 제외된 IP 주소 목록에 IP 주소를 추가하거나 제거하려면 **Excluded Addresses(제외된 주소)** 탭을 선택합니다. 자세한 내용은 주소가 제외된 사용자 에이전트 설정 구성, 2-16페이지를 참고하십시오.
- 또는, 로그 메시지를 보고 로깅을 구성하려면, **Logs(로그)** 탭을 선택합니다. 자세한 내용은 사용자 에이전트 로깅 설정 구성, 2-17페이지를 참고하십시오.
- 또는, 일반 에이전트 설정을 구성하려면 **General(일반)** 탭을 선택합니다. 자세한 내용은 일반 사용자 에이전트 설정 구성, 2-18페이지를 참고하십시오.
- 표 2-1 2-10페이지에 설명된 작업 중 하나를 수행하여 에이전트를 구성할 수 있습니다.

# 사용자 이름이 제외된 사용자 에이전트 설정 구성

**라이센스:** FireSIGHT

로그인 또는 로그오프 이벤트를 위해 폴링할 때 제외할 사용자 이름을 최대 500개까지 정의할 수 있습니다. 제외된 사용자 이름의 로그인이나 로그오프를 검색하면 에이전트는 이 이벤트를 방어 센터에 보고하지 않습니다. 제외하기 전에 보고된 사용자 이름에 대한 로그인 및 로그오프 이벤트는 영향을 받지 않습니다. 제외된 사용자 이름 목록에서 사용자 이름을 제거하면 해당 사용자 이름에 대한 향후 로그인 및 로그오프 이벤트가 방어 센터에 보고됩니다.

모든 도메인 또는 특정 도메인에서 사용자별 모든 로그인 및 로그오프를 제외할 것인지 선택할 수 있습니다. 또한 쉼표로 구분된 값 파일에 저장된 사용자 이름 및 도메인의 목록을 가져오고 내보낼 수 있습니다. 이미 방어 센터에 보고된 사용자를 제외하는 경우 호스트가 데이터베이스에서 비우지 않는 한 해당 사용자는 호스트에서 매핑 해제되지 않음에 유의하십시오.

**제외된 사용자 이름을 구성하는 방법:**

**액세스:** 모두

**1단계** **Excluded Usernames(제외된 사용자 이름)** 탭을 선택합니다.

**2단계** 사용 가능한 다음 행에 **Username(사용자 이름)** 열에서 제외할 사용자 이름을 입력합니다.

제외된 사용자 이름에는 달러 기호 문자($) 또는 따옴표 표시 문자(")를 포함할 수 없습니다.

**3단계** 또는, **Domain(도메인)** 열에 사용자 이름과 관련된 도메인을 입력할 수도 있습니다. 행당 1개의 도메인만 정의할 수 있습니다. 아무 도메인도 지정하지 않으면 모든 도메인의 사용자 이름이 제외됩니다.

**4단계** 추가 사용자 이름을 추가하려면 2단계 및 3단계단계를 반복합니다. 2개 이상의 제외된 사용자 이름이 구성된 경우 각 열 헤더를 클릭하여 **Username(사용자 이름)** 또는 **Domain(도메인)**에 따라 정렬할 수 있습니다.

**5단계** 행을 제거하려면, 다음 방법을 사용하십시오.

- 행을 강조 표시하고 Delete(삭제) 키를 누릅니다.
- 포인터를 사용자 이름의 끝에 두고 삭제될 때까지 백스페이스 키를 누릅니다.

행이 제거됩니다.

여러 행을 제거하려면, Ctrl 키를 클릭하여 여러 행을 선택하고 Delete(삭제) 키를 누릅니다.

**6단계** 쉼표로 구분된 값 파일에 사용자 이름 및 도메인 목록을 내보내려면 **Export List(목록 내보내기)**를 클릭합니다. 파일 경로를 선택하여 파일을 저장합니다.

파일이 저장되었습니다. 기본적으로, 파일 이름은 `Sourcefire_user_agent_excluded_users.csv`로 지정됩니다.

**7단계** 쉼표로 구분된 값 파일에서 사용자 이름 및 도메인 목록을 가져오려면 **Import List(목록 가져오기)**를 클릭합니다. 업로드할 파일을 선택합니다.

기존 사용자 이름이 지워지고, 파일의 사용자 이름이 로드됩니다. 중복된 사용자 이름을 포함하는 파일을 업로드할 수 없습니다. 파일에 구문 오류가 있는 해당 파일을 업로드할 수 없습니다.

쉼표로 구분된 값 파일에 있는 항목은 다음과 같은 형식이어야 합니다.

"*사용자 이름*","*도메인*"

도메인 값은 선택 사항이지만, 견적은 자리 표시자로 필요합니다.

**8단계** 에이전트에 컨피그레이션 변경 사항을 저장 및 적용하려면 **Save(저장)**를 클릭합니다.

업데이트된 설정이 에이전트에 적용됩니다.

**9단계** 다음 옵션을 이용할 수 있습니다.

- 제외된 IP 주소 목록에 IP 주소를 추가하거나 제거하려면 **Excluded Addresses(제외된 주소)** 탭을 선택합니다. 자세한 내용은 주소가 제외된 사용자 에이전트 설정 구성, 2-16페이지를 참고하십시오.
- 표 2-1 2-10페이지에 설명된 작업 중 하나를 수행하여 에이전트를 구성할 수 있습니다.

# 주소가 제외된 사용자 에이전트 설정 구성

**라이센스:** FireSIGHT

로그인 이벤트를 위해 폴링할 때 제외할 IPv4 또는 IPv6 주소를 최대 100개까지 정의할 수 있습니다. 제외된 IP 주소를 포함하는 로그인이나 로그오프 이벤트를 검색하면 에이전트는 이 이벤트를 방어 센터에 보고하지 않습니다. 제외하기 전에 보고된 IP 주소에서의 로그인 및 로그오프 이벤트는 영향을 받지 않습니다. 제외된 주소 목록에서 IP 주소를 제거하면 해당 주소에 대한 향후 로그인 및 로그오프 이벤트가 방어 센터에 보고됩니다.

**제외된 IP 주소를 구성하는 방법:**

**액세스:** 모두

---

**1단계** **Excluded Addresses(제외된 주소)** 탭을 선택합니다.

**2단계** 사용 가능한 다음 행에 **Address(주소)** 열에서 제외할 IP 주소를 입력합니다. 추가 IP 주소를 추가하려면 이 단계를 반복합니다. 2개 이상의 제외된 IP 주소가 구성된 경우 각 열 헤더를 클릭하여 **Address(주소)**에 따라 정렬할 수 있습니다.

잘못된 IP 주소를 입력하면, 행 헤더에 느낌표 아이콘( )이 나타납니다. 잘못된 주소를 복구하지 않고 다른 주소를 입력할 수는 없습니다.

**3단계** IP 주소를 제거하려면, 행을 강조 표시하고 Delete(삭제) 키를 누릅니다.

IP 주소가 제거됩니다. 여러 행을 제거하려면, Ctrl 키를 클릭하여 여러 행을 선택하고 Delete(삭제) 키를 누릅니다.

**4단계** 쉼표로 구분된 값 파일에 IP 주소 목록을 내보내려면 **Export List(목록 내보내기)**를 클릭합니다. 파일 경로를 선택하여 파일을 저장합니다.

파일이 저장되었습니다. 기본적으로, 파일 이름은 `Sourcefire_user_agent_excluded_addresses.csv`입니다.

**5단계** 쉼표로 구분된 값 파일에서 IP 주소 목록을 가져오려면 **Import List(목록 가져오기)**를 클릭합니다. 업로드할 파일을 선택합니다.

기존 IP 주소가 지워지고, 파일의 IP 주소가 로드됩니다. 중복된 IP 주소를 포함하는 파일을 업로드할 수 없습니다. 파일에 구문 오류가 있는 해당 파일을 업로드할 수 없습니다.

**6단계** 에이전트에 컨피그레이션 변경 사항을 저장 및 적용하려면 **Save(저장)**를 클릭합니다.

업데이트된 설정이 에이전트에 적용됩니다.

**7단계** 다음 옵션을 이용할 수 있습니다.

- 로그 메시지를 보고 로깅을 구성하려면, **Logs(로그)** 탭을 선택합니다. 자세한 내용은 사용자 에이전트 로깅 설정 구성, 2-17페이지를 참고하십시오.
- 표 2-1 2-10페이지에 설명된 작업 중 하나를 수행하여 에이전트를 구성할 수 있습니다.

---

# 사용자 에이전트 로깅 설정 구성

**라이센스:** FireSIGHT

**Logs(로그)** 탭에서 에이전트별로 기록된 최대 250개의 상태 메시지를 확인할 수 있습니다. 에이전트는 다음 이벤트가 발생하면 그에 대한 로컬 이벤트 로그에 상태 메시지를 기록합니다.

- 에이전트가 Active Directory 서버에서 성공적으로 데이터를 폴링합니다.
- 에이전트가 Active Directory 서버에 연결하지 못합니다.
- 에이전트가 Active Directory 서버에서 데이터를 검색하지 못합니다.
- 에이전트가 Cisco 장비에 성공적으로 연결합니다
- 에이전트가 Cisco 장비에 연결하지 못합니다.

에이전트는 타임스탬프 및 심각도 수준이 포함된 각 상태 메시지를 로깅합니다. 다음 표는 심각도가 증가함에 따른 심각도 수준에 대해 설명합니다.

***표 2-3 사용자 에이전트 로깅 심각도 수준***

| 수준기 | 색상 | 설명 |
|---|---|---|
| 디버그 | 회색 | 이벤트는 디버깅을 위해 로깅됩니다.<br>이러한 메시지는 기본적으로 표시되지 않습니다. |
| 정보 | 녹색 | 이벤트는 일반 에이전트 작업과 일치합니다. |
| 경고 | 노란색 | 예상치 못한 이벤트였으나 정상적인 에이전트 작동을 반드시 방해하는 것은 아닙니다. |
| 오류 | 빨간색 | 예상치 못한 이벤트였으며 정상적인 에이전트 작동이 중단되었습니다. |

에이전트는 로컬 이벤트 로그 이외에도 Windows 애플리케이션 로그에 상태 메시지를 기록할 수 있습니다. 또한 에이전트는 쉼표로 구분된 값 파일에 로컬 이벤트 로그 내용을 내보낼 수 있습니다.

상태 메시지를 저장할 것인지를 비롯하여 저장 기간과 모든 상태 메시지의 이벤트 로그를 삭제할 것인지 구성할 수 있습니다. 또한 디버그 상태 메시지 확인 및 **Maintenance(유지 관리)** 탭 액세스 등의 유지 관리 옵션을 구성할 수 있습니다.

**참고** 디버그 상태 메시지는 7일간 저장된 후 이벤트 로그에서 제거됩니다. 상태 메시지 저장 기간을 구성하고 이벤트 로그를 제거하는 것은 디버그 상태 메시지 스토리지에 영향을 미치지 않습니다.

**사용자 에이전트 로깅 설정을 구성하는 방법:**

**액세스:** 모두

**1단계** **Logs(로그)** 탭을 선택합니다.

**2단계** 지원 담당자의 지시가 있는 경우에만 **Show Debug Messages in Log(로그에서 디버그 메시지 보기)**를 선택하여 이벤트 로그에서 디버그 상태 메시지를 확인하고 **Maintenance(유지 관리)** 탭을 활성화할 수 있습니다.

**Logs(로그)** 탭에 디버그 메시지가 표시됩니다. **Maintenance(유지 관리)** 탭을 사용할 수 있습니다.

**참고** 지원 담당자가 별도로 안내할 경우에만 이 옵션을 선택하십시오.

**3단계** **Log Messages to Windows Application Log(Windows 애플리케이션 로그에 메시지 기록)**을 선택하여 디버그 상태 메시지가 아닌 메시지를 Windows 애플리케이션 로그 및 로컬 이벤트 로그에 로깅할 수 있습니다.

Windows 애플리케이션 로그를 보려면, Windows 이벤트 뷰어를 엽니다.

**4단계** **Message Cache Size(메시지 캐시 크기)** 드롭다운 목록에서 기간을 선택하여 로컬 이벤트 로그에서 자동으로 삭제될 때까지 상태 메시지를 저장할 기간을 구성할 수 있습니다.

상태 메시지가 일단 로컬 이벤트 로그에 기록되면 **Message Cache Size(메시지 캐시 크기)** 드롭다운 목록에서 선택한 기간 동안 저장된 후 삭제됩니다.

**참고** **Log Messages to Windows Application Log(Windows 애플리케이션 로그에 메시지 로깅)**를 선택한 경우에도 **Message Cache Size(메시지 캐시 크기)**는 로컬 이벤트 로그에만 영향을 미치며 Windows 애플리케이션 로그에는 영향을 주지 않습니다.

**5단계** 마지막 새로 고침 이후 로깅된 새로운 상태 메시지를 확인하려면 Refresh(새로 고침)를 클릭합니다.

마지막 새로 고침 후 새 상태 메시지가 로깅되면 사용 가능한 새로운 상태 메시지가 있음을 알리는 메모가 표시됩니다. 새로 고침 결과가 250개 이상의 메시지를 표시하는 경우 가장 오래된 상태 메시지는 **Logs(로그)** 탭에서 제거됩니다. 250개 이상의 메시지를 보려면, 로그를 내보내십시오. 자세한 내용은 6단계을/를 참조하십시오.

**6단계** **Export Logs(로그 내보내기)**를 클릭하여 로컬 이벤트 로그 내용을 쉼표로 구분된 값 파일로 내보냅니다.

쉼표로 구분된 값 파일에는 모든 이벤트 로그 상태 메시지와 디버그 메시지가 포함되어 있습니다.

**7단계** **Clear Event Log(이벤트 로그 삭제)**를 클릭하여 로컬 이벤트 로그에서 디버그 상태 메시지가 아닌 모든 메시지를 제거할 수 있습니다.

에이전트가 메시지를 제거했음을 알리는 상태 메시지를 제외한 로컬 이벤트가 삭제됩니다.

**8단계** 에이전트에 대한 컨피그레이션 변경 사항을 저장 및 적용하려면 **Save(저장)**를 클릭합니다.

업데이트된 설정이 에이전트에 적용됩니다.

**9단계** 다음 옵션을 이용할 수 있습니다.

- 일반 에이전트 설정을 구성하려면 **General(일반)** 탭을 선택합니다. 자세한 내용은 일반 사용자 에이전트 설정 구성, 2-18페이지를 참고하십시오.
- 표 2-1 2-10페이지에 설명된 작업 중 하나를 수행하여 에이전트를 구성할 수 있습니다.

# 일반 사용자 에이전트 설정 구성

**라이센스:** FireSIGHT

General(일반) 탭에는 기본 사용자 에이전트 컨피그레이션이 포함되어 있습니다. 에이전트가 로그인 데이터를 보고할 때 방어 센터에 보고되는 에이전트 이름을 변경할 수 있습니다. 또한 에이전트 서비스를 시작 및 중지하고, 로그오프 확인 빈도를 변경하고, 현재 서비스 상태를 볼 수도 있습니다.

**일반 사용자 에이전트 설정 구성 방법:**

**액세스:** 모두

**1단계** 에이전트를 설치한 컴퓨터에서, **Start(시작) > Programs(프로그램) > Sourcefire > Configure User Agent(사용자 에이전트 구성)**를 선택합니다.

**2단계** 에이전트 서비스를 시작하려면 시작 버튼( )을 클릭합니다.

에이전트 서비스가 시작됩니다.

**3단계** 에이전트 서비스를 중지하려면 중지 버튼( )을 클릭합니다.

에이전트 서비스를 중지합니다.

**4단계** 또는, 기본적으로 `SFADUA`로 지정되는 에이전트의 **Agent Name(에이전트 이름)**을 수정합니다. 문자, 숫자, 밑줄 (_) 및 대시(-)를 입력할 수 있습니다.

**5단계** 또는, 버전 5.2 이상의 경우 로그오프 데이터에 대한 에이전트 확인 빈도를 변경하기 위해 **Logout Check Frequency(로그아웃 확인 빈도)** 드롭다운 목록에서 기간을 선택합니다. 로그오프 데이터 확인을 비활성화하려면 `0`을 선택합니다.

**6단계** 또는, 에이전트 일정의 우선순위를 변경하기 위해 **Priority(우선순위)** 드롭다운 목록에서 한 수준을 선택합니다. 에이전트가 상당한 양의 사용자 활동을 모니터링하며 검색할 경우에만 `High(높음)`를 선택합니다.

**7단계** 설정을 저장하려면, **Save(저장)**를 클릭합니다.

업데이트된 설정이 에이전트에 적용됩니다.

**8단계** 표 2-1 2-10페이지에 설명된 작업 중 하나를 수행하여 에이전트를 구성할 수 있습니다.

# 사용자 에이전트 유지 관리 설정 구성

**라이센스:** FireSIGHT

컴피그레이션 설정 외에도, 에이전트는 사용자-IP 매핑 정보, 로컬 이벤트 로그, 보고 상태 정보를 SQL CE 데이터베이스에 저장합니다. 에이전트 유지 관리 탭을 이용하면 유지 관리 목적으로 데이터베이스 일부를 삭제할 수 있습니다. 캐시된 사용자-IP 매핑 정보 및 로컬 이벤트 로그 정보를 삭제할 수 있습니다. 또한 구성된 Active Directory 서버의 수동 폴링을 강제하는 보고 상태 캐시도 지울 수 있습니다.

**주의** 지원 담당자가 별도로 안내하지 않는 한 유지 관리 탭의 어떤 설정도 변경하지 **마십시오**.

**사용자 에이전트 유지 관리 설정을 구성하는 방법:**

**액세스:** 모두

**1단계** **Logs(로그)** 탭을 선택합니다.

**2단계** **Show Debug Messages in Log(로그에서 디버그 메시지 보기)**를 선택하여 **Maintenance(유지 관리)** 탭을 활성화합니다.

**3단계** **Maintenance(유지 관리)** 탭을 선택합니다.

**4단계** **Clear user mapping data cache(데이터 캐시를 매핑하는 사용자 삭제)**를 클릭하여 저장된 모든 사용자-IP 매핑 데이터를 지웁니다.

에이전트는 로컬 에이전트 데이터베이스에서 저장된 모든 사용자-IP 매핑 데이터를 삭제합니다. 방어 센터 데이터베이스에 저장된 사용자-IP 매핑 데이터는 로컬 에이전트 데이터베이스의 삭제로부터 영향을 받지 않습니다.

**5단계** 저장된 모든 로그인 이벤트 데이터를 삭제하기 위해 **Clear logon event log cache(로그온 이벤트 로그 캐시 삭제)**를 클릭합니다.

에이전트가 로컬 이벤트 로그에서 저장된 모든 로그인 이벤트 데이터를 삭제합니다.

**6단계** **Clear reporting state cache(보고 상태 캐시 삭제)**를 클릭하여 에이전트가 구성된 방어 센터에 마지막으로 로그인 및 로그오프 정보를 보고한 시점과 관련된 데이터를 삭제합니다.

에이전트는 구성된 방어 센터에 마지막으로 로그인 및 로그오프 정보를 보고한 시점과 관련된 모든 정보를 삭제합니다. 다음 폴링 간격이 시작되면 에이전트가 구성된 모든 Active Directory 서버를 수동으로 폴링하여 **Active Directory Server Max Poll Length(Active Directory 서버 최대 폴링 시간)** 필드에 정의된 시간 범위 내의 정보를 검색합니다. 자세한 내용은 사용자 에이전트 구성 Active Directory 서버 연결, 2-10페이지를 참고하십시오.

**7단계** 로깅된 디버그 메시지의 상세 수준을 구성하려면 **Debug Log Level(디버그 로그 수준)** 드롭다운에서 로깅 세밀성 수준을 선택합니다.

**8단계** 표 2-1 2-10페이지에 설명된 작업 중 하나를 수행하여 에이전트를 구성할 수 있습니다.