# RDP를 사용하여 원격 데스크톱에 로그인하면 IP 주소와 연결된 사용자가 변경됩니다

## 목차

[소개](#)
[사전 요구 사항](#)
[근본 원인](#)
[확인](#)
[솔루션](#)

## 소개

RDP(Remote Desktop Protocol)를 사용하여 원격 호스트에 로그인하는 경우, 원격 사용자 이름이 사용자와 다를 경우 FireSIGHT System에서 FireSIGHT Management Center의 IP 주소와 연결된 사용자의 IP 주소를 변경합니다. 액세스 제어 규칙과 관련하여 사용자의 권한이 변경됩니다. You will notice눈치 that i잘못된 사용자가 워크스테이션에 연결되어 있습니다. 이 문서에서는 이 문제에 대한 해결책을 제공합니다.

## 사전 요구 사항

FireSIGHT System 및 User Agent에 대한 지식이 있는 것이 좋습니다.

> **참고**: 이 문서의 정보는 특정 랩 환경의 디바이스에서 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 근본 원인

이 문제는 Microsoft AD(Active Directory)가 도메인 컨트롤러의 Windows 보안 로그에 RDP 인증 시도를 기록하는 방식 때문에 발생합니다. AD는 연결 중인 RDP 엔드포인트가 아닌 원래 호스트 IP 주소에 대해 RDP 세션에 대한 인증 시도를 기록합니다. 다른 사용자 계정으로 원격 호스트에 로그인하면 원래 워크스테이션의 IP 주소와 연결된 사용자가 변경됩니다.

# 확인

이러한 상황이 발생하는지 확인하려면 원래 워크스테이션의 로그온 이벤트의 IP 주소와 RDP 원격 호스트의 IP 주소가 동일한지 확인할 수 있습니다.

이러한 이벤트를 찾으려면 다음 단계를 따라야 합니다.

1단계: 호스트에서 인증하고 있는 도메인 컨트롤러를 확인합니다.

다음 명령을 실행합니다.

```
nltest /dsgetdc:<windows.domain.name>
```

출력 예:

```
C:\Users\WinXP.LAB>nltest /dsgetdc:support.lab
DC: \\Win2k8.support.lab
Address: \\192.X.X.X
Dom Guid: XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX
Dom Name: support.lab
Forest Name: support.lab
Dc Site Name: Default-First-Site-Name
Our Site Name: Default-First-Site-Name
Flags: PDC GC DS LDAP KDC TIMESERV WRITABLE DNS_DC DNS_DOMAIN DNS_FOREST
CLOSE_SITE FULL_SECRET WS 0x4000
The command completed successfully
```

"DC:"을 시작하는 줄은 도메인 컨트롤러의 이름이 되며 "Address:"을 시작하는 줄은 IP 주소가 됩니다.

2단계: 1단계에서 식별된 도메인 컨트롤러에 RDP 로그 사용

3단계: **Start(시작) > Administrative Tools(관리 툴) > Event Viewer(이벤트 뷰어)로 이동합니다**.

4단계: **Windows 로그 > 보안**으로 **드릴다운합니다**.

5단계: Filter Current Log(현재 로그 필터링)를 클릭하고 XML 탭을 클릭한 다음 edit query(쿼리 수정)를 클릭하여 워크스테이션의 IP 주소를 필터링합니다.

6단계: IP 주소를 <ip address>로 대체하여 다음 XML 쿼리를 입력합니다.

```
<QueryList>
<Query Id="0" Path="Security">
<Select Path="Security">
*[EventData[Data[@Name='IpAddress'] and(Data='<IP address>')]]
</Select>
</Query>
</QueryList>
```

7단계: Logon Event(로그온 **이벤트)**를 클릭하고 Details(**세부사항) 탭**을 클릭합니다.

출력의 예:

```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>
<Provider Name="Microsoft-Windows-Security-Auditing"
Guid="{XXXXXXXX-XXX-XXXX-XXX-XXXXXXXXXXXX}"/>
<EventID>4624</EventID>
<Version>0</Version>
<Level>0</Level>
<Task>12544</Task>
<Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords>
<TimeCreated SystemTime="2014-07-22T20:35:12.750Z" />
<EventRecordID>4130857</EventRecordID>
<Correlation />
<Execution ProcessID="576" ThreadID="704" />
<Channel>Security</Channel>
<Computer>WIN2k8.Support.lab</Computer>
<Security />
</System>
- <EventData>
<Data Name="SubjectUserSid">S-1-0-0</Data>
<Data Name="SubjectUserName">-</Data>
<Data Name="SubjectDomainName">-</Data>
<Data Name="SubjectLogonId">0x0</Data>
<Data Name="TargetUserSid">S-X-X-XX-XXXXXXXXXX-XXXXXXXXXX-XXXXXXXXX-XXXX</Data>
<Data Name="TargetUserName">WINXP-SUPLAB$</Data>
<Data Name="TargetDomainName">SUPPORT</Data>
<Data Name="TargetLogonId">0x13c4101f</Data>
<Data Name="LogonType">3</Data>
<Data Name="LogonProcessName">Kerberos</Data>
<Data Name="AuthenticationPackageName">Kerberos</Data>
<Data Name="WorkstationName" />
<Data Name="LogonGuid">{XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX}</Data>
<Data Name="TransmittedServices">-</Data>
<Data Name="LmPackageName">-</Data>
<Data Name="KeyLength">0</Data>
<Data Name="ProcessId">0x0</Data>
<Data Name="ProcessName">-</Data>
<Data Name="IpAddress">192.0.2.10</Data>
<Data Name="IpPort">2401</Data>
</EventData>
```

RDP를 통해 로그인한 후 동일한 단계를 완료하면 원래 로그온의 로그온 이벤트 XML 데이터에서 다음 줄에 표시된 것과 같은 IP 주소로 다른 로그온 이벤트(이벤트 ID 4624)를 받게 됩니다.

```
<Data Name="IpAddress">192.x.x.x</Data>
```

# 솔루션

사용자 에이전트 2.1 이상을 사용 중인 경우 이 문제를 완화하기 위해 모든 계정을 제외할 수 있습니다
사용자 에이전트 컨피그레이션의 RDP에 주로 사용됩니다.

1단계: User Agent Host에 로그인합니다.

2단계: User Agent 사용자 인터페이스를 시작합니다.

3단계: Excluded Usernames(제외된 사용자 이름) **탭을** 클릭합니다.

4단계: 제외할 모든 사용자 이름을 입력합니다.

5단계: Save(**저장**)를 **클릭합니다**.

이 목록에 입력한 사용자는 FireSIGHT Management Center에서 로그온 이벤트를 생성하지 않으며 IP 주소에 연결됩니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.