



## TS 에이전트 설치 및 구성

- TS 에이전트 설치 또는 업그레이드, 1 페이지
- TS 에이전트 구성 인터페이스 시작, 2 페이지
- 프록시 설정, 2 페이지
- API 토큰 가져오기, 3 페이지
- TS 에이전트 구성, 4 페이지
- REST VDI 역할 생성, 10 페이지

## TS 에이전트 설치 또는 업그레이드

시작하기 전에

- 서버 및 시스템 환경 요구 사항에 설명된 대로 환경에서 TS 에이전트가 지원되는지 확인합니다.
- 현재 사용자 세션 종료에 설명된 대로 모든 현재 사용자 세션을 종료합니다.

단계 1 관리자 권한을 가진 사용자로 서버에 로그인합니다.

단계 2 지원 사이트 ([TSAgent-1.4.1.exe](#))에서 TS 에이전트 패키지를 다운로드합니다.

참고 사이트에서 업데이트를 직접 다운로드합니다. 파일을 이메일로 전송하는 경우 손상될 수 있습니다.

단계 3 TSAgent-1.4.1.exe를 마우스 오른쪽 버튼으로 클릭하고 **Run as Administrator**(관리자 권한으로 실행)를 선택합니다.

단계 4 **Install**(설치)을 클릭하고 프롬프트에 따라 TS 에이전트를 설치 또는 업그레이드합니다.

다음에 수행할 작업

- TS 에이전트 서비스 구성 요소의 상태 보기에 설명된 대로 TS 에이전트가 실행 중인지 확인합니다.
- TS 에이전트 프로세스 시작 및 중지 설명된 대로 TS 에이전트를 시작합니다.

- [TS 에이전트 구성, 4 페이지](#)에 설명된 대로 TS 에이전트를 구성합니다.

이전 TS 에이전트 버전에서 업그레이드하고 Citrix Provisioning을 사용하는 경우, 업그레이드 후 **Reserve Port(s)**(포트 예약) 필드에 **6910**을 입력해야 합니다.



참고 TS 에이전트 설치 프로그램에서 .NET Framework가 실패했다고 보고하면 Windows 업데이트를 실행하고 TS 에이전트 설치를 다시 시도하십시오.

## TS 에이전트 구성 인터페이스 시작

바탕 화면에 TS 에이전트 바로 가기가 있으면 바로 가기를 더블 클릭합니다. 없으면 다음 절차를 사용하여 TS 에이전트 구성 인터페이스를 시작합니다.

단계 1 관리자 권한을 가진 사용자로 서버에 로그인합니다.

단계 2 C:\Program Files (x86)\Cisco\Terminal Services Agent를 엽니다.

단계 3 TS 에이전트용 프로그램 파일을 확인합니다.

참고 프로그램 파일은 보기 전용입니다. 이러한 파일을 삭제, 이동 또는 수정하지 마십시오.

단계 4 TSAgentApp 파일을 더블 클릭하여 TS 에이전트를 시작합니다.

## 프록시 설정

클라우드 사용 Firewall Management Center에서 TS 에이전트가 설치된 시스템과 통신할 수 없는 경우, HTTPS 프로토콜이 활성화된 프록시를 사용해야 합니다.

이를 수행하는 방법은 사용자에게 달려 있습니다. 예를 들어 상업용 프록시가 있고 HTTPS가 활성화된 Windows 시스템 프록시를 사용하여 통신할 수 있습니다.



참고 온프레미스 Firewall Management Center를 TS 에이전트와 함께 사용하거나 CDO를 아예 사용하지 않는 경우에는 이 작업이 필요하지 않습니다.

## 애플리케이션 프록시 설정

이 작업은 TS 에이전트가 실행 중인 Windows Server에서 프록시를 구성하기 위한 한 가지 옵션을 제안합니다. Cisco는 이 절차가 사용자의 상황에서 효과가 있으리라 보장하지 않습니다. 자세한 내용은 프록시 제공자와 논의하거나 [Windows 설명서](#)를 참조하십시오.

시작하기 전에

프록시 서버는 이미 설정되어 있어야 합니다. 자세한 내용은 이 문서에서 다루지 않습니다.

단계 1 Windows Server에 관리자로 로그인합니다.

단계 2 관리자로 텍스트 편집기에서 다음 파일을 엽니다.

```
\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config
```

단계 3 <system.net> 섹션의 machine.config에 다음을 붙여넣습니다. 샘플 IP 주소 및 포트를 프록시 서버의 IP 주소 및 포트로 교체합니다.

```
<!-- Configuration for TS Agent -->
<system.net>
  <defaultProxy>
    <proxy autoDetect="false" bypassonlocal="false" proxyaddress="http://192.0.2.197:3128"
usesystemdefault="false" />
  </defaultProxy>
</system.net>
<!-- Configuration for TS Agent -->
```

단계 4 machine.config에 대한 변경 사항을 저장하고 텍스트 편집기를 종료합니다.

단계 5 변경 사항을 적용하려면 서버를 다시 시작합니다.

다음에 수행할 작업

[API 토큰 가져오기, 3 페이지](#)의 내용을 참조하십시오.

## API 토큰 가져오기

이 작업에서는 TS 에이전트가 Cisco Defense Orchestrator를 통해 인증하는 데 사용하는 API 토큰을 가져오는 방법을 설명합니다.

필수 역할:

- 슈퍼 관리자
- Admin(관리자)
- API 전용이 활성화된 구축 전용(또는 그 이상)



참고 이 작업은 클라우드 사용 Firewall Management Center에만 적용됩니다.

온프레미스 Firewall Management Center를 사용하는 경우 [REST VDI 역할 생성, 10 페이지](#)의 내용을 참조하십시오.


단계 1 다음 역할 중 하나가 있는 사용자로 CDO에 로그인합니다.

- 슈퍼 관리자: 선택적 TS 에이전트 사용자를 생성하거나 API 토큰을 직접 가져옵니다.
- 관리 또는 API 전용이 활성화된 구축 전용: API 토큰을 직접 가져옵니다.

단계 2 (슈퍼 관리자 사용자에게만 해당하는 선택 사항입니다.) 구축 전용 이상의 역할을 가진 TS 에이전트의 사용자를 생성하고 **API Only(API 전용)**를 선택합니다.

단계 3 오른쪽 상단에서 로그인 이름을 클릭한 다음 **Settings(설정)**를 클릭합니다.

단계 4 General Settings(일반 설정) 행에서 **Generate API Token(API 토큰 생성)**을 클릭합니다.

단계 5  을 클릭하여 토큰을 클립보드에 복사합니다.

다음에 수행할 작업

[TS 에이전트 구성, 4 페이지](#)에 설명된 대로 TS 에이전트를 구성합니다.

## TS 에이전트 구성

TS 에이전트 인터페이스를 사용하여 TS 에이전트를 구성합니다. 변경 사항을 저장하고 서버를 재부팅해야 변경 사항이 적용됩니다.

시작하기 전에

- 클라우드 사용 Firewall Management Center 또는 온프레미스 Firewall Management CenterFMC에 연결 중인 경우 [Cisco Secure Firewall Management Center 디바이스 구성 가이드](#)에 설명된 대로 서버가 모니터링하는 사용자를 대상으로 하나 이상의 Active Directory 영역을 구성하고 활성화합니다.
- Firepower System에 연결하는 경우 REST VDI 권한이 있는 사용자 계정을 구성합니다.  
[REST VDI 역할 생성, 10 페이지](#)에서 설명한 대로 Firepower Management Center에서 REST VDI 역할을 생성해야 합니다.
- 이미 클라우드 사용 Firewall Management Center 또는 온프레미스 Firewall Management CenterFMC에 연결되어 있고 다른 클라우드 사용 Firewall Management Center 또는 온프레미스 Firewall Management CenterFMC에 연결하도록 TS 에이전트 구성을 업데이트하는 경우, 새 구성을 저장하기 전에 모든 현재 사용자 세션을 종료해야 합니다. 자세한 내용은 [현재 사용자 세션 종료](#)의 내용을 참고하십시오.
- TS 에이전트 서버의 시간을 클라우드 사용 Firewall Management Center 또는 온프레미스 Firewall Management CenterFMC의 시간과 동기화해야 합니다.
  - 클라우드 사용 Firewall Management Center만 해당:
    - [API 토큰 가져오기, 3 페이지](#)에 설명된 대로 API 토큰 가져오기

- TS 에이전트 구성 필드, 5 페이지에 설명된 대로 구성 필드를 검토하고 이해합니다.

- 단계 1 TS 에이전트를 설치한 서버에서 TS 에이전트 구성 인터페이스 시작, 2 페이지에 설명된 대로 TS 에이전트를 시작합니다.
- 단계 2 **Configure**(구성) 탭을 클릭합니다.
- 단계 3 클라우드 사용 Firewall Management Center만 해당: 페이지 하단의 **Cloud**(클라우드) 탭을 클릭합니다.
- 단계 4 온프레미스 Firewall Management Center만 해당: 페이지 하단의 **On-Prem**(온프레미스) 탭을 클릭합니다.
- 단계 5 TS 에이전트 구성 필드, 5 페이지의 내용을 참조하십시오.
- 단계 6 TS 에이전트를 구성한 후 **Test**(테스트)를 클릭하여 TS 에이전트와 시스템 간의 REST API 연결을 테스트합니다.
- 단계 7 **Save**(저장)를 클릭하고 서버를 재부팅할지 확인합니다.

## TS 에이전트 구성 필드

다음 필드는 TS 에이전트의 설정을 구성하는 데 사용됩니다.

### 일반 설정

표 1: 일반 설정 필드

필드	설명
Max User Sessions(최대 사용자 세션 수)	<p>TS 에이전트에서 모니터링할 최대 사용자 세션 수입니다. 단일 사용자 세션을 실행할 수 있습니다.</p> <p>이 TS 에이전트 버전은 기본적으로 29개의 사용자 세션을 지원하며, 최대 255로 늘릴 수 있습니다.</p>
Server NIC(서버 NIC)	<p>TS 에이전트는 포트 변환 및 서버-시스템 통신에 단일 NIC(Network Interface Card) 사용을 지원합니다. 서버에 유효한 NIC가 두 개 이상 있으면 TS 에이전트가 지정된 주소에 대해서만 포트 변환을 수행합니다.</p> <p>TS 에이전트는 TS 에이전트가 설치된 서버에 있는 각 NIC의 IPv4 주소를 이 필드에 자동으로 채웁니다. 유효한 NIC에는 단일 IPv4 또는 IPv6 유형 중 하나가 있어야 합니다. 유효한 NIC는 동일한 유형의 여러 주소가 있을 수 있습니다.</p> <p>참고 서버의 IP 주소가 변경된 경우 변경 사항을 적용하려면 구성을 저장하고 서버를 재부팅하라는 메시지가 표시됩니다.</p> <p>참고 서버에 연결된 모든 디바이스에서 라우터 알림 메시지를 비활성화합니다. 라우터 알림이 활성화된 경우 디바이스에서 서버의 NIC 주소를 할당하고 TS 에이전트에 사용할 NIC를 무효화할 수 있습니다.</p>

필드	설명
System Ports(시스템 포트)	<p>시스템 프로세스에 사용하는 포트 범위입니다. TS 에이전트는 이 활동을 시작할 위치를 나타내는 <b>Start(시작)</b> 포트를 구성합니다. 각 개별 시스템 프로세스에 대해 지정할 포트 수를 나타내는 <b>Range(범위)</b> 값을 구성합니다.</p> <p>Cisco에서는 <b>Range(범위)</b> 값을 5000 이상으로 권장합니다. TS 에이전트에서 프로세스에 대한 포트가 자주 부족한 경우 <b>Range(범위)</b> 값을 늘리십시오.</p> <p>참고 시스템 프로세스에서 지정된 <b>System Ports(시스템 포트)</b> 외부에 포트가 필요한 경우, <b>Exclude Port(s)</b>(포트 제외) 필드에 포트를 추가합니다. <b>System Ports(시스템 포트)</b> 범위의 시스템 프로세스에서 사용되는 포트를 식별하지 않거나 제외할 경우, 시스템 프로세스가 실패할 수 있습니다.</p> <p>TS 에이전트는 다음 공식을 사용하여 <b>End(종료)</b> 값을 자동으로 채웁니다.</p> $([Start\ value] + [Range\ value]) - 1$ <p>항목의 <b>End(종료)</b> 값이 <b>User Ports(사용자 포트)</b>의 <b>Start(시작)</b> 값을 초과하면 <b>Start(시작)</b> 및 <b>Range(범위)</b> 값을 조정해야 합니다.</p>
User Ports(사용자 포트)	<p>사용자에 대해 지정할 포트 범위입니다. 범위를 시작할 위치를 나타내는 <b>Start(시작)</b> 포트를 구성합니다. 각 개별 사용자 세션의 TCP 또는 UDP 연결에 지정하려는 포트 수를 나타내는 <b>Range(범위)</b> 값을 구성합니다.</p> <p>참고 ICMP 트래픽은 포트 매핑 없이 전달됩니다.</p> <p>Cisco에서는 <b>Range(범위)</b> 값을 1000 이상으로 권장합니다. TS 에이전트에서 트래픽에 대한 포트가 자주 부족한 경우 <b>Range(범위)</b> 값을 늘리십시오.</p> <p>참고 사용되는 포트의 수가 <b>Range(범위)</b>의 값을 초과하면 사용자 트래픽이 차단됩니다.</p> <p>TS 에이전트는 다음 공식을 사용하여 <b>End(종료)</b> 값을 자동으로 채웁니다.</p> $[Start\ value] + ([Range\ value] * [Max\ User\ Sessions\ value]) - 1$ <p>항목의 <b>End(종료)</b> 값이 65535를 초과하는 경우 <b>Start(시작)</b> 및 <b>Range(범위)</b> 값을 조정해야 합니다.</p>
Ephemeral Ports(임시 포트)	<p>TS 에이전트가 모니터링하도록 허용할 임시 포트(동적 포트라고도 함)의 범위입니다.</p>

필드	설명
<p>Unknown Traffic Communication(알 수 없는 트래픽 통신)</p>	<p>TS 에이전트가 시스템 포트를 통한 트래픽을 허용하도록 하려면 <b>Permi</b> 합니다. 그러나 TS 에이전트는 포트 사용량을 추적하지 않습니다. 시스템 계정 또는 다른 로컬 사용자 계정에서 사용됩니다. (로컬 사용자 에이전트 서버에만 존재하며, 해당하는 Active Directory 계정은 없습니다. 선택하면 다음 유형의 트래픽을 허용할 수 있습니다.</p> <ul style="list-style-type: none"> <li>• 로컬 시스템 계정(예: SMB(Server Message Block))에서 실행되는 트 대신 허용합니다. 클라우드 사용 Firewall Management Center 또는 Firewall Management CenterFMC에서는 사용자가 Active Directory에 므로 Unknown user(알 수 없는 사용자)가 이 트래픽을 전송하는 것 다.</li> </ul> <p>또한 이 옵션을 활성화하면 로컬 시스템 계정을 사용하여 TS 에이 그인한 경우 클라우드 사용 Firewall Management Center 또는 온프레 Management CenterFMC와의 연결을 성공적으로 테스트할 수 있습</p> <ul style="list-style-type: none"> <li>• 사용자 또는 시스템 세션이 해당 범위의 사용 가능한 포트를 모두 에이전트는 임시 포트의 트래픽을 허용합니다. 이 옵션은 트래픽을 클라우드 사용 Firewall Management Center 또는 온프레미스 Firewa CenterFMC에서는 Unknown user(알 수 없는 사용자)로부터 발생하 별합니다.</li> </ul> <p>이 기능은 도메인 컨트롤러 업데이트, 인증, WMI(Windows Manage 쿼리 등 시스템을 정상 상태로 유지하기 위해 시스템 포트가 필요하 유용합니다.</p> <p>시스템 포트에서 트래픽을 차단하려면 선택을 취소합니다.</p>

필드	설명
Reserve Port(s)(포트 예약)	<p>TS 에이전트가 무시할 포트입니다. 쉼표로 구분된 목록으로 제외할 포트를 다.</p> <p>TS 에이전트는 <b>Reserve Port(s)(포트 예약)</b>에 Citrix MA Client(2598), Citrix Provisioning(6910), Windows Terminal Server(3389)의 기본 포트 값을 자동으 다. 적절한 포트를 제외하지 않으면 해당 포트를 필요로 하는 애플리케이션 수 있습니다.</p> <p>Citrix Provisioning을 사용하고 이전 TS 에이전트 버전에서 업그레이드하는 드에 <b>6910</b>을 입력해야 합니다.</p> <p>TS 에이전트 <b>Reserve Port(s)(포트 예약)</b> 필드에 지정하는 값은 Citrix Provis <b>and Last UDP port numbers</b>(최초 및 최종 UDP 포트 번호) 포트 중 하나와 니다.</p> <p>주의            올바른 포트를 지정하지 않으면 클라이언트가 부팅되지 않습니</p> <p>참고            서버의 프로세스가 <b>System Ports</b>(시스템 포트) 범위에 없는 포트 거나 수신 대기하는 경우 <b>Reserve Port(s)(포트 예약)</b> 필드를 사- 포트를 수동으로 제외해야 합니다.</p> <p>참고            서버에 클라이언트 애플리케이션이 설치되어 있고 애플리케이션 포트 번호를 사용하는 소켓에 바인딩되도록 구성된 경우, <b>Reserv 트 예약)</b> 필드를 사용하여 해당 포트를 변환에서 제외해야 합니</p>

클라우드 사용 **Firewall Management Center** 설정

샘플 **Cloud**(클라우드) 탭 페이지:



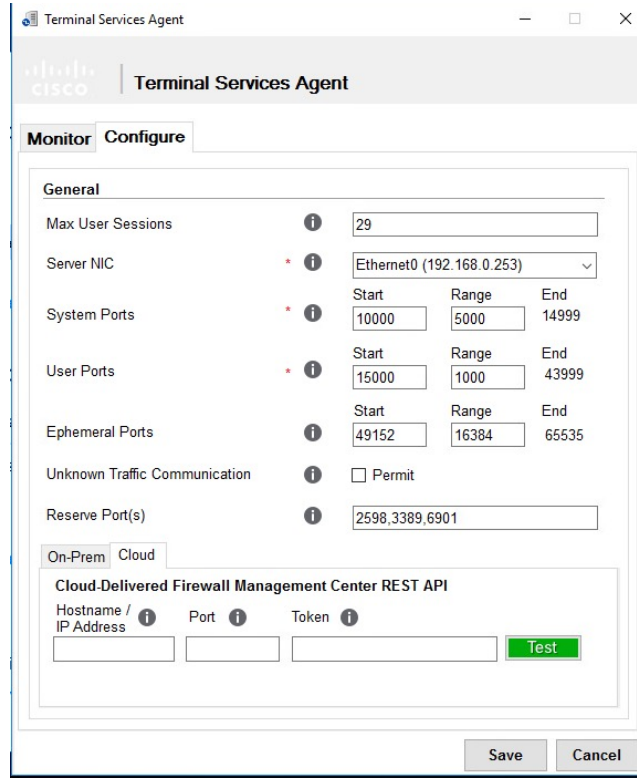


표 2: 클라우드 사용 **Firewall Management Center** 설정 필드

필드	설명
Hostname / IP Address(호스트 이름/IP 주소)	클라우드 사용 Firewall Management Center 인스턴스 호스트 이름 또는 <b>&amp; Services</b> ( 툴 및 서비스) > <b>Firewall Management Center</b> > <b>Monitoring</b> 클릭할 때 표시되는 URL)입니다.
Port(포트)	클라우드 사용 Firewall Management Center에서 REST API 통신에 사용되는 TS 에이전트는 REST API 포트인 <b>443</b> 에 이 필드를 자동으로 채웁니다.
Token(토큰)	Cisco Defense Orchestrator로 인증하는 데 사용되는 API 토큰입니다. 자세한 내용은 <a href="#">토큰 가져오기, 3 페이지</a> 를 참고하십시오.

온프레미스 **Firewall Management Center(FMC)** 설정

기본 연결을 구성할 수 있으며, 필요에 따라 스탠바이(페일오버) 시스템 어플라이언스도 구성할 수 있습니다.

- 시스템 어플라이언스가 독립형이면 FMC/REST API Connection(FMC/REST API 연결) 필드의 두 번째 행을 비워 둡니다.
- 시스템 어플라이언스가 스탠바이(페일오버) 어플라이언스와 함께 구축된 경우, 첫 번째 행을 사용하여 기본 어플라이언스에 대한 연결을 구성하고 두 번째 행을 사용하여 스탠바이(페일오버) 어플라이언스에 대한 연결을 구성합니다.

샘플 On-Prem(온프레미스) 탭 페이지:

표 3: 또는 온프레미스 **Firewall Management CenterFMC** 설정 필드

필드	설명
Hostname / IP Address(호스트 이름/IP 주소)	기본 또는 온프레미스 Firewall Management CenterFMC의 호스트 이름 또는 주소입니다.
Port(포트)	또는 온프레미스 Firewall Management CenterFMC가 REST API 통신에 사용됩니다. TS 에이전트는 또는 온프레미스 Firewall Management CenterFMC의 포트인 <b>443</b> 에 이 필드를 자동으로 채웁니다.
Username and Password(사용자 이름 및 비밀번호)	또는 온프레미스 Firewall Management CenterFMC에서 REST VDI 권한이 있는 또는 온프레미스 Firewall Management CenterFMC 사용자 이름과 비밀번호로 구성된 사용자가 구성하는 방법에 대한 자세한 내용은 <a href="#">REST VDI 역할 생성, 10</a> 내용을 참조하십시오.

## REST VDI 역할 생성

TS 에이전트를 Secure Management Center에 연결하려면 Secure Management Center 사용자에게 REST VDI 역할이 있어야 합니다. REST VDI는 기본적으로 정의되어 있지 않습니다. 역할을 생성하여 TS 에이전트 구성에 사용되는 모든 사용자에게 할당해야 합니다.

사용자 및 역할에 대한 자세한 내용은 *Firepower Management Center* 구성 가이드를 참조하십시오.



**참고** 이 작업은 온프레미스 Firewall Management Center에만 적용됩니다.

클라우드 사용 Firewall Management Center를 사용하는 경우 [API 토큰 가져오기, 3 페이지](#)의 내용을 참조하십시오.

**단계 1** 역할 생성 권한이 있는 사용자로 Secure Management Center에 로그인합니다.

**단계 2** 시스템 (⚙️) > **Users(사용자)** > **System(시스템)** > **Users(사용자)**를 클릭합니다.

**단계 3** **User Roles(사용자 역할)** 탭을 클릭합니다.

**단계 4** User Roles(사용자 역할) 탭 페이지에서 **Create User Role(사용자 역할 생성)**을 클릭합니다.

**단계 5** Name(이름) 필드에 REST VDI를 입력합니다.

역할 이름은 대/소문자를 구분하지 않습니다.

**단계 6** Menu-Based Permissions(메뉴 기반 권한) 섹션에서 **REST VDI**를 선택하고 **Modify REST VDI(REST VDI 수정)**가 선택되어 있는지 확인합니다.

**단계 7** **Save(저장)**를 클릭합니다.

**단계 8** TS 에이전트 구성에 사용되는 사용자에게 역할을 할당합니다.



## 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.