



## TS 에이전트로 사용자 제어

TS 에이전트를 사용자 인식 및 사용자 제어를 위한 ID 소스로 사용하려면, [Cisco TS\(Terminal Services\) Agent 가이드](#)의 설명에 따라 TS 에이전트 소프트웨어를 설치하고 설정합니다.

다음 작업:

- [ID 정책 생성](#)에 설명된 대로 ID 정책을 사용하여 제어할 사용자 및 기타 옵션을 지정합니다.
- [액세스 제어에 다른 정책 연결](#)에 설명된 대로 ID 규칙을 트래픽을 필터링하고 필요에 따라 검사하는 액세스 제어 규칙과 연결합니다.
- [구성 변경 사항 구축](#)에 설명된 대로 관리되는 디바이스에 ID 및 액세스 제어 정책을 구축합니다.
- [Cisco Secure Firewall Management Center 관리 가이드](#)의 워크플로우 사용에 설명된 대로 사용자 활동을 모니터링합니다.
- [TS\(Terminal Services\) 에이전트 ID 소스, 1 페이지](#)
- [TS 에이전트 가이드라인, 2 페이지](#)
- [TS 에이전트로 사용자 제어, 2 페이지](#)
- [TS 에이전트 ID 소스 문제 해결, 2 페이지](#)
- [TS 에이전트 기록, 3 페이지](#)

## TS(Terminal Services) 에이전트 ID 소스

TS 에이전트는 패시브 인증 방법이 시스템에서 지원되는 권한 있는 ID 소스 중 하나입니다. Windows 터미널 서버가 인증을 수행하면, TS 에이전트는 독립형 또는 고가용성 management center에 이를 보고합니다.

Windows 터미널 서버에 설치된 경우, TS 에이전트는 개별 사용자가 모니터링되는 네트워크에 로그인 또는 로그아웃할 때 개별 사용자에게 고유의 포트 범위를 할당합니다. management center는 고유한 포트를 사용하여 시스템에서 개별 사용자를 식별합니다. TS 에이전트 1개를 사용하여 Windows 터미널 서버 1개에서 사용자 활동을 모니터링하고, 암호화된 데이터를 management center에 보낼 수 있습니다.

TS 에이전트는 실패한 로그인 시도를 보고하지 않습니다. TS 에이전트에서 수집한 데이터는 사용자 인식 및 사용자 제어에 사용할 수 있습니다.

## TS 에이전트 가이드라인

TS 에이전트는 다단계 컨피그레이션이 필요하며 다음이 포함됩니다.

1. TS 에이전트가 설치 및 구성된 Windows 터미널 서버
2. 서버에서 모니터링 중인 사용자를 대상으로 하는 하나 이상의 ID 영역

Microsoft Windows 터미널 서버에 TS 에이전트를 설치합니다. 다단계 TS 에이전트 설치 및 구성에 대한 자세한 내용과 서버 및 Firepower System 요건의 전체 내용을 보려면 [Cisco TS\(Terminal Services\) Agent 가이드](#)의 내용을 참조하십시오.

TS 에이전트 데이터는 Users(사용자), User Activity(사용자 활동), Connection Event(연결 이벤트) 테이블에 표시되며 사용자 인식 및 사용자 제어에 사용할 수 있습니다.



참고 TS 에이전트가 동일한 사용자를 다른 패시브 인증 ID 소스(ISE/ISE-PIC)로 모니터링할 경우, management center는 TS 에이전트 데이터에 우선순위를 둡니다. TS 에이전트 및 다른 수동 ID 소스가 동일한 IP 주소별로 활동을 보고할 경우, TS 에이전트 데이터만 management center에 로깅됩니다.

## TS 에이전트로 사용자 제어

TS 에이전트를 사용자 인식 및 사용자 제어를 위한 ID 소스로 사용하려면, [Cisco TS\(Terminal Services\) Agent 가이드](#)의 설명에 따라 TS 에이전트 소프트웨어를 설치하고 설정합니다.

다음 작업:

- ID 정책 생성에 설명된 대로 ID 정책을 사용하여 제어할 사용자 및 기타 옵션을 지정합니다.
- 액세스 제어에 다른 정책 연결에 설명된 대로 ID 규칙을 트래픽을 필터링하고 필요에 따라 검사하는 액세스 제어 규칙과 연결합니다.
- 구성 변경 사항 구축에 설명된 대로 관리되는 디바이스에 ID 및 액세스 제어 정책을 구축합니다.
- Cisco Secure Firewall Management Center 관리 가이드의 워크플로우 사용에 설명된 대로 사용자 활동을 모니터링합니다.

## TS 에이전트 ID 소스 문제 해결

기타 관련 문제 해결 정보를 보려면 [영역 및 사용자 다운로드 문제 해결](#) 및 [사용자 제어 문제 해결](#)을 참조하십시오.

TS 에이전트 통합을 사용하는 데 문제가 발생한 경우 다음을 확인하십시오.

- TS 에이전트 서버의 시간을 management center의 시간과 동기화해야 합니다.

- TS 에이전트가 동일한 사용자를 다른 패시브 인증 ID 소스(ISE/ISE-PIC)로 모니터링할 경우, management center는 TS 에이전트 데이터에 우선순위를 둡니다. TS 에이전트 및 수동 ID 소스가 동일한 IP 주소별로 활동을 보고할 경우, TS 에이전트 데이터만 management center에 로깅됩니다.
- 활성 FTP 세션이 이벤트에서 **Unknown**사용자로 표시됩니다. 활성 FTP에서는 서버(클라이언트 아님)가 연결을 시작하고 FTP 서버에는 관련 사용자 이름이 없으므로 이는 정상입니다. 활성 FTP에 대한 자세한 내용은 [RFC 959](#)를 참조하십시오.

자세한 문제 해결 정보는 [Cisco TS\(Terminal Services\) Agent 가이드](#)의 내용을 참조하십시오.

## TS 에이전트 기록

기능	버전	세부 사항
사용자 제어에 대한 TS 에이전트입니다.	6.2.0	<p>기능이 도입되었습니다. Firepower는 이제 Citrix의 VDI(Virtual Desktop Infrastructure) 같은 공유 환경에서 개별 사용자를 더 잘 식별함으로써, 방화벽에서 사용자 기반 정책 규칙을 정확하게 실행하는 기능을 제공합니다. 사용자는 사용한 포트를 기준으로 식별됩니다.</p> <p>TS 에이전트 소프트웨어는 Firepower Management Center와는 별개로 업데이트됩니다. 자세한 내용은 다음 링크를 참조하십시오.</p> <ul style="list-style-type: none"> <li>• <a href="#">cisco.com</a>에서 확인할 수 있는 <i>Cisco TS(Terminal Services) 에이전트 가이드</i></li> <li>• <a href="#">Cisco FirePOWER 호환성 가이드</a></li> </ul>



## 번역에 관하여

Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.