Firepower 사용자 에이전트 환경 설정 가이드

버전 2.3
2017년 10월 25일 수요일

Cisco Systems, Inc.
www.cisco.com
Cisco는 전 세계에 200여 개 이상의 지사가 있습니다.
주소, 전화번호 및 팩스 번호는
다음 Cisco 웹사이트에 나와 있습니다.
www.cisco.com/go/offices.

동봉한 제품의 소프트웨어 라이센스 및 제한된 보증은 제품과 함께 제공된 정보 패킷에 설명되어 있으며 본 문서에 참조를 통해 포함됩니다. 소프트웨어 라이센스 또는 제한된 보증을 찾을 수 없는 경우 CISCO 담당자에게 문의하여 복사본을 요청하십시오.

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 보려면 다음 URL로 이동하십시오. www.cisco.com/go/trademarks 여기에 언급된 서드파티 상표는 해당 소유권자의 자산입니다. "파트너"라는 용어는 사용에 있어 Cisco와 기타 회사 간의 파트너 관계를 의미하지는 않습니다. (1721R)

이 문서에서 사용된 모든 IP(Internet Protocol) 주소와 전화번호는 실제 주소와 전화번호가 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

사용자 에이전트 소개

버전 2.3의 사용자 에이전트는 Firepower System의 관리되는 디바이스와 함께 사용자 데이터를 수집합니다. 버전 5.x 또는 6.x의 Firepower System이 포함된 에이전트를 사용하는 경우 사용자 에이전트는 사용자 액세스 제어를 구현하는 데에도 필수적입니다.

사용자 에이전트는 최대 5개의 Microsoft Active Directory 서버를 모니터링하고 Active Directory를 통해 인증된 로그인 및 로그오프를 보고합니다. Firepower System은 이러한 레코드를 관리되는 디바이스에서 트래픽 기반 탐지를 사용하여 수집한 정보와 통합합니다.

사용자 에이전트와 관련된 릴리스별 용어 및 기능 지원에 대한 정보는 다음 표를 참조하십시오.

표 1-1 릴리스별 사용자 에이전트 용어

개념	Version 5.x	Version 6.x
시스템	FireSIGHT System	Firepower System
사용자 검색을 위한 기능	네트워크 검색	네트워크 검색 및 ID
사용자 ID 및 사용자 활동 데이터 분석	사용자 인식	사용자 인식
사용자 제어를 위해 사용자 ID 및 사용자 활동 데이터 사용	액세스 제어	액세스 제어
관리하는 어플라이언스	Defense Center	Management Center
관리되는 어플라이언스	관리되는 디바이스	관리되는 디바이스
서버-데이터베이스 연결	사용자 인식 개체	영역

사용자 에이전트 정보

이 섹션에서는 Firepower System에서 사용자 검색 구현 시 사용자 에이전트의 역할을 설명합니다. 사용자 검색, RNA/네트워크 검색 및 ID 소스와 관련된 모든 개념에 대한 더 자세한 내용은 시스템의 환경 설정 가이드를 참조하십시오.

자세한 내용은 다음 섹션을 참조하십시오.

사용자 에이전트의 기본 요소

Firepower System은 조직의 Active Directory 서버에서 사용자 ID와 사용자 활동 정보를 얻을 수 있습니다. 사용자 에이전트를 사용하면 사용자가 Microsoft Active Directory 서버를 통해 인증할 때 사용자를 모니터링할 수 있습니다.

참고 사용자 제어를 수행하려면 조직에서 *반드시* Microsoft Active Directory를 사용해야 합니다. Firepower System은 Active Directory 서버를 모니터링하는 사용자 에이전트를 사용하여 사용자와 IP 주소를 연결하며, 이를 통해 액세스 제어 규칙이 트리거됩니다.

사용자 에이전트를 설치 및 사용하면 사용자 제어를 수행할 수 있습니다. 에이전트는 사용자 이름을 하나 이상의 IP 주소와 연결하며 이 정보는 사용자 조건과 함께 액세스 제어 규칙을 트리거할 수 있습니다.

사용자 제어를 위한 완전한 사용자 에이전트 컨피그레이션에는 다음이 포함됩니다.

- 에이전트가 설치된 컴퓨터
- Management Center 및 사용자 에이전트 컴퓨터 간의 연결
- 각 Management Center 및 모니터링된 Active Directory 서버 간의 연결. 버전 5.x에서는 연결을 *사용자 인식 개체*로 구성하고, 버전 6.x에서는 연결을 ID *영역*으로 구성합니다.

사용자 제어에 대한 자세한 내용은 시스템의 환경 설정 가이드를 참조하십시오.

모니터링하려는 Microsoft Active Directory 서버에 대한 TCP/IP 액세스를 포함한 Microsoft Windows Vista, Microsoft Windows 7, Microsoft Windows 8, Microsoft Windows Server 2008 또는 Microsoft Windows Server 2012 컴퓨터에 사용자 에이전트를 설치할 수 있습니다. 지원되는 운영 체제 중 하나를 실행 중인 Active Directory 서버에 에이전트를 설치할 수도 있지만 이는 비교적 안전하지 않습니다.

참고 Windows Server 2003 또는 이전 운영 체제에서 사용자 에이전트를 설치하는 경우 사용자 에이전트는 Active Directory 컴퓨터에서 실시간으로 통계를 수집할 수 없습니다.

Management Center 연결을 활용하면 사용자 에이전트에서 로그인 및 로그오프가 탐지된 사용자의 메타데이터를 검색할 수 있을 뿐만 아니라 액세스 제어 규칙을 사용할 사용자 및 그룹을 지정할 수도 있습니다. 특정 사용자 이름을 제외하도록 에이전트를 구성한 경우 해당 사용자 이름의 로그인 데이터는 Management Center에 보고되지 않습니다.

에이전트 모니터링, 폴링 및 보고

각 사용자 에이전트는 정기적으로 예약된 폴링 또는 실시간 모니터링을 통해 암호화된 트래픽을 사용하여 신뢰할 수 있는 로그인을 모니터링할 수 있습니다.

다음은 사용자 에이전트가 Management Center에 보고하는 이벤트 중 하나입니다.

- **User Login(사용자 로그인)**: 사용자가 마지막으로 나타난 때의 사용자 이름과 연결되지 않은 IP 주소를 가진 컴퓨터에 로그인하는 경우 발생하는 이벤트입니다.

  즉, 사용자 이름 `james.harvey`가 월요일에 IP 주소 192.0.2.100에 로그인한다고 가정해 보겠습니다. 화요일에 `james.harvey`가 IP 주소 192.0.2.105에 로그인합니다. 이 로그인은 Management Center에서 사용자 로그인 이벤트를 트리거합니다.

  사용자 로그인 이벤트는 사용자가 워크스테이션에 직접 로그인하거나 원격 데스크톱을 사용하는 경우 발생합니다.

- **User Logoff(사용자 로그오프)**: 사용자가 IP 주소에서 로그아웃할 때 발생합니다. 사용자 로그오프 이벤트는 사용자가 컴퓨터에서 로그오프한 이후에 바로 보고되지는 않으며 구성 가능한 간격으로 Management Center에 보고됩니다.

- **New User Identity(새 사용자 ID)**: 사용자 이름이 IP 주소와 처음으로 연결되는 경우 발생하는 일회성 이벤트입니다.

- **Delete User Identity(사용자 ID 삭제)**: Management Center 관리자가 사용자 ID를 삭제한 후에 발생합니다.

로그오프 데이터와 로그인 데이터를 함께 활용하면 사용자의 네트워크 로그인에 대해 좀 더 완전하게 파악할 수 있습니다.

Active Directory 서버를 폴링하면 에이전트가 정의된 폴링 간격으로 일련의 사용자 활동 데이터를 검색할 수 있습니다. Active Directory 서버가 데이터를 수신하는 즉시 실시간 모니터링이 사용자 활동 데이터를 에이전트에 전송합니다.

특정 사용자 이름 또는 IP 주소와 연결된 모든 로그인 또는 로그오프를 보고에서 제외하도록 에이전트를 구성할 수 있습니다. 이 기능은 예를 들어 다음을 대상으로 하는 반복된 로그인을 제외하고자 할 때 유용할 수 있습니다.

- 공유 서버(예: 파일 공유 및 인쇄 서버)
- 사용자 에이전트 컴퓨터
- Active Directory 서버
- 트러블슈팅 목적으로 컴퓨터에 로그인

최대 5개의 Active Directory 서버를 모니터링하고 암호화된 데이터를 최대 5개의 Management Center로 전송하도록 에이전트를 구성할 수 있습니다.

버전 5.x 또는 6.x를 사용하여 액세스 제어를 수행하는 경우 사용자 에이전트에서 보고한 로그인을 통해 사용자가 IP 주소에 연결할 수 있으므로 사용자 조건으로 액세스 제어 규칙이 트리거될 수 있습니다.

참고 여러 사용자가 원격 세션을 사용하여 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 참조하십시오.

표 1-2 폴링 및 모니터링 참고 사항

개념	참고
로그인 탐지	에이전트는 버전 5.2 이상을 실행 중인 Defense Center로 IPv6 주소의 호스트에 대한 사용자 로그인을 보고합니다. 에이전트는 버전 5.0.1 이상을 실행 중인 Defense Center에 신뢰할 수 있는 사용자 로그인 및 NetBIOS 로그인을 보고합니다. Active Directory 서버에 대한 로그인을 탐지하려면 Active Directory 서버 연결을 서버 IP 주소로 구성해야 합니다. 자세한 내용은 사용자 에이전트 Active Directory 서버 연결 구성, 2-20페이지를 참조하십시오.
로그오프 탐지	에이전트는 버전 5.2 이상의 Defense Center에 탐지된 로그오프를 보고합니다. 로그오프는 즉시 탐지되지 않을 수 있습니다. 로그오프와 연결된 타임스탬프는 사용자가 더 이상 호스트 IP 주소에 매핑되지 않음을 에이전트가 탐지한 시간입니다. 이는 사용자가 호스트에서 로그오프한 시간과 일치하지 않을 수 있습니다.
실시간 데이터 검색	Active Directory 서버는 Windows Server 2008 또는 Windows Server 2012를 실행해야 합니다. 사용자 에이전트 컴퓨터는 Windows 7, Windows 8, Windows 10 또는 Server 2003 이상의 Windows Server 버전을 실행해야 합니다.

사용자 에이전트 로그인 데이터

사용자 에이전트는 사용자가 네트워크에 로그인할 때 또는 기타 이유로 Active Directory 자격 증명에 대해 어카운트를 인증할 때 사용자를 모니터링합니다. 사용자 에이전트는 호스트에 대한 인터랙티브 사용자 로그인, 원격 데스크톱 로그인, 파일 공유 인증 및 컴퓨터 어카운트 로그인을 탐지합니다.

사용자 에이전트는 *신뢰할 수 있는* 사용자 로그인을 보고합니다. 로그인 데이터를 신뢰할 수 있는 경우(예: 호스트에 대한 사용자의 원격 데스크톱 로그인 또는 인터랙티브 로그인) 현재 사용자가 호스트 IP 주소에 매핑되어 새로운 로그인의 사용자로 변경됩니다.

네트워크 검색 트래픽 기반 탐지는 *신뢰할 수 없는* 사용자 로그인을 보고합니다. 신뢰할 수 없는 로그인은 현재 사용자를 변경하지 않거나, 사용자 또한 신뢰할 수 없는 경우에만 현재 사용자를 변경합니다.

단, 다음 주의 사항을 참고하십시오.

- 파일 공유 인증을 위한 로그인을 탐지하면 에이전트는 호스트에 대한 사용자 로그인을 보고하지만 호스트의 현재 사용자를 변경하지는 않습니다.
- 호스트에 대한 컴퓨터 어카운트 로그인을 탐지하면 에이전트는 NetBIOS Name Change(NetBIOS 이름 변경) 검색 이벤트를 생성하며 호스트 프로파일은 NetBIOS 이름에 대한 변경 사항을 반영합니다.
- 제외된 사용자 이름의 로그인을 탐지하면 에이전트는 Management Center에 로그인을 보고하지 않습니다.

모든 로그인의 경우 에이전트는 다음 정보를 Management Center에 전송합니다.

- 사용자의 LDAP 사용자 이름

참고 유니코드 문자의 사용자 이름은 Management Center에 정확하게 표시되지 않을 수 있습니다.

- 로그인 또는 기타 인증 시간
- 사용자 호스트의 IP 주소 및 링크 로컬 주소(에이전트가 컴퓨터 어카운트 로그인에 대해 IPv6 주소를 보고하는 경우)

참고 사용자가 Linux 컴퓨터를 사용하여 원격 데스크톱을 통해 Windows 컴퓨터에 로그인하는 경우 에이전트가 로그인을 탐지하면 Linux 컴퓨터 IP 주소가 아닌 Windows 컴퓨터 IP 주소를 Management Center에 보고합니다.

Management Center는 로그인 및 로그오프 정보를 사용자 활동 데이터베이스에 기록하며 사용자 데이터를 사용자 데이터베이스에 기록합니다. 사용자 에이전트가 사용자 로그인 또는 로그오프에서 사용자 데이터를 보고하면 보고된 사용자가 사용자 데이터베이스의 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. 에이전트가 컴퓨터에 대한 첫 번째 사용자 로그인에 이어 두 번째 사용자 로그인을 탐지한 상태에서 두 번째 사용자 로그인과 연결된 사용자 이름을 보고에서 제외한 경우 에이전트는 원래 사용자에 대한 로그오프를 보고합니다. 그러나 두 번째 사용자에 대한 로그인은 보고하지 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 Defense Center로 보고된, 달러 기호 문자($)로 끝나는 사용자 이름은 네트워크 맵을 업데이트하지만 사용자 로그인으로 표시되지는 않습니다. 에이전트는 달러 기호 문자($)로 끝나는 사용자 이름을 다른 버전의 Management Center에 보고하지 않습니다.
- Management Center에서 유니코드 문자가 포함된 사용자 이름을 표시하는 데에는 제한 사항이 있을 수 있습니다.

Management Center가 저장할 수 있는 탐지된 사용자의 총 수는 다음에 따라 다릅니다.

- 버전 5.x에서 사용자의 RNA 또는 FireSIGHT 라이선스
- 버전 6.x에서 사용자의 Management Center 모델

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.

여러 사용자 에이전트 구축

도메인당 둘 이상의 Active Directory 서버를 가진 경우 둘 이상의 사용자 에이전트 설치를 고려할 수 있습니다. Active Directory 서버는 인증 정보를 공유하지만 사용자 에이전트가 정보 중 일부를 수집하는 위치인 보안 로그는 공유하지 않습니다.

따라서 도메인에 둘 이상의 Active Directory 서버가 있는 경우 다음 중 한 가지 작업을 수행할 수 있습니다.

- 둘 이상의 Active Directory 서버와 통신하는 사용자 에이전트를 하나 설치합니다.

  하나의 사용자 에이전트는 최대 5개의 Active Directory 서버와 통신할 수 있습니다.
- 서로 다른 Active Directory 서버 또는 도메인 컨트롤러와 통신하는 사용자 에이전트를 둘 이상 설치합니다.

이 구축 유형은 다음과 같은 경우 사용하는 것이 좋습니다.

- Active Directory 서버는 지리적으로 분산되어 있습니다. Active Directory 서버 또는 Active Directory 서버 컴퓨터 자체(비교적 안전하지 않음)와 지리적으로 가까이 있는 컴퓨터에서 사용자 에이전트를 설치하는 것이 좋습니다.
- Active Directory 서버에 트래픽이 과도하게 로드되어 있습니다.

참고 도메인 컨트롤러의 IP 주소 또는 정규화된 호스트 이름과 통신하도록 각 사용자 에이전트를 구성해야 합니다. 멀티 도메인 시스템에서 각 도메인 컨트롤러가 다른 IP 주소 또는 호스트 이름을 갖는 것이 일반적입니다.

레거시 에이전트 지원

Active Directory 서버에 설치된 버전 1.0(레거시) 사용자 에이전트에서는 Active Directory 서버에서 단일 Management Center로 사용자 로그인 데이터를 계속해서 전송할 수 있습니다. 레거시 에이전트의 구축 요구 사항 및 탐지 기능에는 변경 사항이 없습니다.

Active Directory 서버에 레거시 에이전트를 설치해야 정확히 하나의 Management Center에 연결할 수 있습니다. 그러나 User Agent Status Monitor(사용자 에이전트 상태 모니터링)의 상태 모듈은 레거시 에이전트를 지원하지 않으며 연결된 레거시 에이전트를 통해 Management Center에서 활성화해서는 안 됩니다.

레거시 에이전트에 대한 지원은 단계적으로 중단되므로 향후 릴리스 준비 차원에서 가능한 한 빨리 버전 2.3 사용자 에이전트를 사용하여 구축을 업그레이드하도록 계획해야 합니다.

버전 5.x에서의 사용자 에이전트 및 액세스 제어 정보

라이선스: 제어

조직에서 Microsoft Active Directory 서버를 사용하는 경우 Active Directory 서버를 사용하여 사용자 활동을 모니터링하는 사용자 에이전트를 설치하는 것이 좋습니다. 버전 5.x에서 사용자 제어를 수행하려면 *반드시* 사용자 에이전트를 설치하고 Defense Center에 대한 연결을 구성해야 합니다.

버전 6.x에서의 사용자 에이전트, ISE 및 액세스 제어 정보

Classic 라이선스: 제어

Smart 라이선스: 모두

버전 6.0에서는 사용자 에이전트 대신 Cisco ISE(Identity Services Engine)를 지원합니다. 사용자 에이전트 및 ISE는 사용자 액세스 제어를 위해 데이터를 수집하는 수동 ID 소스입니다. 버전 6.x에서 사용자 제어를 수행하려면 에이전트 또는 ISE 디바이스에 연결된 Management Center에서 모니터링되는 Active Directory 서버의 ID 영역을 구성해야 합니다. 영역, ID 소스 및 ISE/ISE-PIC에 대한 자세한 내용은 시스템의 환경 설정 가이드를 참조하십시오.

사용자 에이전트 컨피그레이션 프로세스

사용자 에이전트 버전 2.3을 사용하여 최대 5개의 Microsoft Active Directory 서버에서 사용자 로그인 데이터를 수집하고 이를 Management Center로 보내려면 우선 사용자 에이전트를 설치한 후 이를 각 Management Center 및 Microsoft Active Directory 서버에 연결하고 일반 설정을 구성해야 합니다. 자세한 내용은 다음 섹션을 참조하십시오.

사용자 에이전트 설정

사용자 에이전트의 설정은 여러 단계로 구성됩니다.

사용자 에이전트를 설정하는 방법:

액세스: 관리자

1단계 각각의 Management Center를 구성하려면 다음 작업을 수행하십시오.

- 에이전트를 설치할 서버의 IP 주소에서 에이전트 연결을 허용합니다.
- Active Directory 개체 또는 영역을 구성하고 활성화합니다. 개체를 설명하는 데 사용되는 용어는 Management Center 버전에 따라 다릅니다. 자세한 내용은 다음 섹션 중 하나를 참조하십시오.
  - 사용자 에이전트에 연결하도록 버전 5.x Defense Center 구성, 2-3페이지
  - 사용자 에이전트에 연결하도록 버전 6.x Management Center 구성, 2-3페이지

2단계 Management Center와 통신하기 위해 사용자 에이전트에 대한 이벤트를 로깅하도록 Active Directory 서버를 구성합니다. 자세한 내용은 Active Directory 서버 구성, 2-3페이지를 참조하십시오.

3단계 도메인에 대한 방화벽을 통해 WMI(Windows Management Instrumentation)를 허용하도록 도메인에서 각 컴퓨터를 구성합니다. 자세한 내용은 도메인 컴퓨터 구성, 2-6페이지를 참조하십시오.

4단계 에이전트를 설치할 컴퓨터에 필수 프로그램을 설치합니다. Active Directory 서버에 대한 컴퓨터의 TCP/IP 액세스를 설정합니다. 자세한 내용은 사용자 에이전트 설치를 위한 컴퓨터 준비, 2-6페이지를 참조하십시오.

5단계 이전 사용자 에이전트가 설치되어 있는 경우 필요에 따라 에이전트 데이터베이스를 백업하여 컨피그레이션 설정을 유지합니다. 자세한 내용은 사용자 에이전트 컨피그레이션 백업, 2-17페이지를 참조하십시오.

6단계 에이전트가 Active Directory 서버와 연결하도록 허용하는 데 필요한 권한을 구성합니다. 자세한 내용은 다음을 참조하십시오.

- 도메인 사용자에게 제한된 권한 부여(요약), 2-8페이지
- 로컬 사용자에게 권한 부여, 2-8페이지

7단계 컴퓨터에 에이전트를 설치합니다.

- 자세한 내용은 사용자 에이전트 설치, 2-18페이지를 참조하십시오.
- 경우에 따라 둘 이상의 사용자 에이전트 설치하려면 여러 사용자 에이전트 구축, 1-5페이지를 참조하십시오.

8단계 하나 이상의 Microsoft Active Directory 서버에 대한 연결을 구성합니다.

9단계 (선택 사항). 에이전트에 대한 폴링 간격 및 최대 폴링 시간을 구성합니다. 자세한 내용은 사용자 에이전트 Active Directory 서버 연결 구성, 2-20페이지를 참조하십시오.

10단계 최대 5개의 Management Center 연결을 구성합니다. 자세한 내용은 사용자 에이전트 Management Center 연결 구성, 2-24페이지를 참조하십시오.

11단계 (선택 사항). 로그인 및 로그오프 데이터에 대한 폴링에서 제외할 사용자 이름 및 IP 주소 목록을 구성합니다. 자세한 내용은 다음을 참조하십시오.

- 사용자 이름이 제외된 사용자 에이전트 설정 구성, 2-25페이지
- 주소가 제외된 사용자 에이전트 설정 구성, 2-26페이지

12단계 (선택 사항). 에이전트 로깅 설정을 구성합니다. 자세한 내용은 사용자 에이전트 로깅 설정 구성, 2-27페이지를 참조하십시오.

13단계 (선택 사항). 에이전트 이름을 구성하고, 서비스를 시작 및 중지하고, 서비스의 현재 상태를 확인합니다. 자세한 내용은 일반 사용자 에이전트 설정 구성, 2-29페이지를 참조하십시오.

14단계 **Save(저장)**를 클릭하여 사용자 에이전트 컨피그레이션을 저장합니다.

주의 Cisco TAC에서 안내하지 않는 한 사용자 에이전트 유지 관리 설정을 수정하지 *마십시오*.

Management Center 컨피그레이션

이 섹션에서는 사용자 에이전트에서 사용자 데이터를 수신하도록 Management Center를 준비하는 방법에 대해 설명합니다.

사용자 에이전트에 연결하도록 버전 5.x Defense Center 구성

사용자 에이전트 버전 2.3을 사용하여 LDAP 로그인 데이터를 버전 5.x Defense Center에 전송하려는 경우 다음을 모두 구성해야 합니다.

- Active Directory 서버에 연결할 에이전트에서 연결을 허용하도록 각 Defense Center를 구성합니다. 이렇게 하면 에이전트는 Defense Center와 안전한 연결을 설정하여 데이터를 전송할 수 있습니다.

  이 연결을 설정하는 데 대한 자세한 내용은 버전 5.x *FireSIGHT System 사용자 가이드*에서 사용자 에이전트를 사용하여 Active Directory 로그인 보고하기를 참조하십시오.

- 사용자 액세스 제어를 구현하려면 Defense Center 및 조직에 있는 하나 이상의 Microsoft Active Directory 서버 간에 연결을 구성하고 활성화해야 합니다. 버전 5.x에서는 이를 *LDAP 연결* 또는 *사용자 인식 개체*라고 합니다.

  이러한 컨피그레이션에는 서버에 대한 연결 설정 및 인증 필터 설정이 포함됩니다. 연결의 사용자 및 그룹 액세스 제어 파라미터는 액세스 제어 규칙에서 사용할 수 있는 그룹과 사용자를 지정합니다. 이 컨피그레이션에 대한 자세한 내용은 버전 5.x *FireSIGHT System 사용자 가이드*에서 사용자 인식 및 제어를 위해 LDAP 서버에 연결하기를 참조하십시오.

사용자 에이전트에 연결하도록 버전 6.x Management Center 구성

버전 2.3 사용자 에이전트를 사용하여 로그인 데이터를 버전 6.x Management Center에 전송하려면 다음을 모두 구성해야 합니다.

- 사용자 서버에 연결할 에이전트에서 연결을 허용하도록 각 Management Center를 구성합니다. 이렇게 하면 에이전트는 Management Center와 안전한 연결을 설정하여 데이터를 전송할 수 있습니다.

  이 연결을 설정하는 데 대한 자세한 내용은 버전 6.x *Firepower Management Center 컨피그레이션 가이드*에서 사용자 에이전트 연결 구성을 참조하십시오.

- 사용자 액세스 제어를 구현하려면 Management Center 및 조직에 있는 하나 이상의 Microsoft Active Directory 서버 간에 연결을 구성하고 활성화해야 합니다. 버전 6.x에서는 이를 *영역*이라고 합니다.

  영역에는 연결 설정 및 서버에 대한 인증 필터 설정이 포함되어 있습니다. 연결의 사용자 다운로드 설정은 액세스 제어 규칙에서 사용할 수 있는 사용자 및 그룹을 지정합니다. 이 컨피그레이션에 대한 자세한 내용은 버전 6.x *Firepower Management Center 컨피그레이션 가이드*에서 영역 생성을 참조하십시오.

Active Directory 서버 구성

이 섹션에서는 Active Directory 서버가 로그인 데이터를 이 로그에 기록할 수 있도록 Active Directory 보안 로그가 활성화되어 있는지 확인하는 방법을 다룹니다.

로깅을 위한 Active Directory 서버 구성

Active Directory 서버가 로그인 데이터를 로깅하는지 확인하는 방법:

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

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

로깅이 활성화된 경우 Security(보안) 로그가 표시됩니다. 로깅이 비활성화된 경우 보안 로깅 활성화에 대한 정보는 MSDN에서 Active Directory 및 LDS 진단 이벤트 로깅을 구성하는 방법을 참조하십시오.

3단계 Active Directory 서버에서 방화벽을 통해 WMI를 허용합니다. Active Directory 서버가 Windows Server 2008 또는 Windows Server 2012를 실행 중인 경우 MSDN 또는 기타 정보에 대해 원격 WMI 연결 설정을 참조하십시오.

Windows 2012 Server에서 로그온/로그오프 이벤트 감사를 활성화하려면 다음 작업을 수행합니다.

1단계 **Start(시작) > Administrative Tools(관리 툴) > Group Policy Management Editor(그룹 정책 관리 편집기)**를 클릭합니다.

2단계 탐색 창에서 **Forest(포리스트): *YourForestName(포리스트 이름)***을 펼치고 **Domains(도메인) > *YourDomainName(도메인 이름)* > Group Policy Objects(그룹 정책 개체)**를 펼칩니다.

3단계 **Default Domain Policy(기본 도메인 정책)**를 마우스 오른쪽 버튼으로 클릭하고 **Edit(편집)**을 클릭합니다.

4단계 **Computer Configuration(컴퓨터 컨피그레이션) > Policies(정책) > Windows Settings(Windows 설정) > Security Settings(보안 설정) > Advanced Audit Policy Configuration(고급 감사 정책 컨피그레이션) > Audit Policies(감사 정책) > Logon/Logoff(로그온/로그오프)**로 이동합니다.

5단계 오른쪽 창에서 **Audit Logoff(감사 로그오프)**를 더블 클릭합니다.

6단계 Edit Logoff Properties(로그오프 속성 편집) 대화 상자에서 **Configure the following audit events(다음 감사 이벤트 구성)** 및 **Success(성공)**를 선택합니다.

7단계 **OK(확인)**를 클릭합니다.

8단계 **Audit Logon(감사 로그온)**에서 동일한 작업을 반복합니다.

참고 사용자 에이전트는 Windows Security Log(Windows 보안 로그) 이벤트 4634를 통해 식별한 로그오프 이벤트를 보고하지 않습니다. 사용자 에이전트는 로그오프에 대한 도메인 컴퓨터를 쿼리하기 위해 원격 WMI(Windows Management Instrumentation) 호출을 사용합니다.

유휴 세션 시간 초과 활성화

이 섹션에서는 경우에 따라 그룹 정책에서 유휴 세션 시간 초과를 활성화하는 방법을 설명합니다. 이렇게 하면 에이전트가 호스트의 여러 세션으로 인해 관련 없는 로그인을 탐지하고 보고하는 것을 방지할 수 있습니다.

Terminal Services를 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 명의 사용자가 워크스테이션에 원격으로 로그인할 수 있습니다. 그러나 해당 사용자가 로그아웃하지 않고 원격 데스크톱 세션 연결을 해제하는 경우 세션은 활성 상태로 유지됩니다. 사용자 입력이 없을 경우 활성 세션은 결국 유휴 상태로 전환됩니다.

또 다른 사용자가 한 세션이 유휴 상태일 때 원격 데스크톱을 사용하여 해당 워크스테이션에 로그인하면 두 로그인이 Management Center에 보고될 수 있습니다. 유휴 세션 시간 초과를 활성화하면 정의된 유휴 시간 초과 기간이 지난 후에 해당 세션이 종료되므로 호스트에서 여러 원격 세션이 실행되는 것을 방지할 수 있습니다.

Citrix 세션은 원격 데스크톱 세션과 유사하게 동작합니다. 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 있습니다.

Terminal Services 세션 시간 초과 활성화

Terminal Services 세션 시간 초과를 활성화하려면 Microsoft TechNet의 Terminal Services 세션에 대한 시간 초과 및 재연결 설정 구성에 설명된 대로 유휴 Terminal Services 세션 시간 초과에 대한 그룹 정책 설정과 Windows Server 2008 또는 Windows Server 2012에 대해 연결 해제된 Terminal Services 세션 시간 초과를 업데이트합니다.

유휴 및 연결 해제된 세션이 다음 로그오프 확인 전에 시간 초과될 수 있도록 세션 시간 초과 시간을 사용자 에이전트 로그오프 확인 빈도보다 짧게 설정합니다. 필수 유휴 세션 또는 연결 해제 세션 시간 초과가 있는 경우 사용자 에이전트의 로그오프 확인 빈도를 세션 시간 초과보다 *길게* 설정합니다. 로그오프 확인 빈도 구성에 대한 자세한 내용은 일반 사용자 에이전트 설정 구성, 2-29 페이지를 참조하십시오.

완료하고 나면 사용자 에이전트 컴퓨터 구성, 2-6페이지를 계속 진행합니다.

원격 데스크톱 세션 시간 초과 활성화

원격 데스크톱 세션 시간 초과를 활성화하려면 유휴 원격 세션 시간 초과 및 연결 해제된 세션 시간 초과의 그룹 정책 설정을 업데이트합니다. 세션 시간 초과 활성화에 대한 자세한 내용은 Microsoft TechNet의 세션 시간 제한을 참조하십시오.

유휴 및 연결 해제된 세션이 다음 로그오프 확인 전에 시간 초과될 수 있도록 원격 데스크톱 시간 초과 시간을 사용자 에이전트 로그오프 확인 빈도보다 *짧게* 설정합니다. 필수 유휴 세션 또는 연결 해제 세션 시간 초과가 있는 경우 사용자 에이전트의 로그오프 확인 빈도를 원격 데스크톱 시간 초과보다 *길게* 설정합니다. 로그오프 확인 빈도 구성에 대한 자세한 내용은 일반 사용자 에이전트 설정 구성, 2-29페이지를 참조하십시오.

완료하고 나면 사용자 에이전트 컴퓨터 구성, 2-6페이지를 계속 진행합니다.

Citrix 세션 시간 초과 활성화

Citrix 세션 시간 초과를 활성화하려면 http://support.citrix.com/에서 Citrix의 설명서를 참조하십시오.

도메인 컴퓨터 구성

로그오프 이벤트를 Management Center에 보내도록 사용자 에이전트를 활성화하려면 도메인에 연결하는 모든 컴퓨터에서 방화벽을 통해 WMI 트래픽을 허용해야 합니다.

다음과 같은 옵션이 있습니다.

- Windows 방화벽을 사용하여 도메인에 대해 WMI를 허용합니다.
- Microsoft TechNet의 고급 보안을 사용하는 Windows 방화벽 배포 가이드 등의 리소스에 설명된 대로 GPO(Group Policy Object)를 사용하여 방화벽 정책을 구성합니다.

사용자 에이전트 컴퓨터 구성

Management Center와 Active Directory 서버를 준비한 후에 에이전트를 설치 및 구성할 컴퓨터를 준비합니다.

사용자 에이전트 설치를 위한 컴퓨터 준비

사용자 에이전트는 이 섹션에서 다룬 요건을 충족하는 Windows 컴퓨터에서 설치할 수 있습니다.

컴퓨터 컨피그레이션

컴퓨터로 다음 중 하나가 사용될 수 있습니다.

- (권장 사항) Active Directory 서버에 액세스할 수 있으며 신뢰할 수 있는 네트워크에 있는 컴퓨터. 이 컴퓨터는 네트워크 관리자만 사용할 수 있어야 합니다.

  이 설치 방법이 가장 안전하므로 이 방법을 사용하는 것이 좋습니다.
- Active Directory 서버

사용자 에이전트 설치에 대한 사전 요구 사항

Windows 컴퓨터는 다음 사전 요구 사항을 충족해야 합니다.

- 컴퓨터에서 Windows Vista, Windows 7, Windows 8, Windows Server 2008 또는 Windows Server 2012를 실행하고 있습니다. 보안을 위해 Active Directory 서버 컴퓨터가 *아니라* 도메인 컴퓨터에서 사용자 에이전트를 설치하는 것이 좋습니다.
- 컴퓨터에 Microsoft .NET Framework 버전 4.0 Client Profile 및 Microsoft SQL CE(SQL Server Compact) 버전 3.5가 설치되어 있습니다.
  - Microsoft .NET Framework 버전 4.0 Client Profile 재배포 가능 패키지는 Microsoft 다운로드 사이트(`dotNetFx40_Client_x86_x64.exe`)에서 제공됩니다.
  - SQL Server Compact 3.5는 Microsoft 다운로드 사이트(`SSCERuntime-ENU.exe`)에서 제공됩니다.

참고 .NET Framework가 설치되지 않은 상태에서 에이전트 실행 파일(`setup.exe`)을 시작하면 다운로드하라는 프롬프트가 표시됩니다. 자세한 내용은 사용자 에이전트 설치, 2-18페이지를 참조하십시오.

- 사용자 에이전트용 사용자 생성, 2-7페이지에 설명된 대로 사용자 에이전트를 실행하도록 사용자를 생성합니다.
- 컴퓨터에 모니터링하려는 Active Directory 서버에 대한 TCP/IP 액세스가 있으며 Active Directory 서버와 동일한 버전의 인터넷 프로토콜이 사용됩니다. 에이전트가 Active Directory 서버를 실시간으로 모니터링하는 경우 로그인 데이터를 검색할 수 있도록 컴퓨터의 TCP/IP 액세스가 항상 켜져 있어야 합니다.

참고 Windows Server 2003 또는 이전 운영 체제에서 사용자 에이전트를 설치하는 경우 사용자 에이전트는 Active Directory 컴퓨터에서 실시간으로 통계를 수집할 수 없습니다.

- 컴퓨터에 데이터 및 IPv4 주소를 보고할 위치인 Management Center에 대한 TCP/IP 액세스가 있습니다.
- IPv6 주소로 호스트에서의 로그오프를 탐지하려는 경우에는 컴퓨터에 IPv6 주소가 있고, IPv4 주소로 호스트에서의 로그오프를 탐지하려는 경우에는 IPv4 주소가 있습니다.
- 컴퓨터에 레거시 에이전트나 버전 2.x의 에이전트가 아직 설치되어 있지 않습니다. 이러한 에이전트는 자동으로 제거되지 않으므로 기존 에이전트를 제거하려면 Windows 제어판에서 **프로그램 추가/제거**를 사용합니다.

주의 이전 버전의 사용자 에이전트가 설치되어 있는 경우 컨피그레이션 설정을 유지하려면 반드시 데이터베이스를 백업해야 합니다.

사용자 에이전트용 사용자 생성, 2-7페이지을 계속 진행합니다.

사용자 에이전트용 사용자 생성

최소 필수 권한으로 사용자 에이전트를 실행할 수 있으려면 사용자 에이전트용 사용자 어카운트를 생성해야 합니다.

- 사용자 에이전트의 이전 버전을 업그레이드하는 경우 이 단계는 필요하지 않습니다.

  이 경우에는 사용자 에이전트 컨피그레이션 백업, 2-17페이지를 참조하십시오.
- Active Directory 서버와 별개인 컴퓨터에서 사용자 에이전트를 실행하려면 사용자는 도메인 사용자여야 합니다.
- Active Directory 서버에서 사용자 에이전트를 실행하려면 사용자는 로컬 어카운트여야 합니다.

사용자를 생성하는 방법:

1단계 Domain Admins(도메인 관리자) 그룹의 멤버로 Active Directory 서버에 로그인합니다.

2단계 Active Directory 서버에서 사용자 에이전트를 실행하려면 로컬 사용자 어카운트를 생성합니다. 이 어카운트는 Domain Admins(도메인 관리자) 그룹에 속해야 하지만 사용자는 Administrators(관리자) 그룹에 속하지 않아도 됩니다.

이 섹션의 나머지 단계를 건너뛰고 사용자 권한 부여, 2-8페이지에서 작업을 계속 진행합니다.

3단계 별도의 컴퓨터에서 사용자 에이전트를 실행할 수 있도록 도메인 사용자를 생성하려면 **Start(시작) > Active Directory Users and Computers(Active Directory 사용자 및 컴퓨터)**를 클릭합니다.

4단계 왼쪽 창에서 사용자를 추가할 도메인 및 폴더를 펼칩니다.

5단계 사용자를 추가할 폴더를 마우스 오른쪽 버튼으로 클릭합니다.

6단계 팝업 메뉴에서 **New(새로 만들기) > User(사용자)**를 클릭합니다.

7단계 도메인 사용자를 생성하고 사용자에게 강력한 암호를 부여하려면 화면에 표시되는 프롬프트에 따라 작업을 수행합니다.

주의 보안을 위해 이 사용자 어카운트를 네트워크 관리자만 알고 있는지 확인하십시오.

사용자 권한 부여

이 섹션에서는 다음 가능성에 대해 다룹니다.

- Active Directory 서버에서 도메인 관리자 그룹에 로컬 사용자 추가.

  이 방법은 간단하지만 비교적 안전하지 않으므로 사용하지 않는 것이 좋습니다. 로컬 사용자에게 권한 부여, 2-8페이지를 참조하십시오.
- 도메인 사용자에게 사용자 에이전트를 실행하기 위한 최소 권한 부여. 도메인 사용자에게 제한된 권한 부여(요약), 2-8페이지를 참조하십시오.

로컬 사용자에게 권한 부여

Active Directory 서버에서 사용자 에이전트를 실행하려면 사용자를 Domain Admins(도메인 관리자) 그룹에 추가해야 합니다. 사용자 에이전트를 쉽게 설치할 수 있도록 경우에 따라 사용자를 Administrators(관리자) 그룹에 추가해야 할 수도 있습니다.

도메인 사용자에게 제한된 권한 부여(요약)

이 섹션에서는 도메인 사용자에게 사용자 에이전트를 실행하기 위한 최소 권한을 부여하는 데 필요한 작업에 대한 요약을 제공합니다. 예시는 도메인 사용자에게 제한된 권한 부여(단계별 예시), 2-9페이지를 참조하십시오.

도메인 사용자에게 제한된 권한을 부여하는 방법:

1단계 Domain Admins(도메인 관리자) 그룹의 멤버로 Active Directory 서버에 로그인합니다.

2단계 사용자 에이전트 사용자를 다음 그룹에 추가합니다.

- **Distributed COM Users(분산된 COM 사용자)**
- **Event Log Readers(이벤트 로그 판독기)**

3단계 Microsoft TechNet에 설명된 대로 WMI(Windows Management Instrumentation) 제어 콘솔을 사용하여 사용자에게 `Root\CIMV2` 노드에 대한 다음 권한을 부여합니다.

- **메서드 실행**
- **어카운트 활성화**
- **원격 활성화**
- **보안 읽기**

4단계 Active Directory 서버의 실시간 처리를 사용하도록 사용자 에이전트를 활성화합니다.

- Microsoft TechNet에 설명된 대로 RPC(Remote Procedure Call) 엔드포인트 매퍼 서비스로의 인바운드 네트워크 트래픽을 허용하도록 Windows 방화벽 규칙에 대한 GPO(Group Policy Object) 보안 정책을 생성합니다.
- Microsoft TechNet에 설명된 대로 임의 RPC 포트에서 인바운드 트래픽을 허용하도록 Windows 방화벽 규칙에 대한 GPO 보안 정책을 생성합니다.

실시간 처리에 대한 자세한 내용은 사용자 에이전트 Active Directory 서버 연결 구성, 2-20페이지를 참조하십시오.

5단계 `gupdate /force` 명령 또는 동등한 방법으로 GPO(Group Policy Object) 정책을 업데이트합니다.

도메인 사용자에게 제한된 권한 부여(단계별 예시)

이 섹션에서는 도메인 사용자에게 사용자 에이전트를 실행하기 위한 최소 권한을 부여하는 단계별 예시를 제공합니다.

이 섹션의 절차를 따르기 위해 시스템에서 다음을 사용 중이라고 가정하겠습니다.

- Windows Server 2012
- 사용자의 에이전트 사용자 이름: `limited.ua`
- 도메인 이름: `sesame.example.com`
- 하나의 Active Directory 서버와 하나의 Firepower Management Center에 연결하는 사용자 에이전트
- 실시간으로 Active Directory 서버에서 이벤트를 처리하는 사용자 에이전트

사용자에게 WMI(Windows Management Instrumentation) 권한 부여

이 섹션에서는 도메인 사용자 WMI 권한을 Active Directory 서버의 `Root(루트) > CIMV2` 노드에 부여하여 사용자가 도메인 컴퓨터에서 로그오프 이벤트를 검색할 수 있는 방법에 대한 설명을 제공합니다.

도메인 사용자에게 WMI 권한을 부여하는 방법:

1단계 Domain Admins(도메인 관리자) 그룹의 멤버로 Active Directory 서버에 로그인합니다.

2단계 사용자 에이전트 사용자를 다음 그룹에 추가합니다.

- **Distributed COM Users(분산된 COM 사용자)**
- **Event Log Readers(이벤트 로그 판독기)**

3단계 **Start(시작)**를 클릭하고 `wmimgmt.msc`를 입력합니다.

4단계 **Console Root(콘솔 루트) > WMI Control (Local)(WMI 제어(로컬))**을 마우스 오른쪽 버튼으로 클릭하고 **Properties(속성)**를 클릭합니다.

5단계 WMI Control (Local) Properties(WMI 제어(로컬) 속성) 대화 상자에서 **Security(보안)** 탭을 클릭합니다.

6단계 **Root(루트) > CIMV2**를 클릭합니다.

7단계 **Security(보안)**를 클릭합니다.

8단계 ROOT\CIMV2에 대한 Security(보안) 대화 상자에서 **Add(추가)**를 클릭합니다.

9단계 **Enter object names to select(선택할 개체 이름 입력)** 필드에 `limited.ua`를 입력하고 **Check Names(이름 확인)**를 클릭합니다.

Windows에서 사용자 이름을 찾아 필드에 표시합니다.

10단계 **OK(확인)**를 클릭합니다.

11단계 사용자에게 다음 권한을 부여합니다.

- **메서드 실행**
- **어카운트 활성화**
- **원격 활성화**
- **보안 읽기**

12단계 Root\CIMV2에 대한 Security(보안) 대화 상자에서 **OK(확인)**를 클릭합니다.

13단계 WMI Control Properties(WMI 제어 속성) 대화 상자에서 **OK(확인)**를 클릭합니다.

WMI 권한 테스트

Active Directory 서버에서 사용자 에이전트 사용자에게 WMI 권한을 부여한 이후에 사용자 에이전트를 설치할 컴퓨터에서 이 권한을 테스트해야 합니다.

WMI 권한을 테스트하는 방법:

1단계 사용자 에이전트를 설치할 도메인 컴퓨터에 로그인합니다.

2단계 검색 필드에 `wbemtest`를 입력합니다. 일부 버전의 Windows에서는 먼저 **Start(시작)**를 클릭해야 합니다.

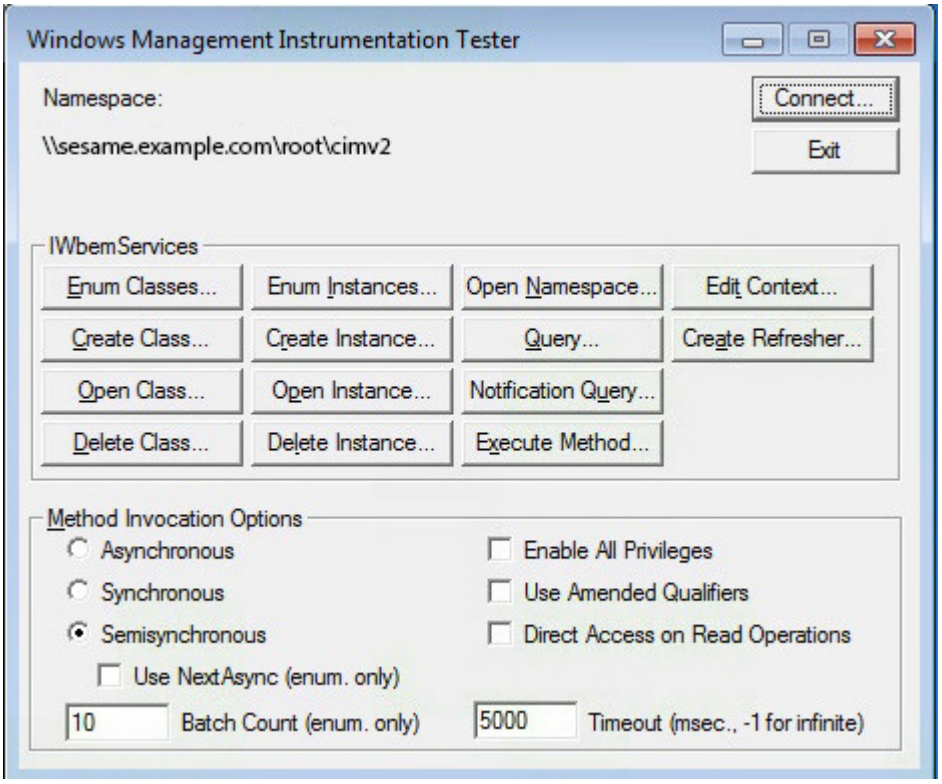
3단계 Windows Management Instrumentation Tester(Windows Management Instrumentation 테스터) 대화 상자에서 **Connect(연결)**를 클릭합니다.

4단계 Connect(연결) 대화 상자에 다음 정보를 입력합니다.

- **Namespace(네임스페이스)** 필드: `\\`*`namespace`*`\root\cimv2` 형식을 사용하여 Active Directory 서버의 이름과 경로를 입력합니다. 이 예시에서는 `\\sesame.example.com\root\cimv2`를 입력합니다.
- **Credentials(자격 증명)** 필드: *`domain`*`\`*`username`* 형식의 사용자 이름을 **User(사용자)** 필드에 입력하고 사용자 비밀번호를 **Password(비밀번호)** 필드에 입력합니다. 이 예시에서는 사용자 이름이 `sesame\limited.ua`입니다.
- 일반적으로 이 대화 상자에서 다른 옵션은 변경할 필요가 없습니다.

5단계 **Connect(연결)**를 클릭합니다.

연결에 성공하면 Windows Management Instrumentation Tester(Windows Management Instrumentation 테스터) 대화 상자가 다음과 같이 표시됩니다.



오류가 표시되면 다음을 시도합니다.

- `The RPC server is unavailable(RPC 서버를 사용할 수 없습니다.)`은 네임스페이스가 올바르지 않거나 Active Directory 서버에 액세스할 수 없음을 나타냅니다(네트워크 문제, 서버 다운됨 등).
- `Access is denied(액세스가 거부되었습니다.)`는 올바르지 않은 사용자 이름 또는 비밀번호를 나타냅니다.

6단계 테스트에 성공하면 **Query(쿼리)**를 클릭합니다.

7단계 Query(쿼리) 대화 상자에 다음을 입력합니다.

```
select * from Win32_NTLogEvent where Logfile = 'Security' and (EventCode=672 or
EventCode=4768 or EventCode=538 or EventCode=4364 or EventCode=528 or EventCode=4624 or
EventCode=4634) and TimeGenerated > "date-code"
```

date-code는 `YYYYMMDDHHMMSS.fractionalSecond-utc_timezone_offset` 형식의 Microsoft 시간 및 날짜 코드입니다.

예를 들어 미국 중부 표준 시간대(UTC-6시간)에서 2017년 5월 1일 자정에 쿼리하도록 하려면 다음과 같이 입력합니다.

```
select * from Win32_NTLogEvent where Logfile = 'Security' and (EventCode=672 or
EventCode=4768 or EventCode=538 or EventCode=4364 or EventCode=528 or EventCode=4624 or
EventCode=4634) and TimeGenerated > "20170501000000.000000-600"
```

8단계 **Query Type(쿼리 유형)** 목록에서 **WQL**을 클릭합니다.

9단계 **Apply(적용)**를 클릭합니다.

쿼리가 새 대화 상자에 표시됩니다.

`Invalid class`(유효하지 않은 클래스) 또는 `Invalid query`(유효하지 않은 쿼리) 오류가 표시되는 경우 명령 구문을 확인하고 다시 시도합니다. 결과가 표시되지 않으면 날짜 코드를 확인합니다.

10단계 로그 보기를 마치면 **Close(닫기)**를 클릭합니다.

11단계 Windows Management Instrumentation Tester(Windows Management Instrumentation 테스터) 대화 상자에서 **Exit(종료)**을 클릭합니다.

사용자 에이전트가 DCOM(Distributed Component Object Management)에 액세스하도록 허용

이 섹션에서는 사용자 에이전트가 원격으로 Active Directory 서버에 있는 개체에 액세스할 수 있도록 DCOM 액세스를 허용하는 방법을 설명합니다.

사용자에게 DCOM 액세스 권한을 부여하는 방법:

1단계 Domain Admins(도메인 관리자) 그룹의 멤버로 Active Directory 서버에 로그인합니다.

2단계 **시작 > [실행]**을 클릭하고 `dcomcnfg`를 입력한 다음 Enter 키를 누릅니다.

3단계 Component Services(구성 요소 서비스) 창에서 **Component Services(구성 요소 서비스) > Computers(컴퓨터)**를 클릭합니다.

4단계 **My Computer(내 컴퓨터)**를 마우스 오른쪽 버튼으로 클릭하고 **Properties(속성)**를 클릭합니다.

5단계 My Computer Properties(내 컴퓨터 속성) 대화 상자에서 **COM Security(COM 보안)** 탭을 클릭합니다.

6단계 Launch and Activation Permissions(실행 및 활성화 권한)에서 **Edit Limits(제한 사항 편집)**를 클릭합니다.

7단계 Launch and Activation Permissions(실행 및 활성화 권한) 대화 상자에서 **Add(추가)**를 클릭합니다.

8단계 **Enter the object names to select(선택할 개체 이름 입력)** 필드에 `limited.ua`를 입력하고 **Check Names(이름 확인)**를 클릭합니다.

9단계 이름이 일치하면 **OK(확인)**를 클릭합니다.

10단계 사용자에게 **Remote Launch(원격 실행)** 및 **Remote Activation(원격 활성화)** 권한을 부여합니다.

11단계 Launch and Activation Permissions(실행 및 활성화 권한) 대화 상자에서 **OK(확인)**를 클릭합니다.

12단계 My Computer Properties(내 컴퓨터 속성) 대화 상자에서 **OK(확인)**를 클릭합니다.

Active Directory 보안 로그에 액세스할 수 있도록 그룹 개체 정책을 업데이트하는 방법:

1단계 **Start(시작) > [All Programs(모든 프로그램)] > Administrative Tools(관리 툴) > Group Policy Management(그룹 정책 관리)**를 클릭합니다.

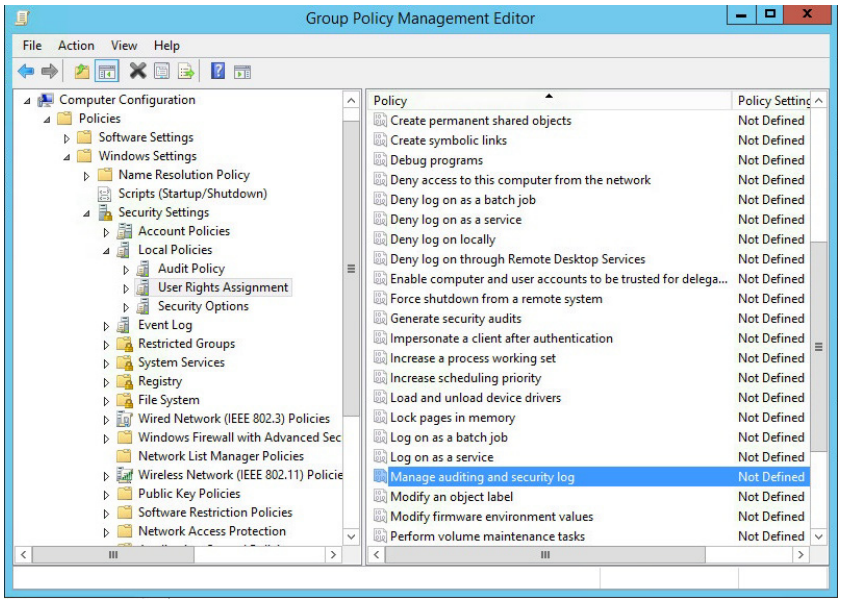
2단계 탐색 창에서 **Forest(포리스트):** ***YourForestName(포리스트 이름)***을 펼치고 **Domains(도메인) >** ***YourDomainName(도메인 이름)*** **> Group Policy Objects(그룹 정책 개체)**를 펼칩니다.

3단계 **Default Domain Policy(기본 도메인 정책)**를 마우스 오른쪽 버튼으로 클릭하고 **Edit(편집)**을 클릭합니다.

4단계 **Computer Configuration(컴퓨터 컨피그레이션) > Policies(정책) > Windows Settings(Windows 설정) > Security Settings(보안 설정) > Local Policies(로컬 정책) > User Rights Assignment(사용자 권한 할당)**로 이동합니다.

5단계 오른쪽 창에서 **Manage auditing and security log(감사 및 보안 로그 관리)**를 더블 클릭합니다.

다음 그림에 예시가 나와 있습니다.



6단계 **Define these policy settings(이 정책 설정 정의)**를 선택합니다.

7단계 **Add User or Group(사용자 또는 그룹 추가)**을 클릭합니다.

8단계 Add User or Group names(사용자 또는 그룹 이름 추가) 필드에서 사용자 에이전트 사용자 이름을 입력하거나 **Browse(찾아보기)**를 클릭하여 찾아봅니다.

9단계 Manage auditing and security log Properties(감사 및 보안 로그 관리 속성) 대화 상자에서 **OK(확인)**를 클릭합니다.

Windows 방화벽에 대한 그룹 정책 개체 규칙 생성

이 섹션은 사용자 에이전트가 Active Directory 서버의 실시간 이벤트 처리를 사용하는 데 필요합니다. 실시간 이벤트 처리에 대한 자세한 내용은 사용자 에이전트 Active Directory 서버 연결 구성, 2-20페이지를 참조하십시오.

인바운드 RPC(Remote Procedure Call) 네트워크 트래픽을 허용하려면 Group Policy Management(그룹 정책 관리)에서 Advanced Security(고급 보안) 노드가 있는 Windows 방화벽을 사용하여 두 개의 방화벽 규칙을 생성합니다.

- 첫 번째 규칙은 동적으로 할당된 포트 번호(클라이언트가 서비스와 통신하기 위해 사용해야 함)에 응답하는, RPC 엔드포인트 매퍼 서비스에 들어오는 트래픽을 허용합니다.
- 두 번째 규칙은 동적으로 할당된 포트 번호로 전송되는 네트워크 트래픽을 허용합니다.

두 가지 규칙을 사용하면 RPC 동적 포트 리디렉션이 수신된 컴퓨터에서 전송되는 네트워크 트래픽과 RPC 엔드포인트 매퍼에서 할당된 포트 번호로만 전송되는 네트워크 트래픽만 허용함으로써 컴퓨터를 보호할 수 있습니다.

사용자 에이전트가 액세스를 필요로 하는 모든 Active Directory 서버에서 다음 절차에 설명된 작업을 수행합니다.

RPC 트래픽을 허용하도록 GPO 방화벽 규칙을 생성하는 방법:

1단계 아직 이 작업을 수행하지 않은 경우 Domain Admins(도메인 관리자) 그룹의 멤버로 Active Directory 서버에 로그인합니다.

2단계 **Start(시작)Administrative Tools(관리 툴)**를 선택합니다.

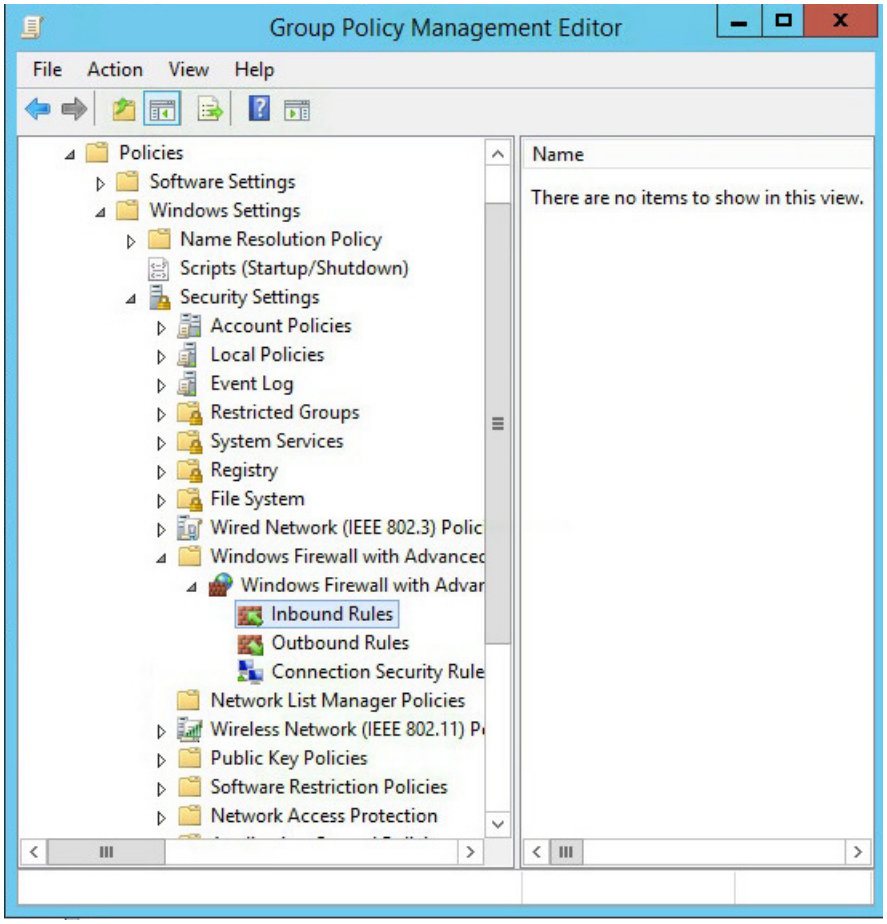
3단계 Administrative Tools(관리 툴) 창에서 **Group Policy Management(그룹 정책 관리)**를 더블 클릭합니다.

4단계 탐색 창에서 **Forest(포리스트): *YourForestName(포리스트 이름)***을 펼치고 **Domains(도메인)**, > ***YourDomainName(도메인 이름)*** > **Group Policy Objects(그룹 정책 개체)**를 펼친 다음, 수정할 GPO를 마우스 오른쪽 버튼으로 클릭하고 **Edit(편집)**을 클릭합니다.

일반적으로 **Default Domain Policy(기본 도메인 정책)**를 편집해야 합니다.

5단계 왼쪽 창에서 **Computer Configuration(컴퓨터 컨피그레이션) > Policies(정책) > Windows Settings(Windows 설정) > Security Settings(보안 설정) > Windows Firewall with Advanced Security(고급 보안을 사용하는 Windows 방화벽) > Windows Firewall with Advanced Security(고급 보안을 사용하는 Windows 방화벽)**를 펼칩니다.

다음 그림에 예시가 나와 있습니다.



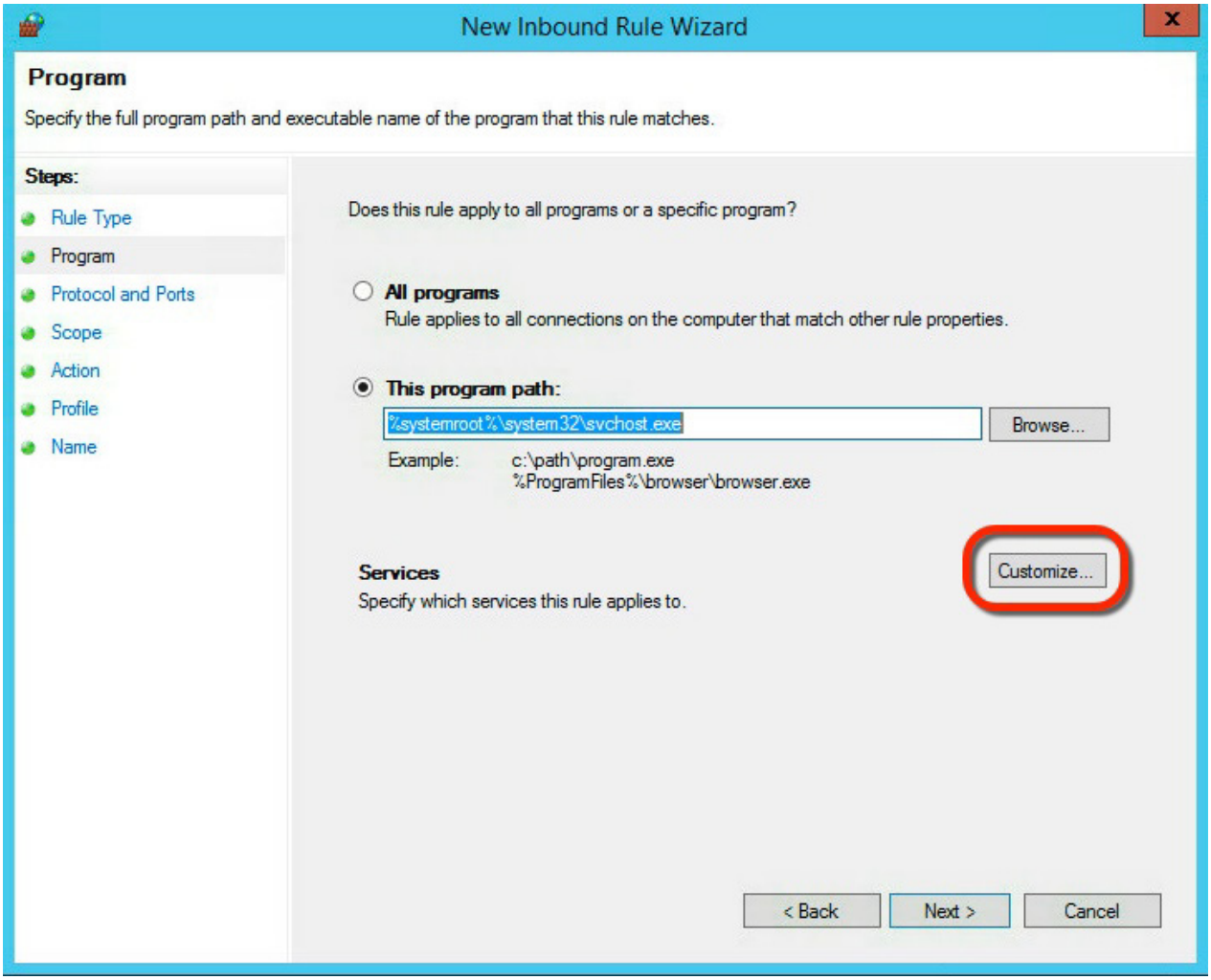
6단계 **Inbound Rules(인바운드 규칙)**를 마우스 오른쪽 버튼으로 클릭하고 **New Rule(새 규칙)**을 클릭합니다.

7단계 New Inbound Rule Wizard(새 인바운드 규칙 마법사) 대화 상자에서 **Custom(맞춤화)**을 클릭하고 **Next(다음)**를 클릭합니다.

8단계 **This program path(이 프로그램 경로)**를 클릭한 다음 `%systemroot%\system32\svchost.exe`를 입력합니다.

9단계 Services(서비스) 옆에 있는 **Customize(맞춤화)**를 클릭합니다.

다음 그림에 예시가 나와 있습니다.



10단계 Customize Service Settings(서비스 설정 맞춤화) 대화 상자에서 **Apply to this service(이 서비스에 적용)**를 클릭하고 **RPC(Remote Procedure Call)**(짧은 이름은 **RpcSs**)를 클릭한 다음 **OK(확인)**를 클릭합니다.

11단계 **Next(다음)**를 클릭합니다. 작업을 확인해야 합니다.

12단계 Protocol and Ports(프로토콜 및 포트) 대화 상자에서 **Protocol type(프로토콜 유형)**으로 **TCP**를 클릭합니다.

13단계 **Local port(로컬 포트)**에서 **RPC Endpoint Mapper(RPC 엔드포인트 매퍼)**를 선택한 다음 **Next(다음)**를 클릭합니다.

14단계 Scope(범위) 페이지에서 **Which remote IP addresses does this rule apply to?(이 규칙을 적용할 원격 IP 주소는 무엇입니까?)** 섹션에서 **These IP addresses(이 IP 주소)**를 선택하고 **Add(추가)**를 클릭한 다음 사용자 에이전트 컴퓨터의 IP 주소를 입력합니다.

15단계 **Next(다음)**를 클릭합니다.

16단계 Action(작업) 페이지에서 **Allow the connection(연결 허용)**을 선택한 후 **Next(다음)**를 클릭합니다.

17단계 Profiles(프로파일) 페이지에서 **Domain(도메인)**만 선택하고 **Next(다음)**를 클릭합니다.

18단계 Name(이름) 페이지에서 이 규칙을 식별할 이름을 입력하고 **Finish(완료)**를 클릭합니다.

동적으로 매핑된 포트를 허용하도록 GPO 규칙을 생성하는 방법:

1단계 Windows 방화벽에 대한 그룹 정책 개체 규칙 생성, 2-13페이지의 1 단계단계~4 단계단계를 완료합니다.

2단계 New Inbound Rule Wizard(새 인바운드 규칙 마법사) 대화 상자에서 **Custom(맞춤화)**을 클릭하고 **Next(다음)**를 클릭합니다.

3단계 **This program path(이 프로그램 경로)**를 클릭한 다음 `%systemroot%\system32\svchost.exe`를 입력합니다.

4단계 Services(서비스) 옆에 있는 **Customize(맞춤화)**를 클릭합니다.

5단계 Customize Service Settings(서비스 설정 맞춤화) 대화 상자에서 **Apply to this service(이 서비스에 적용)**를 클릭하고 **Windows Event Log(Windows 이벤트 로그)**(짧은 이름은 **EventLog(이벤트 로그)**)를 클릭한 다음 **OK(확인)**를 클릭합니다.

6단계 **Next(다음)**를 클릭합니다. 작업을 확인해야 합니다.

7단계 Protocol and Ports(프로토콜 및 포트) 대화 상자에서 **Protocol type(프로토콜 유형)**으로 **TCP**를 클릭합니다.

8단계 Local port(로컬 포트)에서 **RPC Dynamic Ports(RPC 동적 포트)**를 클릭한 후 **Next(다음)**를 클릭합니다.

9단계 Scope(범위) 페이지에서 **These IP addresses(이 IP 주소)**를 클릭하고 **Add(추가)**를 클릭한 다음 사용자 에이전트 컴퓨터의 IP 주소를 입력합니다.

10단계 **Next(다음)**를 클릭합니다.

11단계 Action(작업) 페이지에서 **Allow the connection(연결 허용)**을 클릭하고 **Next(다음)**를 클릭합니다.

12단계 Profiles(프로파일) 페이지에서 **Domain(도메인)**만 선택하고 **Next(다음)**를 클릭합니다.

13단계 Name(이름) 페이지에서 이 규칙을 식별할 이름을 입력하고 **Finish(완료)**를 클릭합니다.

GPO 정책을 적용하는 방법:

1단계 `gupdate /force` 명령 또는 동등한 방법으로 새 GPO 정책을 적용합니다.

GPO 정책 적용에 대한 자세한 내용은 다음 자료를 참조하십시오.

- 초보자를 위한 GPO 정책(Microsoft TechNet)
- 정책 처리(Microsoft TechNet)

참고 상승된 권한을 사용하여 `gpupdate /force` 명령을 실행해야 합니다. Active Directory 서버에 Administrator(관리자)로 로그인하거나 명령 프롬프트를 관리자 권한으로 실행(명령 프롬프트 바로가기를 마우스 오른쪽 버튼으로 클릭하고 **Run as Administrator(관리자 권한으로 실행)**를 클릭)합니다.

사용자 에이전트 컨피그레이션 백업

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

참고 버전 2.2 이상의 사용자 에이전트가 설치되어 있다면 데이터베이스를 백업할 필요가 없습니다. 이 경우 새로운 버전의 사용자 에이전트를 설치할 때 컨피그레이션 설정을 자동으로 가져오게 됩니다. 사용자 에이전트 설치, 2-18페이지을 계속 진행합니다.

컨피그레이션 설정을 유지하는 방법:

1단계 에이전트를 설치한 컴퓨터에서, **Start(시작) > Programs(프로그램) > Cisco > Configure Cisco Firepower User Agent for Active Directory(Active Directory용 Cisco Firepower 사용자 에이전트 구성)**를 클릭합니다.

2단계 에이전트 서비스를 중지하려면 중지 버튼(■)을 클릭합니다.

3단계 에이전트가 설치된 컴퓨터에서 `CiscoUserAgent.sdf`를 찾아 해당 파일을 로컬에 복사합니다.

참고 2.2 이전 버전에서 업데이트하는 경우 `SourcefireUserAgent.sdf`를 찾아 복사합니다. 파일의 사본을 만들고 사본의 이름을 `CiscoUserAgent.sdf`로 변경합니다.

4단계 제어판의 **프로그램 추가/제거** 옵션을 사용하여 Cisco User Agent를 제거합니다. 에이전트를 제거합니다.

5단계 최신 버전의 사용자 에이전트를 설치합니다. 자세한 내용은 사용자 에이전트 설치, 2-18페이지를 참조하십시오.

6단계 에이전트를 설치한 컴퓨터에서 **Start(시작) > Programs(프로그램) > Cisco > Configure Cisco Firepower User Agent for Active Directory(Active Directory용 Cisco Firepower 사용자 에이전트 구성)**를 선택합니다.

7단계 에이전트 서비스를 중지하려면 중지 버튼(■)을 클릭합니다.

8단계 최신 버전의 에이전트가 설치된 컴퓨터에서 `CiscoUserAgent.sdf`를 찾습니다. 현재 파일을 이전 버전의 에이전트에서 만든 로컬 백업으로 교체합니다.

9단계 최신 버전의 에이전트를 설치한 컴퓨터에서 **Start(시작) > Programs(프로그램) > Cisco > Configure Cisco Firepower User Agent for Active Directory(Active Directory용 Cisco Firepower 사용자 에이전트 구성)**를 선택합니다.

10단계 ▶ 아이콘을 클릭하여 서비스를 시작합니다.

사용자 에이전트 설치, 2-18페이지를 계속 진행합니다.

사용자 에이전트 설치

라이선스: FireSIGHT 또는 해당 없음

Active Directory 서버에 연결할 권한을 구성하고 유휴 원격 세션 시간 초과를 구성한 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, 2-17페이지를 참조하십시오.

기본적으로 에이전트는 **로컬 시스템** 어카운트를 사용하는 서비스로 실행됩니다. 에이전트를 실행 중인 Windows 컴퓨터가 네트워크에 연결되어 있다면 사용자가 해당 컴퓨터에 실제로 로그인되어 있지 않은 경우에도 서비스를 통해 사용자 데이터를 폴링하고 전송하는 작업이 계속 진행됩니다.

각 에이전트에 대해 하나 이상의 Active Directory 서버 및 최대 5개의 Management Center에 대한 연결을 구성할 수 있습니다. Management Center 연결을 추가하기 전에 Management Center 컨피그레이션에 에이전트를 추가해야 합니다. 자세한 내용은 다음을 참조하십시오.

- 사용자 에이전트에 연결하도록 버전 5.x Defense Center 구성, 2-3페이지
- 사용자 에이전트에 연결하도록 버전 6.x Management Center 구성, 2-3페이지

둘 이상의 사용자 에이전트 구축에 대한 자세한 내용은 여러 사용자 에이전트 구축, 1-5페이지를 참조하십시오.

고가용성 컨피그레이션에서는 에이전트에 기본 및 보조 Management Center를 모두 추가함으로써 사용자 로그인 데이터 업데이트를 활성화하여 두 Management Center의 데이터가 모두 유지되도록 합니다.

사용자 에이전트를 설치하는 방법:

액세스: 모두

1단계 사용자 에이전트용 사용자 생성, 2-7페이지에서 생성한 사용자로 사용자 에이전트를 설치할 Windows 컴퓨터에 로그인합니다.

- 사용자 에이전트의 이전 버전을 업그레이드하는 경우 해당 컴퓨터에 로그인합니다.
- (권장 사항) Active Directory 서버와 별개인 컴퓨터에서 사용자 에이전트를 설치하려면 해당 컴퓨터에 로그인합니다.
- Active Directory 서버에 사용자 에이전트를 설치하려면 Domain Admins(도메인 관리자) 그룹의 멤버로 Active Directory 서버에 로그인하고, 경우에 따라 Administrators(관리자) 그룹으로 로그인합니다.

2단계 지원 사이트에서 사용자 에이전트 설치 파일 (`Cisco_Firepower_User_Agent_for_Active_Directory_2.3-10.zip`)을 다운로드합니다.

참고 지원 사이트에서 직접 사용자 에이전트 설치 파일이 포함되어 있는 압축된 아카이브를 다운로드합니다. 파일이 손상될 수 있으므로 이메일로 전송하지 마십시오.

3단계 `.zip` 파일을 마우스 오른쪽 버튼으로 클릭하고 **Extract All(모두 추출)**을 선택합니다.

4단계 파일을 추출할 폴더를 선택합니다.

에이전트를 설치하는 데에는 3MB의 하드 드라이브 공간이 필요합니다. 에이전트 로컬 데이터베이스에 4GB의 하드 드라이브 공간을 할당하는 것이 좋습니다.

5단계 파일을 추출한 폴더에서 `setup.exe`를 더블 클릭합니다.

참고 `setup.msi` *가 아닌* `setup.exe`를 더블 클릭하십시오. `setup.msi`는 사용자 에이전트를 설치하기 전에 필수 소프트웨어를 확인하지 않습니다. 이로 인해 에이전트 설치 또는 실행 중에 오류가 발생할 수 있습니다.

정보 관리자 그룹의 멤버가 아닌 어카운트를 사용하고 Windows 컴퓨터에 새 애플리케이션을 설치하는 데 필요한 권한을 보유하지 않은 경우 설치를 시작하는 데 적합한 권한을 보유한 관리자 그룹에 속해 있는 사용자에게 에스컬레이션해야 합니다. 에스컬레이션 옵션에 액세스하려면 `setup.exe` 파일을 마우스 오른쪽 버튼으로 클릭하고 **Run As(다음 자격으로 실행)**를 클릭합니다. 적합한 사용자를 선택하고 해당 사용자의 비밀번호를 입력합니다.

6단계 설치를 계속하려면 라이선스 계약을 수락해야 합니다.

7단계 에이전트를 설치하려는 Windows 컴퓨터에 Microsoft .NET Framework 버전 4.0 Client Profile 및 SQL Server Compact 3.5가 설치되어 있지 않다면 적합한 파일을 다운로드하라는 프롬프트가 표시됩니다. 파일을 다운로드하고 설치합니다.

8단계 마법사의 프롬프트를 따라 에이전트를 설치합니다.

컴퓨터에서 사용자 어카운트 제어를 활성화한 경우 변경을 수행하는 권한을 요청하는 모든 프롬프트에 **Yes(예)**라고 대답해야 합니다.

9단계 에이전트 구성을 시작하려면 사용자 에이전트 구성, 2-19페이지를 참조하십시오.

사용자 에이전트 구성

라이선스: FireSIGHT 또는 해당 없음

에이전트가 설치된 후 Active Directory 서버에서 데이터를 수신하고 Management Center로 정보를 보고하며 보고에서 특정 사용자 이름 및 IP 주소를 제외하고 로컬 이벤트 로그나 Windows 애플리케이션 로그에 상태 메시지를 로깅하도록 구성할 수 있습니다.

에이전트를 구성하는 방법:

액세스: 모두

1단계 에이전트를 설치한 컴퓨터에서, **Start(시작) > Programs(프로그램) > Cisco > Configure Cisco Firepower User Agent for Active Directory(Active Directory용 Cisco Firepower 사용자 에이전트 구성)**를 선택합니다.

다음 표에서는 에이전트 구성 시 수행해야 할 작업과 이를 구성할 위치를 설명합니다.

표 2-1 사용자 에이전트 컨피그레이션 작업

작업	방법
에이전트 이름 변경, 로그오프 확인 빈도 변경, 서비스 시작 및 중지, 우선순위 일정 설정	**General(일반)** 탭을 클릭합니다. 자세한 내용은 일반 사용자 에이전트 설정 구성, 2-29페이지를 참조하십시오.
Active Directory 서버 추가/수정/제거, 실시간 Active Directory 서버 데이터 검색 활성화, Active Directory 서버 폴링 간격 및 최대 폴링 시간 수정	**Active Directory Servers(Active Directory 서버)** 탭을 클릭합니다. 자세한 내용은 사용자 에이전트 Active Directory 서버 연결 구성, 2-20페이지를 참조하십시오.
Management Center 추가 또는 제거	**Firepower Management Centers** 탭을 클릭합니다. 자세한 내용은 사용자 에이전트 Management Center 연결 구성, 2-24페이지를 참조하십시오.
보고에서 제외된 사용자 이름 추가, 수정 또는 제거	**Excluded Usernames(제외된 사용자 이름)** 탭을 클릭합니다. 자세한 내용은 사용자 이름이 제외된 사용자 에이전트 설정 구성, 2-25페이지를 참조하십시오.
보고에서 제외된 IP 주소 추가, 수정 또는 제거	**Excluded Addresses(제외된 주소)** 탭을 클릭합니다. 자세한 내용은 주소가 제외된 사용자 에이전트 설정 구성, 2-26페이지를 참조하십시오.
이벤트 로그 보기/내보내기/지우기, Windows 애플리케이션 로그에 로깅, 메시지 유지 기간 수정	**Logs(로그)** 탭을 클릭합니다. 자세한 내용은 사용자 에이전트 로깅 설정 구성, 2-27페이지를 참조하십시오.
Cisco TAC의 안내에 따라 트러블슈팅 및 유지 관리 작업 수행	**Logs(로그)** 탭을 클릭하고 **Show Debug Messages in Log(로그에 디버그 메시지 표시)**를 활성화한 다음 **Maintenance(유지 관리)** 탭을 선택합니다. 자세한 내용은 사용자 에이전트 유지 관리 설정 구성, 2-30페이지를 참조하십시오.
에이전트 설정 변경 사항 저장	**Save(저장)**를 클릭합니다. 변경 사항이 저장되지 않은 경우 알림 메시지가 표시됩니다.
에이전트 설정에 대한 변경 사항을 저장하지 않고 에이전트 닫기	**Cancel(취소)**을 클릭합니다.

사용자 에이전트 Active Directory 서버 연결 구성

라이선스: FireSIGHT 또는 해당 없음

사용자 에이전트에서 하나 이상의 Active Directory 서버에 대한 연결을 추가하여 다음을 구성할 수 있습니다.

- 에이전트가 로그인 및 로그오프 데이터를 실시간으로 검색할 수 있게 할 것인지 아니면 주기적으로 데이터에 대해 Active Directory 서버를 폴링할 수 있게 할 것인지 여부
- 에이전트가 얼마나 자주 사용자 활동 데이터에 대해 폴링하게 할 것인지, 또는 연결이 끊어진 경우 Active Directory 서버와의 실시간 연결을 설정 또는 재설정하려는 시도를 얼마나 자주 할 것인지 여부

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

사용자 에이전트가 실시간으로 데이터를 검색하도록 구성되어 있고 실시간 모니터링을 사용할 수 없는 경우 에이전트에서 대신 실시간 모니터링을 다시 사용할 수 있을 때까지 데이터에 대해 Active Directory 서버 폴링을 시도합니다.

정보 사용자 에이전트가 검색한 사용자 활동량이 상당할 경우 실시간 데이터 검색 대신 폴링을 구성하는 것이 좋습니다. 활동이 많은 환경에서는 1분의 폴링 간격을 구성하고 최대 폴링 시간은 10분을 넘지 않게 구성합니다.

실시간 모니터링에는 Windows Server 2008 이상을 실행 중인 Active Directory 서버가 필요합니다.

참고 Windows Server 2003 또는 이전 운영 체제에서 사용자 에이전트를 설치하는 경우 사용자 에이전트는 Active Directory 컴퓨터에서 실시간으로 통계를 수집할 수 없습니다.

사용자 에이전트에서 탭이 선택되면 해당 시점의 현재 Active Directory 서버 폴링 상태, 에이전트에 보고된 마지막 로그인, 에이전트에서 마지막으로 Active Directory 서버를 폴링한 시간을 확인할 수 있습니다.

또한, 에이전트가 실시간으로 Active Directory 서버를 폴링하고 있는지와 탭이 선택된 시점의 실시간 데이터 검색 상태를 확인할 수 있습니다. 서버 상태에 대한 자세한 내용은 다음 표를 참조하십시오.

표 2-2 Active Directory 서버 상태

Active Directory 서버 상태	폴링 가용성	실시간 가용성
available(사용 가능)	서버는 폴링할 수 있습니다.	서버는 실시간 데이터 검색을 사용할 수 있습니다.
unavailable(사용 불가)	서버는 폴링할 수 없습니다.	서버는 실시간 데이터 검색을 사용할 수 없거나 폴링을 하도록 구성되었습니다.
pending(보류 중)	서버 컨피그레이션이 추가되었으나 통신이 아직 시작되지 않았습니다.	서버 컨피그레이션을 추가 및 저장한 후 사용자 에이전트와 통신을 시작하려면 시간이 조금 필요합니다. pending(보류 중) 상태가 지속되는 경우 사용자 에이전트와 서버 간의 통신을 확인하십시오.
Unknown(알 수 없음)	에이전트가 시작되었지만 아직 사용할 수 없는 상태이거나 에이전트가 아직 Active Directory 서버를 확인하지 않았습니다.	에이전트가 시작되었지만 아직 사용할 수 없는 상태이거나 에이전트가 아직 Active Directory 서버를 확인하지 않았습니다.

참고 각 사용자 에이전트가 다른 연결을 탐지하여 관련이 없는 로그인을 보고할 수 있으므로 동일한 Active Directory 도메인 컨트롤러에 둘 이상의 사용자 에이전트를 연결하지 않아야 합니다. 연결하는 경우 각 사용자 에이전트가 동일한 Active Directory 서버를 폴링하는 에이전트를 실행 중인 다른 모든 호스트의 IP 주소와 해당 에이전트가 로그인하는 데 사용하는 사용자 이름을 제외하도록 구성해야 합니다. 자세한 내용은 주소가 제외된 사용자 에이전트 설정 구성, 2-26페이지를 참조하십시오.

Active Directory 서버 연결을 구성하는 방법:

액세스: 모두

1단계 필요한 경우 사용자 에이전트가 설치된 컴퓨터에 로그인합니다.

2단계 **Start(시작)** > **[All(모든)] Programs(프로그램)** > **Cisco** > **Configure Cisco Firepower Agent for Active Directory(Active Directory용 Cisco Firepower Agent 구성)**를 클릭합니다.

3단계 **Active Directory Servers(Active Directory 서버)** 탭을 클릭합니다.

4단계 다음과 같은 옵션이 있습니다.

- 서버에 새 연결을 추가하려면 **Add(추가)**를 클릭합니다.
- 기존 연결을 수정하려면 서버 이름을 더블 클릭합니다.
- 기존 연결을 제거하려면 서버 이름을 클릭하고 **Remove(제거)**를 클릭합니다.

5단계 **Server Name/IP Address(서버 이름/IP 주소)** 필드에 Active Directory 서버 또는 도메인 컨트롤러의 정규화된 서버 이름이나 IP 주소를 입력합니다. Active Directory 서버에 대한 로그인을 탐지할 경우 IP 주소를 입력합니다.

에이전트가 Active Directory 서버에 설치되어 있는 경우 에이전트를 설치한 위치에 에이전트를 추가하려면 서버 이름으로 `localhost`를 입력합니다. 사용자 이름 및 비밀번호를 추가할 수도 있습니다. 해당 정보를 생략하는 경우 해당 Active Directory 서버를 대상으로 인증 중인 사용자의 로그오프는 탐지할 수 없습니다. 서버는 사용자 이름 및 비밀번호 입력 여부와 관계없이 폴링할 수 있습니다.

참고 Active Directory 시스템에 여러 개의 도메인 컨트롤러가 있는 경우 사용자 에이전트가 통신할 도메인 컨트롤러의 호스트 이름 또는 IP 주소를 입력합니다. Active Directory 도메인 컨트롤러는 보안 로그를 공유하지 않으므로 각 컨트롤러에 별도의 사용자 에이전트 연결이 있어야 합니다. 시스템이 분산되었거나 트래픽이 심한 경우 여러 사용자 에이전트 구축, 1-5페이지에 설명된 대로 둘 이상의 사용자 에이전트를 설치할 수도 있습니다.

6단계 **Authorized User(권한이 부여된 사용자)** 및 **Password(비밀번호)** 필드에 Active Directory 서버의 사용자 로그인 및 로그오프 데이터를 쿼리할 권한이 있는 사용자 이름 및 비밀번호를 입력합니다.

프록시를 사용하여 인증하려면 정규화된 사용자 이름을 입력합니다.

기본적으로 에이전트가 설치된 컴퓨터에 로그인하는 데 사용한 어카운트의 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.

7단계 **Domain(도메인)** 필드에 Active Directory 도메인의 이름을 입력합니다.

8단계 Active Directory 서버에 대한 로그인을 탐지하려면 **Local Login IP Address(로컬 로그인 IP 주소)** 필드를 선택합니다. 에이전트에서는 이 필드가 **Server Name/IP Address(서버 이름/IP 주소)** 필드에 지정된 서버와 연결된 모든 IP 주소로 자동으로 채워집니다.

Server Name/IP Address(서버 이름/IP 주소) 필드가 비어 있거나 `localhost`가 입력되어 있는 경우 이 필드는 로컬 호스트와 연결된 모든 IP 주소로 채워집니다.

9단계 **Process real time events(실시간 이벤트 진행)**를 선택하여 사용자 에이전트가 이 Active Directory 서버에서 실시간으로 로그인 이벤트를 검색할 수 있도록 합니다.

10단계 **Add(추가)**를 클릭하여 새 서버를 추가하거나 **Save(저장)**를 클릭하여 기존 서버에 변경 사항을 저장합니다.

서버 연결 정의가 Active Directory 서버 목록에 표시됩니다. 둘 이상의 서버 연결이 구성된 경우 각 열 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 시 사용자 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 서버 구성, 2-3페이지 를 참조하십시오.

11단계 (선택 사항). 에이전트가 사용자 로그인 데이터에 대해 Active Directory 서버를 자동으로 폴링하는 간격을 변경하려면 **Active Directory Server Polling Interval(Active Directory 서버 폴링 간격)** 목록에서 시간을 선택합니다.

설정을 저장하고 나면 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 시작됩니다.

Active Directory 서버에 대한 실시간 이벤트 처리가 활성화되어 있으며 사용자 에이전트와 서버 간의 연결이 해제된 경우 에이전트는 응답을 받고 실시간 데이터 검색을 사용할 수 있을 때까지 지속적으로 폴링을 시도합니다. 연결이 설정되고 나면 실시간 데이터 검색이 다시 시작됩니다.

12단계 (선택 사항). 에이전트가 사용자 로그인 데이터에 대해 Active Directory 서버를 폴링하기 위한 연결을 처음 또는 다시 설정할 때, 폴링되는 최대 시간 범위를 변경하려면 **Active Directory Server Max Poll Length(Active Directory 서버 최대 폴링 시간)** 목록에서 시간을 선택합니다.

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

13단계 에이전트에 대한 컨피그레이션 변경 사항을 저장 및 적용하려면 **Save(저장)**를 클릭합니다.

14단계 다음과 같은 옵션이 있습니다.

- Management Center 연결을 추가하거나 제거하려면 **Firepower Management Centers** 탭을 선택합니다. 자세한 내용은 사용자 에이전트 Management Center 연결 구성, 2-24페이지를 참조하십시오.

  사용자 로그인과 로그오프 데이터를 보고하려면 에이전트에 하나 이상의 Management Center를 추가해야 합니다.
- 에이전트를 구성하려면 표 2-1, 2-20페이지에 설명된 작업 중 하나를 수행합니다.

사용자 에이전트 Management Center 연결 구성

라이선스: FireSIGHT 또는 해당 없음

사용자 에이전트에서 최대 5개의 Management Center에 Active Directory 사용자 데이터를 전송할 수 있습니다. 에이전트에서는 탭이 선택된 시점의 Management Center 상태(`available(사용 가능)`, `unavailable(사용 불가)`, 또는 에이전트를 처음 시작하는 경우 `unknown(알 수 없음)`)을 확인하고 에이전트가 보고한 마지막 로그인을 확인할 수 있습니다.

연결을 추가하기 전에 Management Center 컨피그레이션에 사용자 에이전트를 추가해야 합니다. 자세한 내용은 사용자 에이전트에 연결하도록 버전 5.x Defense Center 구성, 2-3페이지, 사용자 에이전트에 연결하도록 버전 5.x Defense Center 구성, 2-3페이지 또는 사용자 에이전트에 연결하도록 버전 6.x Management Center 구성, 2-3페이지를 참조하십시오.

참고 버전 5.x에서는 Management Center를 Defense Center라고 합니다.

고가용성 컨피그레이션에서는 에이전트에 기본 및 보조 Management Center를 모두 추가함으로써 사용자 로그인 및 로그오프 데이터 업데이트를 활성화하여 두 Management Center의 데이터가 모두 유지되도록 합니다.

Management Center 연결을 구성하는 방법:

액세스: 모두

1단계 필요한 경우 사용자 에이전트가 설치된 컴퓨터에 로그인합니다.

2단계 **Start(시작)** > **[All(모든)] Programs(프로그램)** > **Cisco** > **Configure Cisco Firepower Agent for Active Directory(Active Directory용 Cisco Firepower Agent 구성)**를 클릭합니다.

3단계 **Firepower Management Centers** 탭을 클릭합니다.

4단계 **Add(추가)**를 클릭합니다.

5단계 추가하려는 Management Center의 호스트 이름 또는 IP 주소를 입력합니다.

6단계 **Add(추가)**를 클릭합니다.

Management Center 연결 컨피그레이션이 추가됩니다. 호스트 이름 또는 IP 주소는 여러 번 추가할 수 없습니다. 호스트 이름 및 IP 주소로 Management Center를 추가해서는 안 됩니다. Management Center가 둘 이상의 네트워크 어댑터를 보유하고 있는 경우 서로 다른 IP 주소를 사용하여 이를 여러 번 추가해서는 안 됩니다.

둘 이상의 Management Center 연결이 구성된 경우에는 각 열 헤더를 클릭하여 **Host(호스트)**, **Status(상태)** 또는 **Last Reported(최종 보고)**에 따라 정렬할 수 있습니다.

참고 컨피그레이션 시 사용자 에이전트가 Management Center에 연결할 수 없는 경우 해당 Management Center를 추가할 수 없습니다. 에이전트에 Management Center에 대한 TCP/IP 액세스가 있는지 확인하십시오.

7단계 에이전트에 대한 컨피그레이션 변경 사항을 저장 및 적용하려면 **Save(저장)**를 클릭합니다. 업데이트된 설정이 에이전트에 적용됩니다.

8단계 다음과 같은 옵션이 있습니다.

- (선택 사항). 제외된 사용자 이름 목록에 사용자 이름을 추가하거나 제거하려면 **Excluded Usernames(제외된 사용자 이름)** 탭을 선택합니다. 자세한 내용은 사용자 이름이 제외된 사용자 에이전트 설정 구성, 2-25페이지를 참조하십시오.
- (선택 사항). 제외된 IP 주소 목록에 IP 주소를 추가하거나 제거하려면 **Excluded Addresses(제외된 주소)** 탭을 선택합니다. 자세한 내용은 주소가 제외된 사용자 에이전트 설정 구성, 2-26페이지를 참조하십시오.
- (선택 사항). 로그 메시지를 보고 로깅을 구성하려면 **Logs(로그)** 탭을 선택합니다. 자세한 내용은 사용자 에이전트 로깅 설정 구성, 2-27페이지를 참조하십시오.
- (선택 사항). 일반 에이전트 설정을 구성하려면 **General(일반)** 탭을 클릭합니다. 자세한 내용은 일반 사용자 에이전트 설정 구성, 2-29페이지를 참조하십시오.
- 에이전트를 구성하려면 표 2-1, 2-20페이지에 설명된 작업 중 하나를 수행합니다.

사용자 이름이 제외된 사용자 에이전트 설정 구성

라이선스: FireSIGHT 또는 해당 없음

로그인 또는 로그오프 이벤트에 대해 폴링할 때 제외할 사용자 이름을 최대 500개까지 정의할 수 있습니다. 에이전트는 제외된 사용자 이름의 로그인이나 로그오프 이벤트를 검색하는 경우 이 이벤트를 Management Center에 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 Management Center에 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 Management Center에 보고된 사용자를 제외하는 경우 호스트가 데이터베이스에서 삭제되지 않는 한 해당 사용자는 호스트에서 매핑 해제되지 않습니다.

예를 들어, Active Directory 서버와 별개인 컴퓨터에 사용자 에이전트를 설치한 경우 이 옵션을 사용하여 Management Center에 로그인하는 사용자 에이전트 사용자를 제외할 수 있습니다.

제외된 사용자 이름을 구성하는 방법:

액세스: 모두

1단계 필요한 경우 사용자 에이전트가 설치된 컴퓨터에 로그인합니다.

2단계 **Start(시작) > [All(모든)] Programs(프로그램) > Cisco > Configure Cisco Firepower Agent for Active Directory(Active Directory용 Cisco Firepower Agent 구성)**를 클릭합니다. **Excluded Usernames(제외된 사용자 이름)** 탭을 선택합니다.

3단계 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.

4단계 (선택 사항). **Domain(도메인)** 열에 사용자 이름과 연결된 도메인을 입력합니다.

행당 하나의 도메인만 정의할 수 있습니다. 도메인을 지정하지 않으면 모든 도메인의 사용자 이름이 제외됩니다.

5단계 추가 사용자 이름을 추가하려면 3 단계 및 4 단계단계를 반복합니다. 둘 이상의 제외된 사용자 이름이 구성된 경우 각 열 헤더를 클릭하여 **Username(사용자 이름)** 또는 **Domain(도메인)**에 따라 정렬할 수 있습니다.

6단계 행을 제거하려면, 다음 방법을 사용하십시오.

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

행이 제거됩니다.

여러 행을 제거하려면 Ctrl 키를 누른 상태에서 클릭하여 여러 행을 선택하고 Delete 키를 누릅니다.

7단계 쉼표로 구분된 값 파일에 사용자 이름 및 도메인 목록을 내보내려면 **Export List(목록 내보내기)**를 클릭합니다. 파일 경로를 선택하여 파일을 저장합니다.

파일이 저장됩니다. 기본적으로 파일 이름은 `Cisco_user_agent_excluded_users.csv`입니다.

8단계 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 파일은 업로드할 수 없습니다. 파일에 구문 오류가 있는 경우 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.

9단계 에이전트에 컨피그레이션 변경 사항을 저장 및 적용하려면 **Save(저장)**를 클릭합니다.

10단계 다음과 같은 옵션이 있습니다.

- 제외된 IP 주소 목록에 IP 주소를 추가하거나 제거하려면 **Excluded Addresses(제외된 주소)** 탭을 선택합니다. 자세한 내용은 주소가 제외된 사용자 에이전트 설정 구성, 2-26페이지를 참조하십시오.
- 에이전트를 구성하려면 표 2-1, 2-20페이지에 설명된 작업 중 하나를 수행합니다.

주소가 제외된 사용자 에이전트 설정 구성

라이선스: FireSIGHT 또는 해당 없음

로그인 이벤트에 대해 폴링할 때 제외할 IPv4 및 IPv6 주소를 최대 100개까지 구성할 수 있습니다. 사용자 에이전트는 제외된 IP 주소가 포함된 로그인 또는 로그오프 이벤트를 검색하는 경우 이 이벤트를 Management Center에 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 Management Center에 보고됩니다.

예를 들어, Active Directory 서버와 별개인 컴퓨터에 사용자 에이전트를 설치한 경우 이 옵션을 사용하여 Management Center에 로그인하는 사용자 에이전트 사용자를 제외할 수 있습니다.

제외된 IP 주소를 구성하는 방법:

액세스: 모두

1단계 필요한 경우 사용자 에이전트가 설치된 컴퓨터에 로그인합니다.

2단계 **Start(시작) > [All(모든)] Programs(프로그램) > Cisco > Configure Cisco Firepower Agent for Active Directory(Active Directory용 Cisco Firepower Agent 구성)**를 클릭합니다. **Excluded Addresses(제외된 주소)** 탭을 선택합니다.

3단계 사용 가능한 다음 행에 **Address(주소)** 열에서 제외할 IP 주소를 입력합니다. 추가 IP 주소를 추가하려면 이 단계를 반복합니다.

둘 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 표시됩니다. 잘못된 주소를 수정하지 않고 다른 주소를 입력할 수는 없습니다.

4단계 IP 주소를 제거하려면 해당 행을 강조 표시하고 Delete 키를 누릅니다.

IP 주소가 제거됩니다. 여러 행을 제거하려면 Ctrl 키를 누른 상태에서 클릭하여 여러 행을 선택하고 Delete 키를 누릅니다.

5단계 쉼표로 구분된 값 파일에 IP 주소 목록을 내보내려면 **Export List(목록 내보내기)**를 클릭합니다. 파일 경로를 선택하여 파일을 저장합니다.

파일이 저장됩니다. 기본적으로 파일 이름은 `Cisco_user_agent_excluded_addresses.csv`입니다.

6단계 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 파일은 업로드할 수 없습니다. 파일에 구문 오류가 있는 경우 해당 파일을 업로드할 수 없습니다.

7단계 에이전트에 컨피그레이션 변경 사항을 저장 및 적용하려면 **Save(저장)**를 클릭합니다.

8단계 다음과 같은 옵션이 있습니다.

- 로그 메시지를 보고 로깅을 구성하려면 **Logs(로그)** 탭을 선택합니다. 자세한 내용은 사용자 에이전트 로깅 설정 구성, 2-27페이지를 참조하십시오.
- 에이전트를 구성하려면 표 2-1, 2-20페이지에 설명된 작업 중 하나를 수행합니다.

사용자 에이전트 로깅 설정 구성

라이선스: FireSIGHT 또는 해당 없음

Logs(로그) 탭에서 에이전트별로 로깅된 최대 250개의 상태 메시지를 확인할 수 있습니다. 에이전트는 다음과 같은 이벤트가 발생하면 해당 이벤트에 대한 로컬 이벤트 로그에 상태 메시지를 로깅합니다.

- 에이전트가 Active Directory 서버에서 성공적으로 데이터를 폴링합니다.
- 에이전트가 Active Directory 서버에 연결하지 못합니다.
- 에이전트가 Active Directory 서버에서 데이터를 검색하지 못합니다.
- 에이전트가 Management Center에 성공적으로 연결합니다.
- 에이전트가 Management Center에 연결하지 못합니다.

에이전트는 타임스탬프 및 심각도 레벨이 포함된 각 상태 메시지를 로깅합니다. 다음 표에서는 심각도 레벨을 심각도 증가순으로 설명합니다.

표 2-3 사용자 에이전트 로깅 심각도 레벨

레벨	색	설명
Debug(디버그)	회색	이벤트가 디버깅 목적으로 로깅됩니다. 이러한 메시지는 기본적으로 표시되지 않습니다.
Information(정보)	녹색	이벤트가 정상적인 에이전트 작업과 일치합니다.
Warning(경고)	노란색	예상치 못한 이벤트지만 정상적인 에이전트 작업을 반드시 중단할 필요는 없습니다.
Error(오류)	빨간색	예상치 못한 이벤트이며 정상적인 에이전트 작업이 중단됩니다.

에이전트는 로컬 이벤트 로그 이외에도 Windows 애플리케이션 로그에 상태 메시지를 로깅할 수 있습니다. 또한, 에이전트는 로컬 이벤트 로그 내용을 쉼표로 구분된 값 파일로 내보낼 수 있습니다.

상태 메시지를 저장할 것인지를 비롯하여 저장 기간과 모든 상태 메시지의 이벤트 로그를 지울 것인지를 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 지워도 디버그 상태 메시지 스토리지는 영향을 받지 않습니다.

사용자 에이전트 로깅 설정을 구성하는 방법:

액세스: 모두

1단계 필요한 경우 사용자 에이전트가 설치된 컴퓨터에 로그인합니다.

2단계 **Start(시작)** > **[All(모든)] Programs(프로그램)** > **Cisco** > **Configure Cisco Firepower Agent for Active Directory(Active Directory용 Cisco Firepower Agent 구성)**를 클릭합니다.

3단계 **Logs(로그)** 탭을 클릭합니다.

4단계 Cisco TAC에서 안내하는 경우, **Show Debug Messages in Log(로그에 디버그 메시지 표시)**를 선택하여 이벤트 로그에서 디버그 상태 메시지를 확인하고 **Maintenance(유지 관리)** 탭 페이지를 활성화합니다.

참고 Cisco TAC에서 안내하는 경우에만 이 옵션을 선택합니다.

5단계 **Log Messages to Windows Application Log(Windows 애플리케이션 로그에 메시지 로깅)**를 선택하여 디버그 상태 메시지가 아닌 메시지를 Windows 애플리케이션 로그 및 로컬 이벤트 로그에 로깅합니다.

Windows 애플리케이션 로그를 보려면 Windows 이벤트 뷰어를 엽니다.

6단계 **Message Cache Size(메시지 캐시 크기)** 드롭다운 목록에서 기간을 선택하여 로컬 이벤트 로그에서 자동으로 삭제될 때까지 상태 메시지를 저장할 기간을 구성합니다.

상태 메시지가 일단 로컬 이벤트 로그에 로깅되면 **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 주며 Windows 애플리케이션 로그에는 영향을 주지 않습니다.

7단계 마지막 새로 고침 이후 로깅된 새로운 상태 메시지를 확인하려면 **Refresh(새로 고침)**를 클릭합니다.

마지막 새로 고침 후 새 상태 메시지가 로깅되면 새로운 상태 메시지가 있음을 알리는 메시지가 표시됩니다. 새로 고침 후 250개가 넘는 메시지가 표시되는 경우 가장 오래된 상태 메시지는 **Logs(로그)** 탭 페이지에서 제거됩니다. 250개가 넘는 메시지를 보려면 로그를 내보냅니다. 자세한 내용은 8 단계단계를 참조하십시오.

8단계 **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.

9단계 **Clear Event Log(이벤트 로그 지우기)**를 클릭하여 로컬 이벤트 로그에서 디버그 상태 메시지가 아닌 메시지를 모두 제거합니다.

에이전트가 메시지를 지웠음을 알리는 상태 메시지를 제외한 로컬 이벤트가 지워집니다.

10단계 에이전트에 대한 컨피그레이션 변경 사항을 저장 및 적용하려면 **Save(저장)**를 클릭합니다.

11단계 다음과 같은 옵션이 있습니다.

- 일반 에이전트 설정을 구성하려면 **General(일반)** 탭을 선택합니다. 자세한 내용은 일반 사용자 에이전트 설정 구성, 2-29페이지를 참조하십시오.
- 에이전트를 구성하려면 표 2-1, 2-20페이지에 설명된 작업 중 하나를 수행합니다.

일반 사용자 에이전트 설정 구성

라이선스: FireSIGHT 또는 해당 없음

General(일반) 탭에는 기본 사용자 에이전트 컨피그레이션이 포함되어 있습니다. 에이전트가 로그인 데이터를 보고할 때 Management Center에 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) > Cisco > Configure Cisco Firepower User Agent for Active Directory(Active Directory용 Cisco Firepower 사용자 에이전트 구성)**를 선택합니다.

2단계 에이전트 서비스를 시작하려면 시작( )을 클릭합니다.

3단계 에이전트 서비스를 중지하려면 중지( )를 클릭합니다.

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

5단계 (선택 사항). 로그오프 데이터에 대한 에이전트 확인 빈도를 변경하려면 **Logout Check Frequency(로그아웃 확인 빈도)** 목록에서 기간을 선택합니다. 로그오프 데이터 확인을 비활성화하려면 **0**을 선택합니다.

6단계 (선택 사항). 에이전트 일정의 우선순위를 변경하려면 **Priority(우선순위)** 목록에서 레벨을 선택합니다. 에이전트가 상당한 양의 사용자 활동을 모니터링하고 검색하며 이 작업이 성능에 영향을 주는 경우에만 `High(높음)`를 선택합니다.

7단계 설정을 저장하려면 **Save(저장)**를 클릭합니다.

8단계 에이전트를 구성하려면 표 2-1, 2-20페이지에 설명된 작업 중 하나를 수행합니다.

사용자 에이전트 유지 관리 설정 구성

라이선스: FireSIGHT 또는 해당 없음

컨피그레이션 설정 외에도 에이전트는 사용자-IP 주소 매핑 정보, 로컬 이벤트 로그, 보고 상태 정보를 SQL CE 데이터베이스에 저장합니다. 에이전트의 Maintenance(유지 관리) 탭을 이용하면 유지 관리 목적으로 데이터베이스 일부를 지울 수 있습니다. 캐시된 사용자-IP 주소 매핑 정보 및 로컬 이벤트 로그 정보를 지울 수 있습니다. 또한, 구성된 Active Directory 서버의 수동 폴링을 강제로 수행하는 보고 상태 캐시를 지울 수 있습니다.

주의 지원 팀에서 안내하지 않는 한 Maintenance(유지 관리) 탭 페이지의 어떠한 설정도 변경하지 *마십시오*.

사용자 에이전트 유지 관리 설정을 구성하는 방법:

액세스: 모두

1단계 에이전트를 설치한 컴퓨터에서, **Start(시작) > Programs(프로그램) > Cisco > Configure Cisco Firepower User Agent for Active Directory(Active Directory용 Cisco Firepower 사용자 에이전트 구성)**를 선택합니다.

2단계 **Logs(로그)** 탭을 클릭합니다.

3단계 **Show Debug Messages in Log(로그에 디버그 메시지 표시)**를 클릭하여 **Maintenance(유지 관리)** 탭을 활성화합니다.

4단계 **Maintenance(유지 관리)** 탭을 클릭합니다.

5단계 **Clear user mapping data cache(데이터 캐시를 매핑하는 사용자 지우기)**를 클릭하여 저장된 모든 사용자-IP 주소 매핑 데이터를 지웁니다.

에이전트는 로컬 에이전트 데이터베이스에서 저장된 모든 사용자-IP 주소 매핑 데이터를 삭제합니다. Management Center 데이터베이스에 저장된 사용자-IP 주소 매핑 데이터는 로컬 에이전트 데이터베이스를 지울 때 영향을 받지 않습니다.

6단계 **Clear logon event log cache(로그온 이벤트 로그 캐시 지우기)**를 클릭하여 저장된 모든 로그인 이벤트 데이터를 지웁니다.

7단계 **Clear reporting state cache(보고 상태 캐시 지우기)**를 클릭하여 에이전트가 구성된 Management Center에 마지막 로그인 및 로그오프 정보를 보고한 시점과 관련된 데이터를 지웁니다.

에이전트는 구성된 Management Center에 마지막 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 Active Directory 서버 연결 구성, 2-20페이지를 참조하십시오.

8단계 로깅된 디버그 메시지의 상세 레벨을 구성하려면 **Debug Log Level(디버그 로그 레벨)** 드롭다운에서 로깅 세분화 레벨을 선택합니다.

9단계 에이전트를 구성하려면 표 2-1, 2-20페이지에 설명된 작업 중 하나를 수행합니다.

사용자 에이전트 트러블슈팅

다음 섹션에서는 사용자 에이전트 사용 시 발생할 수 있는 문제의 해결책에 대해 설명합니다.

Management Center에 연결할 수 없음

사용자 에이전트의 **Firepower Management Centers** 탭 페이지에서 Management Center의 상태가 `unavailable(사용 불가)`인 경우 Management Center에서 ID 소스로 사용자 에이전트를 추가했는지 확인합니다. 사용자 에이전트 컨피그레이션에 대한 자세한 내용은 *환경 설정 가이드*를 참조하십시오.

버전 6.X Management Center에서 사용자 에이전트 ID 소스를 확인하는 방법:

1단계 관리자로 Management Center에 로그인합니다.

2단계 **System(시스템)** > **Integration(통합)**을 클릭합니다.

3단계 **Identity Sources(ID 소스)** 탭을 클릭합니다.

4단계 **User Agent(사용자 에이전트)**를 클릭합니다.

5단계 사용자 에이전트가 정의되어 있는지 확인하고 IP 주소를 확인합니다. 변경한 사항이 있으면 **Save(저장)**를 클릭합니다.

6단계 사용자 에이전트의 **Firepower Management Centers** 탭 페이지에서 Management Center의 상태를 다시 확인합니다.

Management Center를 올바르게 구성했는데 여전히 연결할 수 없는 경우 다음 작업을 시도합니다.

- 사용자 에이전트에서 구성한 Management Center의 호스트 이름 또는 IP 주소를 더블 클릭합니다.
- 호스트 이름을 사용하여 Management Center에 액세스하는 경우 `nslookup` *`hostname`* 명령을 사용하여 호스트 이름이 IP 주소로 확인되는지 확인합니다.
- IP 주소를 사용하여 Management Center에 액세스하는 경우 `ping` *`ip-address`* 명령을 사용하여 사용자 에이전트 컴퓨터에 액세스 가능한지 확인합니다.

사용자 에이전트 응답 없음

사용자 에이전트에서 데이터를 가져오지 않고 있다고 의심되는 경우 다음 작업을 수행할 수 있습니다.

- 사용자 에이전트 컴퓨터에 로그인하여 상태를 확인합니다. 자세한 내용은 일반 사용자 에이전트 설정 구성, 2-29페이지를 참조하십시오.
- 다음 절차에 설명된 대로 Management Center에서 상태를 모니터링하도록 사용자 에이전트 상태 정책을 설정합니다.

  사용자 에이전트 상태 정책을 설정하면 Management Center가 사용자 에이전트에서 하트비트를 수신하지 않는 경우 이를 알 수 있습니다. 자세한 내용은 환경 설정 가이드를 참조하십시오.

6.X Management Center에서 사용자 에이전트 상태 정책을 설정하는 방법:

1단계 관리자 또는 유지 관리 사용자 권한이 있는 사용자로 Management Center에 로그인합니다.

2단계 **System(시스템) > Health(상태) > Policy(정책)**를 클릭합니다.

3단계 **Create Policy(정책 생성)**를 클릭합니다.

4단계 Create Policy(정책 생성) 페이지에서 다음 정보를 입력합니다.

- **Copy Policy(정책 복사)** 목록: **Default Health Policy(기본 상태 정책)** 같은 정책을 선택합니다.
- **New Policy Name(새 정책 이름)** 필드: 이 정책을 식별하는 이름을 입력합니다.
- **New Policy Description(새 정책 설명)** 필드: 정책 설명을 입력합니다(선택 사항).

새 정책이 표시됩니다.

5단계 (편집) 아이콘을 클릭합니다.

6단계 왼쪽 열에서 **User Agent Status Monitor(사용자 에이전트 상태 모니터링)**를 클릭합니다.

7단계 오른쪽 열에서 **On(켜짐)**을 클릭합니다.

8단계 페이지 하단에서 **Save Policy and Exit(정책 저장 및 종료)**을 클릭합니다.

9단계 정책 이름 옆의 (적용) 아이콘을 클릭합니다.

10단계 화면에 표시되는 프롬프트에 따라 관리되는 디바이스에 정책을 적용합니다.

11단계 언제든지 사용자 에이전트를 모니터링하려면 **Health(상태) > Monitor(모니터링)**를 클릭하거나 Management Center의 (모니터링) 아이콘을 통해 메시지를 확인합니다.

사용자 에이전트 하트비트가 관리되는 디바이스에서 탐지되지 않는 경우 다음과 유사한 메시지가 표시됩니다.

```
Some user agents are not up-to-date(일부 사용자 에이전트가 최신 상태가 아님)
```

사용자 에이전트가 모든 로그인을 표시하지는 않음

사용자 에이전트는 IP 주소별로 사용자 이름을 추적합니다. 동일한 사용자가 동일한 IP 주소에 여러 번 로그인하는 경우 해당 사용자에 대한 Management Center의 User Login(사용자 로그인) 이벤트를 하나만 확인할 수 있습니다.

다음 시나리오에서는 사용자에 대한 여러 사용자 로그인 이벤트를 볼 수 있습니다.

- 사용자가 다른 IP 주소(예: 데스크톱 및 휴대전화)에서 로그인합니다.
- 사용자 patricia.nolan이 이 순서로 다음 IP 주소에서 로그인합니다.
  - 192.0.2.102
  - 192.0.2.210
  - 192.0.2.102

patricia.nolan이 IP 주소에서 로그아웃하는지와 관계없이 Management Center는 최소 2번(각 고유한 IP 주소에 대해 한 번씩)의 사용자 로그인 이벤트를 보고합니다. 즉, 처음과 동일한 IP 주소에서 로그인했으므로 Management Center는 마지막 로그인을 보고하지 않습니다.

사용자 에이전트가 실시간 이벤트를 처리하지 않음

Active Directory 서버에서 실시간 이벤트를 처리할 수 있으려면 사용자 에이전트에 Active Directory 서버에 대한 RPC(Remote Procedure Call) 액세스가 필요합니다. 실시간 처리 상태가 사용자 에이전트의 **Active Directory Servers(Active Directory 서버)** 탭 페이지에 unknown(알 수 없음) 또는 unavailable(사용 불가)로 오래 표시되는 경우 사용자 에이전트 로그에서 오류를 확인하고 이 섹션에서 설명된 다른 제안 사항을 시도합니다.

실시간 처리 문제 해결 방법:

1단계 필요한 경우 사용자 에이전트가 설치된 컴퓨터에 로그인합니다.

2단계 **Start(시작) > Programs(프로그램) > Cisco > Configure Cisco Firepower User Agent for Active Directory(Active Directory용 Cisco Firepower User Agent 구성)**를 클릭합니다.

3단계 **Logs(로그)** 탭을 클릭합니다.

4단계 **Show debug messages in log(로그에 디버그 메시지 표시)**를 선택합니다.

5단계 로그 메시지를 확인하거나 **Export logs(로그 내보내기)**를 클릭하여 로그 메시지를 파일로 내보냅니다.

6단계 다음과 같은 메시지를 확인합니다.

"error","[2317] - Unable to attach event listener to *host or IP address*. Check firewall settings on AD server. RPC server is unavailable("오류","[2317] - 호스트 또는 IP 주소에 이벤트 수신기를 연결할 수 없습니다. AD 서버에서 방화벽 설정을 확인하십시오. RPC 서버를 사용할 수 없습니다.)

위 메시지는 Active Directory 서버의 방화벽 컨피그레이션 문제를 나타냅니다. 사용자 에이전트가 DCOM(Distributed Component Object Management)에 액세스하도록 허용, 2-12페이지의 지침을 검토하고 다시 시도합니다.

방화벽에서 문제를 분리하려면 경우에 따라 Active Directory 서버의 방화벽을 몇 분 동안 비활성화한 다음 사용자 에이전트가 실시간 이벤트를 처리할 수 있는지 확인합니다.

7단계 사용자 에이전트에서 Active Directory 서버 컨피그레이션을 삭제하고 다시 추가해 봅니다.

사용자 에이전트가 사용자 로그오프 이벤트를 표시하지 않음

Management Center에서 User Logoff(사용자 로그오프) 이벤트를 볼 수 없는 경우 모든 도메인 컴퓨터에서 방화벽을 통해 WMI를 허용해야 합니다. 자세한 내용은 도메인 컴퓨터 구성, 2-6페이지를 참조하십시오.