paloalto TECHDOCS

Prisma Access 릴리즈 노트

5.2.0-h14 and 5.2.1

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

October 24, 2024

Table of Contents

Prisma Access 릴리즈 정보

어디에서 사용할 수 있습니까?	무엇이 필요합니까?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 라이센스 ❑ Minimum Required Prisma Access Version 5.2 또는 5.2.1 Preferred 또는 Innovation

Prisma Access 릴리즈 업데이트 정보

Prisma Access 릴리즈 및 업데이트를 통해 최신 정보를 유지하고 사용자를 보호할 수 있습니다. Prisma Access 인프라 업데이트와 같은 일부 업데이트는 Palo Alto Networks에서 관리하며 사전에 알림을 받으므로 이에 대한 계획을 세울 수 있습니다. 일부 업데이트는 사용자의 책임이므로 지정된 버전의 콘텐츠 업데이트 및 소프트웨어 업데이트를 예약해야 합니다. Prisma Access 클라우드 관리 대신 Panorama를 사용하여 Prisma Access를 관리하는 경우, 플러그인에서 Panorama에 사용할 수 있는 새로운 기능을 활용하기 위해 최신 플러그인 버전으로 업그레이드할 시기를 결정해야 합니다.

Panorama 관리형 Prisma Access를 사용하는 경우 이 Panorama 관리형 릴리즈에 대한 Panorama 및 플러그인 요구 사항을 보십시오.

Prisma Access에서 사용할 수 있는 지원되는 **GlobalProtect** 버전

End-of-Life(EoL)가 아닌 모든 GlobalProtect 버전은 Prisma Access에서 사용할 수 있습니다. 그러나 Prisma Access 5.2에는 GlobalProtect 및 필수 버전을 위한 권장 소프트웨어 버전이 포함되어 있습니다.

다음은 Prisma Access에 포함되거나 통합되는 제품 및 서비스의 최신 업데이트에 대한 자세한 내용을 알아볼 수 있습니다.

최신 **Prisma Access** 릴리즈 업데이트	이전 **Prisma Access** 릴리즈 버전	**Prisma Access**에서 지원되는 서비스 및 추가 기능에 대한 업데이트
• Prisma Access 5.2 및 5.2.1의 새로운 기능 • Prisma Access 클라우드 관리의 새로운 기능	• Prisma Access 버전 5.1 • Prisma Access 버전 5.0 • Prisma Access 버전 4.2 • Prisma Access 버전 4.1 • Prisma Access 버전 4.0 • Prisma Access 버전 3.2 Preferred 및 Innovation • Prisma Access 버전 3.1 Preferred 및 Innovation	• Prisma Access 인사이트 • 자율 DEM • SaaS 보안 • 엔터프라이즈 DLP • GlobalProtect • Prisma SASE 멀티테넌트 클라우드 관리 플랫폼 • Prisma SD-WAN

최신 **Prisma Access** 릴리즈 업데이트	이전 **Prisma Access** 릴리즈 버전	**Prisma Access**에서 지원되는 서비스 및 추가 기능에 대한 업데이트
	• Prisma Access 버전 3.0 Preferred 및 Innovation • Prisma Access 버전 2.2 Preferred • Prisma Access 2.2 Preferred 이전 릴리즈	

Prisma Access 5.2 및 5.2.1의 새로운 기능

어디에서 사용할 수 있습니까?	무엇이 필요합니까?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 라이센스 ❑ Minimum Required Prisma Access Version 5.2 또는 5.2.1 Preferred 또는 Innovation

이 섹션에서는 Prisma Access 5.2 및 5.2.1 Preferred 및 Innovation의 새로운 기능 목록과 사용해야 하는 권장 및 필수 소프트웨어 버전을 제공합니다.

이 문서에는 로드맵 정보가 포함되어 있으며 정보 제공 및 계획 목적으로만 공유됩니다. 이는 구속력 있는 약속이 아니며 변경될 수 있습니다.

- Prisma Access 5.2.1 Preferred 및 Innovation을 위한 권장 소프트웨어 버전
- Prisma Access 5.2.1 Preferred 및 Innovation 기능에 대한 인프라, 플러그인 및 데이터플레인 종속성
- Prisma Access 5.2.1 기능

Prisma Access 5.2.1 Preferred 및 Innovation을 위한 권장 소프트웨어 버전

Prisma Access 5.2.1 버전은 두 가지가 있습니다.

- 5.2.1 Preferred는 PAN-OS 10.2.10 데이터플레인을 실행합니다. 구축에서 하위 데이터플레인 버전을 실행하는 경우 5.2.1 Preferred 기능을 구현하려면 PAN-OS 10.2.10으로 데이터플레인을 업그레이드해야 합니다.
- 5.2.1 Innovation은 PAN-OS 11.2.4 데이터플레인을 실행합니다. 5.2 Innovation 기능을 구현하려면 PAN-OS 11.2.4로 업그레이드해야 합니다.

새로운 Prisma Access 5.2.1 Innovation 기능의 경우, Prisma Access에서는 플러그인을 설치하기 전에 **Prisma Access**를 다음 버전으로 업그레이드할 것을 권장합니다.

Prisma Access 버전	클라우드 서비스 플러그인 버전	**5.2.1**용 필수 데이터플레인 버전	권장 **GlobalProtect** 버전	권장 **Panorama** 버전
5.2.1	5.2.0 핫픽스	PAN-OS 10.2.10(5.2.1 Preferred에 필요) PAN-OS 11.2.4(5.2.1 Innovation에 필요)	6.0.7+ 6.1.3+ 6.2.1+	10.2.10+ 11.0.1+ 11.1.0 11.2.4

Prisma Access 5.2 Preferred 및 Innovation을 위한 권장 소프트웨어 버전

Prisma Access 5.2 버전은 두 가지가 있습니다.

- 5.2 Preferred는 PAN-OS 10.2.10 데이터플레인을 실행합니다. 구축에서 하위 데이터플레인 버전을 실행하는 경우 5.2 Preferred 기능을 구현하려면 PAN-OS 10.2.10으로 데이터플레인을 업그레이드해야 할 수 있습니다. 기존 고객인 경우 Prisma Access 5.2.1 Preferred 및 Innovation 기능에 대한 인프라, 플러그인 및 데이터플레인 종속성을 참조하여 Prisma Access 5.2 기능에 데이터플레인 업그레이드가 필요한지 확인하십시오.
- 5.2 Innovation은 PAN-OS 11.2.3 데이터플레인을 실행합니다. 5.2 Innovation 기능을 구현하려면 PAN-OS 11.2.3으로 업그레이드해야 합니다.

새로운 Prisma Access 5.2 Innovation 기능의 경우, Prisma Access에서는 플러그인을 설치하기 전에 **Prisma Access**를 다음 버전으로 업그레이드할 것을 권장합니다.

Prisma Access 버전	클라우드 서비스 플러그인 버전	**5.2**용 필수 데이터플레인 버전	권장 **GlobalProtect** 버전	권장 **Panorama** 버전
5.2	5.2	PAN-OS 10.2.10(5.2 Preferred에 필요) PAN-OS 11.2.3(5.2 Innovation에 필요)	6.0.7+ 6.1.3+ 6.2.1+	10.2.10+ 11.0.1+ 11.1.0 11.2.3

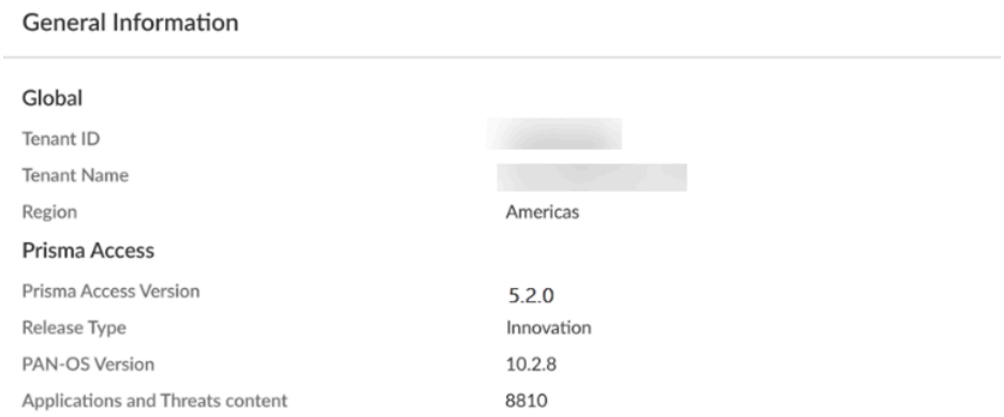
Prisma Access 5.2.1 Preferred 및 Innovation 기능에 대한 인프라, 플러그인 및 데이터플레인 종속성

Prisma Access 5.2.1 기능이 작동하려면 다음 구성 요소 중 하나 이상이 필요합니다.

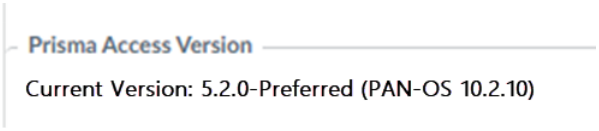
- 인프라 업그레이드 - 인프라에는 기본 서비스 백엔드, 오케스트레이션 및 모니터링 인프라가 포함됩니다.Prisma Access는 Prisma Access 릴리즈의 일반 출시(GA) 날짜 전에 인프라를 업그레이드합니다.

  인프라 업그레이드만 잠금 해제하면 되는 기능은 버전에 관계없이 인프라 업그레이드 시 모든 Prisma Access 구축에 적용됩니다.
- 플러그인 업그레이드(**Prisma AccessPanorama** 관리형 구축 전용) - 플러그인을 설치하면 해당 릴리즈에서 사용할 수 있는 기능이 활성화됩니다. Prisma Access를 관리하는 Panorama에 플러그인을 다운로드하여 설치합니다.

- 데이터플레인 업그레이드 - 데이터플레인을 사용하면 네트워크 및 사용자 트래픽에 대한 트래픽 검사 및 보안 정책 시행이 가능합니다.
  - Prisma Access (Managed by Strata Cloud Manager)의 경우, 관리 > 구성 > **NGFW** 및 **Prisma Access** > 개요로 이동하십시오.



  - Prisma Access (Managed by Panorama) 구축의 경우, **Panorama** > 클라우드 서비스 > 구성 > 서비스 설정으로 이동하고 **Prisma Access** 버전을 확인하여 데이터플레인 버전을 볼 수 있습니다. Prisma Access 5.2.1 Preferred는 PAN-OS 10.2.10을 실행하고 Prisma Access Innovation은 PAN-OS 11.2.4를 실행합니다.



*5.2.1 Innovation*으로 데이터플레인을 업그레이드하는 것은 선택 사항이며, 데이터플레인 업그레이드가 필요한 기능을 활용하려는 경우에만 필요합니다.

이러한 기능은 Prisma Access의 인프라 업그레이드를 통해서만 활성화됩니다.

- 고성능 지사 사이트 가시성
- Prisma Access 에이전트 관찰 가능성
- 새로운 Prisma Access (Managed by Strata Cloud Manager) 구축을 위한 RFC6598 모바일 사용자 주소 풀
- 지사 사이트 및 서비스 연결에서의 라우팅 테이블 가시성
- ZTNA 커넥터 보기 및 모니터링 업데이트
- 에이전트 기반 명시적 프록시 보기
- 이스라엘 및 사우디아라비아 Strata 로깅 서비스 지역 지원
- 기존 Prisma Access 구축을 위한 네이티브 IPv6 지원

이러한 기능을 사용하려면 인프라 및 플러그인 업그레이드가 필요하지만 데이터플레인 업그레이드는 필요하지 않습니다. 그러나 이러한 기능을 사용하려면 최소 10.2.4의 데이터플레인 버전이 필요합니다.

- Colo-Connect에 대한 명시적 프록시 지원
- DNS 프록시에 대한 명시적 프록시 지원
- ZTNA 커넥터와의 명시적 프록시 통합
- 와일드카드 FQDN을 사용한 ZTNA 커넥터 정책 구성 업데이트
- 명시적 프록시 타사 엔터프라이즈 브라우저 통합

다음 5.2.1 기능을 사용하려면 인프라 및 플러그인 업그레이드가 필요하고 최소 PAN-OS 10.2.10의 데이터 플레인 버전이 필요하므로 Prisma Access 5.2.1 Preferred 기능이 됩니다.

- 온보딩 애플리케이션을 위한 ZTNA 커넥터 향상
- 없음

다음 5.2 기능을 사용하려면 PAN-OS 11.2.4로의 인프라**,** 플러그인 및 데이터플레인 업그레이드가 필요하므로 Prisma Access 5.2.1 Innovation 기능이 됩니다.

- 원격 네트워크 - 고성능 프라이빗 앱 액세스 지원
- 모바일 사용자를 위한 고정 IP 주소 향상
- 모바일 사용자를 위한 고정 IP 주소 할당 보기

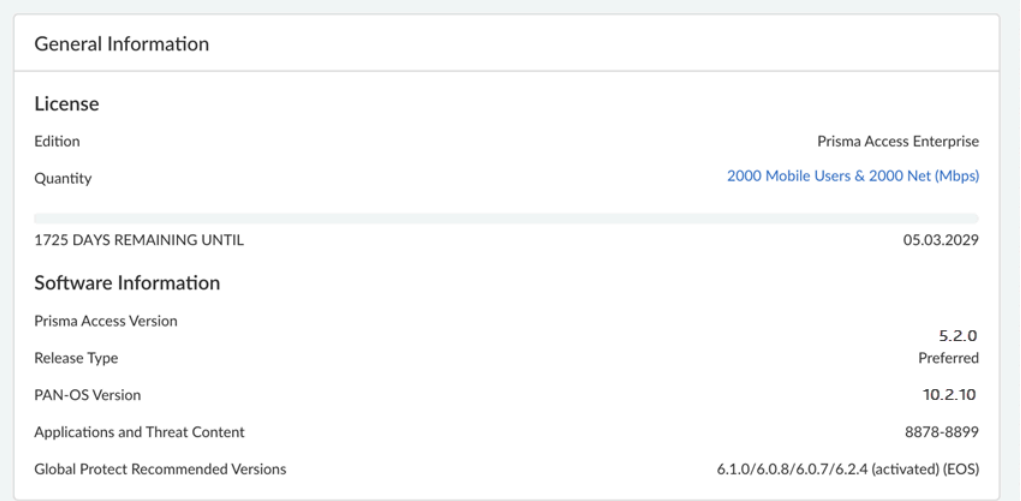
Prisma Access 5.2 Preferred 및 Innovation 기능에 대한 인프라, 플러그인 및 데이터플레인 종속성

Prisma Access 5.2 기능이 작동하려면 다음 구성 요소 중 하나 이상이 필요합니다.

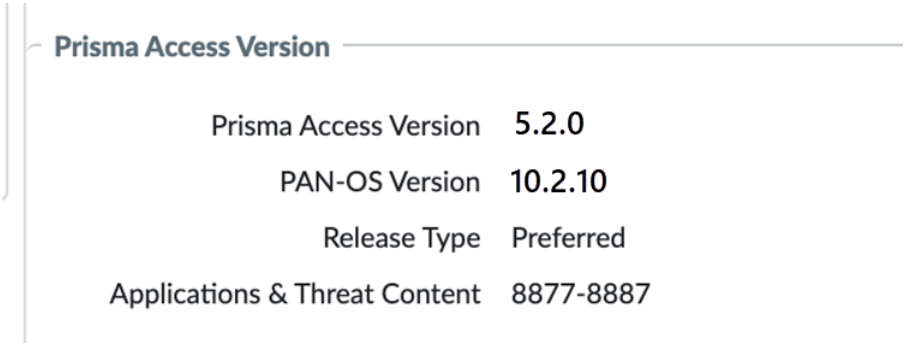
- 인프라 업그레이드 - 인프라에는 기본 서비스 백엔드, 오케스트레이션 및 모니터링 인프라가 포함됩니다.Prisma Access는 Prisma Access 릴리즈의 일반 출시(GA) 날짜 전에 인프라를 업그레이드합니다.

  인프라 업그레이드만 잠금 해제하면 되는 기능은 버전에 관계없이 인프라 업그레이드 시 모든 Prisma Access 구축에 적용됩니다.
- 플러그인 업그레이드**(Prisma AccessPanorama** 관리형 구축 전용**)** - 플러그인을 설치하면 해당 릴리즈에서 사용할 수 있는 기능이 활성화됩니다. Prisma Access를 관리하는 Panorama에 플러그인을 다운로드하여 설치합니다.

- 데이터플레인 업그레이드 - 데이터플레인을 사용하면 네트워크 및 사용자 트래픽에 대한 트래픽 검사 및 보안 정책 시행이 가능합니다.
  - Prisma Access (Managed by Strata Cloud Manager)의 경우, 관리 > 구성 > **NGFW** 및 **Prisma Access** > 개요로 이동하십시오.



  - Prisma Access (Managed by Panorama) 구축의 경우, **Panorama** > 클라우드 서비스 > 구성 > 서비스 설정으로 이동하고 **Prisma Access** 버전을 확인하여 데이터플레인 버전을 볼 수 있습니다. Prisma Access 5.2 Preferred는 PAN-OS 10.2.10을 실행하고 Prisma Access Innovation은 PAN-OS 11.2.3을 실행합니다.



*5.2 Innovation*으로 데이터플레인을 업그레이드하는 것은 선택 사항이며, 데이터플레인 업그레이드가 필요한 기능을 활용하려는 경우에만 필요합니다.

이러한 기능은 Prisma Access의 인프라 업그레이드를 통해서만 활성화됩니다.

- 엔드포인트 DLP
- 모바일 사용자를 위한 IP 최적화 및 명시적 프록시 구축을 통해 Prisma Access SaaS 연결 간소화
- 트래픽 복제를 위한 TLS 1.3 및 PubSub 지원
- Colo-Connect 보기 및 모니터링

이러한 기능을 사용하려면 인프라 및 플러그인 업그레이드가 필요하지만 데이터플레인 업그레이드는 필요하지 않습니다.

- 25,000개의 원격 네트워크 및 50,000개의 IKE 게이트웨이 지원
- 프라이빗 IP 주소 가시성 및 에이전트 기반 프록시 트래픽 적용
- 명시적 프록시 사용자를 위한 IP 주소 최적화 - 프록시 구축
- 클라우드 서비스 플러그인에 대한 RBAC 지원
- 간소화된 Prisma Access 프라이빗 앱 연결
- AWS용 SP 백본 통합 지원
- Strata Cloud Manager에서 Prisma Access, 데이터플레인, 애플리케이션 및 위협 콘텐츠 버전 보기

다음 5.2 기능을 사용하려면 인프라 및 플러그인 업그레이드가 필요하고 최소 PAN-OS 10.2.10의 데이터 플레인 버전이 필요하므로 Prisma Access 5.2 Preferred 기능이 됩니다.

- 원격 네트워크 - 고성능

다음 5.2 기능을 사용하려면 Prisma Access 11.2.3으로의 인프라, 플러그인 및 데이터플레인 업그레이드가 필요하므로 Prisma Access 5.2 Innovation 기능이 됩니다.

- CIAM을 통한 동적 권한 액세스를 위한 SC-NAT 지원
- 커밋리스 앱 온보딩을 위한 ZTNA 커넥터 지원

Prisma Access 5.2.1 기능

다음 표는 Prisma Access 5.2.1에서 일반적으로 사용할 수 있는 새로운 기능을 설명합니다.

Colo-Connect에 대한 명시적 프록시 지원

지원 대상: Prisma Access 5.2.1 Preferred 및 Innovation

콜로케이션 시설에 직접 연결된 대규모 데이터 센터가 있는 경우 이제 Prisma Access 명시적 프록시를 통해 연결하여 프라이빗 애플리케이션에 고속으로 액세스할 수 있습니다. 이러한 향상을 통해 지역당 최대 20Gbps의 처리량을 얻을 수 있습니다.

Colo-Connect를 명시적 프록시와 통합하면 다음과 같은 이점이 있습니다.

- 명시적 프록시는 가장 가까운 Prisma Access 컴퓨팅 위치에 자동으로 연결하여 가능한 최상의 지연 시간을 제공합니다.
- 네트워크 및 라우팅 종속성을 제거하고 프라이빗 애플리케이션에 대한 자동화된 보안 터널 관리 및 라우팅을 제공합니다.
- Colo-Connect는 중첩된 네트워크에서 프라이빗 애플리케이션 검색을 지원하여 유연성과 접근성을 보장합니다.

DNS 프록시에 대한 명시적 프록시 지원

지원 대상: Prisma Access (Managed by Strata Cloud Manager) 5.2.1 Preferred 및 Innovation

명시적 프록시는 DNS 프록시 사용자 지정을 포함하도록 지원을 확장합니다. 명시적 프록시는 지역 DNS, 사용자 지정 DNS 등과 같은 DNS 설정을 지원합니다. 또한 타사 DNS 확인자 또는 온프레미스 DNS 확인자를 사용하여 퍼블릭 및 프라이빗 앱을 확인하고 FQDN별로 사용할 수 있습니다. 이 기능은 현재 에서만 지원됩니다.

명시적 프록시를 통한 타사 엔터프라이즈 브라우저의 안전한 통합

지원 대상: Prisma Access 5.2.1 Preferred 및 Innovation

이제 Prism Access는 타사 엔터프라이즈 브라우저를 통해 프라이빗 애플리케이션에 안전하게 액세스할 수 있습니다. 이러한 향상을 통해 타사 엔터프라이즈 브라우저와 Prisma Access 간에 사용자 정보를 안전하고 투명하게 교환할 수 있으며, Prisma Access 내에서 사용자 ID 기반 정책 규칙을 적용할 수 있습니다. 이를 통해 최종 사용자가 타사 엔터프라이즈 브라우저에 이미 로그인한 경우 Prisma Access에서 다시 인증할 필요가 없습니다.

ZTNA 커넥터와의 명시적 프록시 통합

지원 대상: Prisma Access 5.2.1 Preferred 및 Innovation

이제 ZTNA 커넥터를 통해 프라이빗 애플리케이션에 연결하는 사용자는 Prisma Access 명시적 프록시를 통해 연결을 설정할 수 있습니다. 이 통합은 Prisma Access 브라우저 및 에이전트 프록시를 위한 최대 10Gbps 용량의 ZTNA 커넥터를 지원합니다.

다음은 추가적인 이점입니다.

- 명시적 프록시는 명시적 프록시를 사용하여 가장 가까운 Prisma Access 컴퓨팅 위치에 자동으로 연결하여 최적의 지연 시간을 보장합니다.
- 네트워크 및 라우팅 종속성을 제거하고 프라이빗 애플리케이션에 대한 자동화된 보안 터널 관리 및 라우팅을 보장합니다.
- ZTNA 커넥터는 프라이빗 애플리케이션을 자동으로 검색할 수 있는 클라우드 ID 엔진(CIE)를 지원합니다.
- ZTNA 커넥터는 중첩된 네트워크에서 프라이빗 애플리케이션 검색을 지원하여 유연성과 접근성을 보장합니다.

고성능 지사 사이트 가시성

지원 대상: Prisma Access 5.2.1 Preferred 및 Innovation

Prisma Access의 고성능 지사(RN-HP)는 레거시 지사와 비교하여 다른 특징을 가지고 있으며, 둘 다 고객 환경 내에서 공존하게 됩니다. 관리 시스템은 네트워크 관리자가 문제 해결을 돕기 위해 새로운 RN-HP 지사 유형을 수용해야 합니다.

기존 **Prisma Access** 구축을 위한 네이티브 **IPv6** 지원

지원 대상: 모든 구축을 위한 Prisma Access 5.2.1 Preferred 및 Innovation(새로운 구축에 대한 IPv6 지원은 Prisma Access 5.1.1부터 지원되고 기존 구축에 대한 지원은 Prisma Access 5.2.1에 추가됨)

Prisma Access는 프라이빗 애플리케이션에서 IPv6 지원을 확장하여 모바일 사용자, 원격 네트워크 및 서비스 연결에 대한 포괄적인 종단 간 IPv6 지원을 포함하며, 기존 Prisma Access 구축에 네이티브 IPv6 지원을 추가합니다.

네이티브 IPv6 지원의 장점 중 하나는 IPv6 전용 엔드포인트를 활용하는 모바일 사용자가 GlobalProtect를 사용하여 IPv6 연결을 통해 Prisma Access와 연결을 설정할 수 있다는 점입니다. 또한 이러한 지원을 통해 인터넷을 통해 퍼블릭 SaaS 애플리케이션에 쉽게 액세스할 수 있으며, 특히 해당 대상에 IPv6 연결이 필요한 경우 더욱 그렇습니다.

IPv6은 IPv4에 비해 더 큰 주소 공간을 자랑하므로 고유 IP 주소를 거의 무제한으로 수용할 수 있습니다. Prisma Access는 네이티브 IPv6 지원을 통해 IPv6 및 이중 스택 연결 모두와 호환되도록 설계되어 IPv4에서 IPv6으로의 마이그레이션 프로세스를 용이하게 합니다. 이러한 호환성은 이전 버전과의 호환성을 보장하고 조직이 클라우드 기반 및 IPv6 지원 네트워크로 전환할 수 있도록 지원합니다.

Prisma Access 에이전트 관찰 가능성

지원 대상: Prisma Access 5.2.1 Preferred 및 Innovation

Prisma Access 에이전트는 Prisma Access를 사용하여 모바일 인력을 보호할 수 있는 차세대 모바일 액세스 에이전트입니다. 오늘날의 하이브리드 인력을 위해 설계된 Prisma Access 에이전트는 엔터프라이즈 앱과 인터넷 모두에 안전하고 편리한 액세스를 제공하고 조직의 네트워크, IT 및 보안 운영을 간소화합니다. Strata Cloud Manager에서 인사이트 > 활동 인사이트 > 사용자로 이동하여 Prisma Access 에이전트 구축에 대한 정보를 확인하십시오.

원격 네트워크 - 고성능 프라이빗 앱 액세스 지원

지원 대상: Prisma Access 5.2.1 Preferred 및 Innovation

Prisma Access 원격 네트워크 - 고성능은 기존의 인터넷 송신 지원 외에도 프라이빗 앱 액세스 지원을 추가합니다. 이러한 지원을 통해 다음을 수행할 수 있습니다.

- 고성능 원격 네트워크로 연결된 지사에서 프라이빗 앱 검색
- 서비스 연결을 사용하여 다른 지사와 통신(지사-지사 트래픽)
- 서비스 연결을 사용하여 모바일 사용자와 통신(모바일 사용자-지사 트래픽)

지사 사이트 및 서비스 연결에서의 라우팅 테이블 가시성

지원 대상: Prisma Access 5.2.1 Preferred 및 Innovation

모바일 사용자를 위한 고정 **IP** 주소 향상

지원 대상: Prisma Access 5.2.1 Innovation

Prisma Access는 모바일 사용자를 위한 정적 IP 주소 기능을 추가하여 Prisma Access 극장이나 사용자 ID를 기반으로 사용자에게 정적 IP 주소를 할당할 수 있습니다.

모바일 사용자의 IP 주소 할당을 개선하기 위해 이제 극장 및 사용자 ID뿐 아니라 위치 그룹과 사용자 그룹을 기준으로 사용할 수 있습니다.

또한, 지원되는 IP 주소 풀 프로파일 수가 10,000개로 늘어났습니다.

새로운 **Prisma Access (Managed by Strata Cloud Manager)** 구축을 위한 **RFC6598** 모바일 사용자 주소 풀

지원 대상: Prisma Access (Managed by Strata Cloud Manager) 5.2.1 Preferred 및 Innovation

모든 Prisma Access 구축에는 모바일 사용자 주소 IP 풀이 필요합니다. Prisma Access는 이 풀의 IP 주소를 GlobalProtect에 연결된 각 디바이스에 할당합니다. Palo Alto Networks는 GlobalProtect 모바일 사용자의 온보딩을 간소화하기 위해 RFC6598의 기본 IP 주소 풀을 사용하여 새로운 Prisma Access(Strata Cloud Manager에서 관리됨) 구축을 제공합니다. IP 풀은 100.92.0.0/16입니다. 더 많은 주소가 필요하거나 자체 주소를 사용하려는 경우 이 풀을 수정하거나 삭제하고 고유한 IP 주소 풀을 추가할 수 있습니다.

이스라엘 및 사우디아라비아 **Strata** 로깅 서비스 지역 지원

지원 대상: Prisma Access 5.2.1 Preferred 및 Innovation

Prisma Access는 이스라엘 및 사우디아라비아 Strata 로깅 서비스 지역을 지원합니다.

ZTNA 커넥터 보기 및 모니터링 업데이트

지원 대상: Prisma Access 5.2.1 Preferred 및 Innovation

제로 트러스트 네트워크 액세스(ZTNA) 커넥터는 모든 애플리케이션에 대한 프라이빗 애플리케이션 액세스를 간소화합니다. 사용자 환경의 ZTNA 커넥터 VM은 프라이빗 애플리케이션과 간의 터널을 자동으로 형성합니다. Prisma Access 5.2.1부터 사용하기 쉽도록 ZTNA 커넥터 페이지의 디자인을 수정하고 와일드카드, FQDN 및 IP 서브넷 대상에 대한 세부 정보가 포함된 표를 추가했습니다.

에이전트 기반 명시적 프록시 보기

지원 대상: Prisma Access 5.2.1 Preferred 및 Innovation

설명을 기다리고 있습니다.

모바일 사용자를 위한 고정 IP 주소 할당 보기

지원 대상: Prisma Access 5.2.1 Innovation

정적 IP 풀을 모니터링하려면 인사이트 > 활동 인사이트 > 사용자로 이동하여 **IP** 풀 사용률 위젯에서 정적 IP 풀을 모니터링합니다. 정적 IP 할당 기능을 사용하면 Prisma Access 모바일 사용자에게 고정 IP 주소를 할당할 수 있습니다. 이 기능은 네트워크 구축이 네트워크 및 애플리케이션 설계의 일환으로 IP 주소를 사용하여 리소스에 대한 사용자 액세스를 제한하는 경우 유용합니다. 이 기능을 사용하면 극장 및 사용자에 따라 IP 풀을 정의할 수 있습니다.

ZTNA 커넥터의 보안 정책에 대한 와일드카드 FQDN 구성

지원 대상: Prisma Access 5.2.1 Preferred 및 Innovation

보안 정책 규칙에서 wildcard FQDN의 사용은 현재 프로토콜 제한에 의해 제한됩니다. 결과적으로, 현재 보안 정책 규칙에서 와일드카드 FQDN에 대한 HTTP 및 HTTPS 프로토콜만 지원됩니다.

이 개선 사항을 통해 다음이 가능해집니다.

- 와일드카드 애플리케이션 FQDN을 기반으로 보안 정책을 구성할 수 있습니다.
- 동일한 와일드카드 FQDN을 공유하는 모든 검색된 애플리케이션에 동일한 보안 정책이 적용됩니다.
- 와일드카드 FQDN과 일치하는 새로운 애플리케이션이 검색되면 새 커밋을 요구하지 않고도 트래픽이 통과할 수 있습니다.

온보딩 애플리케이션을 위한 **ZTNA** 커넥터 향상

지원 대상: Prisma Access 5.2.1 Preferred 및 Innovation

기업의 사용자가 많은 수의 프라이빗 앱에 액세스하는 경우 인프라의 애플리케이션 수가 15,000개를 초과하면 ZTNA 커넥터에서 확장성 문제가 발생할 수 있습니다.

ZTNA 커넥터는 확장성을 향상시키는 개선 사항을 제공하여 사용자가 다음을 온보딩할 수 있도록 합니다.

- 테넌트당 20,000개의 애플리케이션 및 커넥터 그룹당 4000개의 애플리케이션
- 컴퓨팅 지역당 16Gbps 대역폭을 갖춘 테넌트 전체에 400개의 커넥터

온보딩 애플리케이션을 위한 **ZTNA** 커넥터

지원 대상: Prisma Access 5.2.1 Preferred 및 Innovation

기업의 사용자가 많은 수의 프라이빗 앱에 액세스하는 경우 인프라의 애플리케이션 수가 15,000개를 초과하면 ZTNA 커넥터에서 확장성 문제가 발생할 수 있습니다.

ZTNA 커넥터는 확장성을 향상시키는 개선 사항을 제공하여 사용자가 다음을 온보딩할 수 있도록 합니다.

- 테넌트당 20,000개의 애플리케이션 및 커넥터 그룹당 4000개의 애플리케이션
- 컴퓨팅 지역당 16Gbps 대역폭을 갖춘 테넌트 전체에 400개의 커넥터

와일드카드 **FQDN**을 사용한 **ZTNA** 커넥터 정책 구성 업데이트

지원 대상: Prisma Access 5.2.1 Preferred 및 Innovation

보안 정책 규칙에서 wildcard FQDN의 사용은 현재 프로토콜 제한에 의해 제한됩니다. 결과적으로, 현재 보안 정책 규칙에서 와일드카드 FQDN에 대한 HTTP 및 HTTPS 프로토콜만 지원됩니다.

이 개선 사항을 통해 다음이 가능해집니다.

- 와일드카드 애플리케이션 FQDN을 기반으로 보안 정책을 구성할 수 있습니다.
- 동일한 와일드카드 FQDN을 공유하는 모든 검색된 애플리케이션에 동일한 보안 정책이 적용됩니다.
- 와일드카드 FQDN과 일치하는 새로운 애플리케이션이 검색되면 새 커밋을 요구하지 않고도 트래픽이 통과할 수 있습니다.

Prisma Access 5.2 기능

이 섹션에서는 Prisma Access 5.2에서 사용할 수 있는 새로운 기능을 설명합니다.

25,000개의 원격 네트워크 및 **50,000**개의 **IKE** 게이트웨이 지원

지원 대상**:** Prisma Access 5.2 Preferred 및 Innovation

이 기능을 구현하려면 Palo Alto Networks 계정 팀에 문의하십시오. 그러면 담당 계정 팀이 요청을 수용하기 위해 SRE 케이스를 열어드립니다.

프라이빗 **IP** 주소 가시성 및 에이전트 기반 프록시 트래픽 적용

지원 대상**:** Prisma Access 5.2 Preferred 및 Innovation

지사에서 GlobalProtect 에이전트를 통해 Prisma Access 명시적 프록시에 연결하는 사용자는 엔드포인트의 프라이빗 IP 주소를 활용하여 로깅하거나 IP 주소 기반 시행을 적용할 수 있습니다.

명시적 프록시 사용자를 위한 **IP** 주소 최적화 **-** 프록시 구축

지원 대상**:** Prisma Access 5.2 Preferred 및 Innovation

IP 주소 최적화는 구축에서 전체 IP 주소 수를 줄여서 허용 목록 워크플로를 간소화하는 동시에 복원력을 개선하고 Prisma Access 테넌트의 빠른 온보딩을 가능하게 하는 일련의 아키텍처 개선 사항입니다.

IP 주소 고정성

IP 주소 고정성을 사용하면 사용자 세션 전체에서 Prisma Access의 동일한 송신 IP 주소를 유지하기 위해 사용자 세션이 필요한 SaaS 앱 및 웹사이트를 보호할 수 있습니다.

SaaS 애플리케이션 온보딩 간소화

Prisma Access 위치를 추가하거나 기존 Prisma Access 위치에서 스케일링 이벤트가 발생하면 명시적 프록시 구축에 새로운 IP 주소가 할당될 수 있습니다. 새로운 송신 및 게이트웨이 IP 주소를 검색하여 SaaS 애플리케이션 허용 목록에 추가하는 것이 가장 좋습니다. IP 주소 최적화는 대규모 구축에서 관리해야 하는 IP 주소 수를 줄입니다.

엔드포인트 **DLP**

지원 대상**:** Prisma Access 5.2 Preferred 및 Innovation

Prisma Access 에이전트가 필요합니다.

엔드포인트 DLP를 사용하면 주변 디바이스가 조직의 엔드포인트에 연결될 때 보안 관리자에게 알리거나 해당 사용을 허용 또는 차단하여 주변 디바이스의 사용을 제어할 수 있습니다. 민감한 데이터가 주변 디바이스로 유출되지 않도록 하려면 고급 감지 방법 및 사용자 정의 데이터 프로파일을 사용하여 자체 트래픽 일치 기준 또는 사전정의된 ML 기반 및 regex 데이터 프로파일을 정의하십시오.

보호하려는 엔드포인트에 를 설치하면 엔드포인트와 주변 디바이스 간의 파일 이동을 감지할 수 있으며, 파일 이동을 감지했을 때 엔드포인트 DLP 정책 규칙을 평가하고 시행합니다. 필요한 경우, 에서는 트래픽을 에 포워드하여 검사 및 판결 렌더링을 수행합니다. 그런 다음, 에서는 엔드포인트 DLP 정책 규칙에서 구성된 작업을 수행하는 에 판결을 커뮤니케이션합니다. 또한, 도 DLP 인시던트가 생성될 때 최종 사용자에게 알림을 표시해야 합니다.

를 사용하는 엔드포인트의 검사는 다음과 같습니다. 여기에서는 가 성공적으로 설치되었으며 엔드포인트 DLP 정책 규칙을 구성했다고 가정합니다.

1. 조직의 사용자가 주변 디바이스를 노트북에 연결합니다.
2. 사용자는 엔드포인트의 파일을 연결된 주변 디바이스로 이동합니다.
3. 에서는 사용자가 엔드포인트의 파일을 주변 디바이스로 이동하려는 시도를 기록하고 엔드포인트 DLP 정책 규칙 기준을 평가합니다.
   - 정책 규칙 일치 없음 - 엔드포인트 DLP 정책 규칙 일치가 식별되지 않은 경우 주변 디바이스 연결이 허용되며 엔드포인트는 주변 디바이스에 대한 전체 읽기 및 쓰기 액세스 권한을 가집니다.
   - 주변 제어 정책 규칙 - 주변 제어 정책 규칙을 생성하여 액세스를 제어하면 에서는 정책 규칙에서 구성된 허용 또는 차단 작업을 수행합니다.

     예를 들어, 엔드포인트 DLP 정책 규칙이 주변 디바이스에 대한 연결을 차단하면 에서 주변 디바이스에 대한 쓰기 권한을 취소합니다. 이 경우 엔드포인트는 파일을 주변 디바이스에 업로드할 수 없습니다.

     그 반대로, 엔드포인트 DLP 정책 규칙이 주변 디바이스에 연결을 허용하는 경우 에서 주변 디바이스에 엔드포인트 쓰기 액세스 권한을 부여합니다. 이 경우 엔드포인트는 파일을 주변 디바이스에 업로드할 수 있습니다.
   - 이동 중인 데이터 정책 규칙 - 주변 디바이스에 대한 연결이 허용됩니다. 가 엔드포인트에서 주변 디바이스로의 파일 이동을 감지하면 파일을 에 포워드하여 검사 및 판결 렌더링을 수행합니다. 는 또한 가 포워딩된 각 파일을 식별하는 데 사용하는 `fileSHA`와 같은 중요한 파일 메타데이터를 포워드합니다. 그런 다음,

     는 판결을 에 전송하고, 는 민감한 데이터를 감지하면 엔드포인트 DLP 정책 규칙 작업을 수행합니다. 가 `fileSHA`를 기반으로 이미 검사된 파일이라고 감지하면 에서 기존 판결을 에 반환합니다. 는 동일한 파일을 두 번 검사하지 않습니다.
4. 는 주변 제어 또는 이동 중인 데이터 정책 규칙에 구성된 엔드포인트 DLP 정책 규칙 작업을 시행합니다.
5. DLP 인시던트는 적합한 경우에 생성됩니다. 최종 사용자 코칭을 구성한 경우 엔드포인트에 알림이 표시되어 사용자에게 알립니다.

명시적 프록시 중국 지원

지원 대상: Prisma Access 5.2 Preferred 및 Innovation

Prisma Access는 중국에서의 명시적 프록시 구축을 지원합니다.

클라우드 서비스 플러그인에 대한 **RBAC** 지원

지원 대상: Prisma Access (Managed by Panorama) 5.2 Preferred 및 Innovation

원격 네트워크 **-** 고성능

지원 대상: Prisma Access 5.2 Preferred 및 Innovation

Prisma Access는 대규모 사이트, 자동화된 로드 밸런싱, 간소화된 온보딩, 지역 이중화, 단일 송신 IP 관리, Prisma SD-WAN을 포함한 다양한 SD-WAN 솔루션과의 호환성을 지원하여 고대역폭 IPsec 종료를 위한 포괄적인 솔루션을 제공합니다. 이러한 기능은 전체적으로 원격 사이트 연결의 확장성, 성능 및 안정성을 향상시킵니다.

비즈니스가 확장되고 사무실 위치가 지리적으로 분산됨에 따라 원격 네트워크 - 고성능이라고도 하는 Prisma Access 고성능 원격 네트워크를 사용하여 높은 대역폭을 갖춘 지사 사이트를 신속하게 온보딩할 수 있습니다. 이러한 네트워크는 다음과 같은 이점을 제공합니다.

- 서비스 IP 주소 또는 서비스 엔드포인트 주소당 최대 3Gbps의 총 대역폭을 지원하므로 IPsec 터널 종료에 사용할 수 있는 IP 주소 또는 FQDN의 수가 줄어듭니다.
- 가용성 및 내결함성을 개선하기 위한 지역 이중화를 포함합니다.
- NAT를 사용하여 퍼블릭 송신 IP 주소를 줄입니다.
- 지리적 가용성에 따라 위치를 선택할 수 있는 제품 내 권장 사항을 통해 온보딩을 간소화합니다.
- Prisma SD-WAN이 퍼블릭 및 프라이빗 트랜스포트와 프라이빗 WAN 언더레이 경로를 통해 보안 패브릭 VPN 경로를 능동적으로 조사하여 링크 품질을 결정하는 링크 품질 메트릭(LQM)에 대한 지원이 포함됩니다. 프로브는 지터, 지연 시간 및 패킷 손실과 같은 네트워크 성능 메트릭을 지속적으로 측정합니다. 이러한 메트릭은 애플리케이션별 성능 메트릭 및 레이어 1부터 레이어 7까지의 연결 가능성과 함께 신규 및 기존 애플리케이션 흐름에 대한 트래픽 전달 결정에 영향을 줍니다.

동적 권한 액세스를 위한 경로 요약

지원 대상: Prisma Access (Managed by Strata Cloud Manager) 5.2 Innovation

동적 권한 액세스가 활성화된 Prisma Access 테넌트에서 온프레미스 네트워크에 모바일 사용자(MU) 경로를 알릴 때 경로를 요약할 수 있습니다. 경로 요약은 기본 클라우드 라우터와 같이 용량이 제한적인 온프레미스 장비를 보유한 기업에 유용합니다. 경로 요약을 통해 이러한 디바이스에 대한 수요를 줄임으로써 디바이스가 데이터 센터와 통신할 때 경로 용량을 초과하지 않도록 할 수 있습니다.

경로 요약을 활성화하려면 여러 프로젝트에서 사용할 수 있는 대규모 IP 풀 목록으로 구성된 글로벌 요약 풀을 구성합니다. 그런 다음 Prisma Access 서비스 연결에서 경로 요약을 활성화합니다. 사용자가 Prisma Access 에이전트를 사용하여 구성된 글로벌 요약 풀 범위 내의 IP 주소를 가진 프로젝트에 연결하는 경우,

서비스 연결은 더 작은 프로젝트 수준 경로 대신 글로벌 요약 풀을 알립니다. 이는 네트워크로 전송되는 경로 수를 줄이는 데 도움이 됩니다.

CIAM을 통한 동적 권한 액세스를 위한 **SC-NAT** 지원

지원 대상: Prisma Access 5.2 Innovation

DPA를 사용하고 데이터 센터 또는 본사 위치에서 프라이빗 앱에 액세스하기 위한 서비스 연결을 생성한 경우 동적 권한 액세스(DPA)에 SC-NAT 지원을 사용하십시오. 인프라 서브넷의 IP 주소가 겹칠 경우 DPA 환경의 여러 프로젝트에서 IP 주소 고갈이 발생할 수 있습니다. 이 문제를 해결하기 위해 Prisma Access는 IP 주소에 대해 소스 NAT(SNAT)를 구현할 수 있습니다.

- Prisma Access에서 서비스 연결을 사용하여 프라이빗 앱에 액세스하는 모바일 사용자의 단일 IP 주소를 매핑할 수 있음
- 간편한 라우팅을 위한 SNAT 제공
- IP 풀 중복 제거
- Prisma Access와 데이터 센터 또는 본사 위치 간의 IP 풀 IPv4 고갈 제거

간소화된 **Prisma Access** 프라이빗 앱 연결

지원 대상: Prisma Access 5.2 Preferred 및 Innovation

프라이빗 앱에 액세스하는 한 가지 방법은 서비스 연결-기업 액세스 노드(SC-CAN)라고도 하는 서비스 연결을 사용하는 것입니다. 다음과 같은 이유로 서비스 연결을 사용하여 프라이빗 앱에 연결하기 어려울 수 있습니다.

- SC-CAN 병목 현상으로 인한 프라이빗 애플리케이션의 비결정적 처리량
- 잘못된 전송 홉으로 인한 지연
- SC-CAN 구축의 운영 복잡성

이 문제를 해결하기 위해 Prisma Access는 다음과 같은 라우팅 인프라 라우팅 개선 사항을 강화했습니다.

- 내부 네트워크를 개선하여 SC-CAN 병목 현상 제거
- 필요한 경우 앵커 SC-CAN을 오케스트레이션하여 잘못된 전송 홉과 비효율적인 라우팅 방지

이 설계는 다음과 같은 이점을 제공합니다.

- 구축하기 쉬운 라우팅 설정
- 간편한 데이 제로 설정
- 지정된 SC-CAN에서 프라이빗 앱이 위치한 데이터 센터 또는 본사까지의 결정적 1Gbps 대역폭

모바일 사용자를 위한 **IP** 최적화 및 명시적 프록시 구축을 통해 **Prisma Access SaaS** 연결 간소화

지원 대상: Prisma Access 5.2 Preferred 및 Innovation

Prisma Access는 명시적 프록시 및 모바일 사용자 - GlobalProtect에 대한 IP 최적화 기능을 제공하여 해당 기능을 확장합니다.

모바일 사용자 - GlobalProtect 구축의 경우, 많은 수의 사용자가 한 위치에서 GlobalProtect 게이트웨이에 액세스하면 Prisma Access는 해당 위치를 자동으로 확장하고 다른 GlobalProtect 게이트웨이를 추가합니다. IP 최적화는 자동 확장된 게이트웨이가 이전에 할당된 IP 주소와 동일한 IP 주소를 사용하도록 NAT 레이어를 사용하므로 조직의 허용 목록에 IP 주소를 더 추가할 필요가 없습니다.

Prisma Access는 NAT 레이어를 명시적 프록시 보안 처리 노드(SPN)와 모바일 사용자 SPN으로 확장하여 명시적 프록시 구축을 위해 IP 주소 목록을 허용해야 하는 필요성을 줄입니다. 이 명시적 프록시 NAT 레이어는 프록시 모드 또는 터널 및 프록시 모드에서 모바일 사용자 및 명시적 프록시 구축을 설정하는 경우에 유용합니다.

AWS용 **SP** 백본 통합 지원

지원 대상: Prisma Access 5.2 Preferred 및 Innovation

이 기능을 구현하려면 Palo Alto Networks 계정 팀에 문의하십시오. 그러면 담당 계정 팀이 요청을 수용하기 위해 SRE 케이스를 열어드립니다.

Prisma Access 버전 5.2부터 사용자(서비스 공급자)는 이제 고객의 퍼블릭 클라우드 송신 트래픽에 대해 AWS와 GCP를 유연하게 선택할 수 있습니다. 라이센스 활성화에서 추가 지역을 볼 수 있고, 연결 및 IP 주소 풀에서 GCP 및 AWS에 대한 다른 탭을 볼 수 있으며, 퍼블릭 클라우드를 별도로 모니터링할 수도 있습니다.

트래픽 복제를 위한 **TLS 1.3** 및 **PubSub** 지원

지원 대상: Prisma Access 5.2 Preferred 및 Innovation

트래픽 복제를 사용하는 대규모 조직이라면 이를 구축하고 사용하는 데 다음과 같은 문제가 발생할 수 있습니다.

- 패킷 캡처(PCAP) 파일을 사용하는 도구는 많은 PCAP 파일을 처리하기 위해 버킷을 자주 쿼리해야 합니다. 해당 도구는 버킷에 오버헤드를 생성할 수 있으며 클라우드 공급자에 의해 사용이 제한될 수 있습니다.
- 포렌식 분석을 위해 PCAP 파일을 사용하는 경우 SSL 복호화 트래픽에 액세스하면 효율성이 더 높아지고 상당량의 트래픽이 TLS 1.3으로 암호화됩니다.

이러한 문제를 해결하기 위해 Prisma Access는 타사 도구의 효율성을 높이고 확장을 쉽게 할 수 있도록 다음과 같은 개선 사항을 제공합니다.

- **Pub/Sub** 알림 - Prisma Access는 새로운 PCAP 파일이 스토리지 버킷에 업로드되면 사전에 Pub/Sub 알림을 전송합니다. 새로운 PCAP 파일에 Pub/Sub 알림을 사용하면 버킷에 새 파일이 있을 때 알림을 제공하는 도구를 개발할 필요가 없습니다.
- **TLS 1.3** 복호화 지원 - Prisma Access는 PCAP 파일을 복호화할 때 TLS 1.3을 사용하여 트래픽에 대한 더 깊은 가시성을 제공합니다. 이 지원은 PCAP 파일에 SSL/TLS 복호화 정책 규칙 사용을 활성화한 원격 네트워크 구축에 적용됩니다.

Colo-Connect 보기 및 모니터링

지원 대상**:** Prisma Access 5.2 Preferred 및 Innovation

Colo-Connect는 Colo 기반 성능 허브 개념을 기반으로 구축되었으며, 기존 성능 허브에서 Prisma Access에 대한 레이어 2/3 연결과 함께 고대역폭 프라이빗 연결을 제공합니다. Colo-Connect는 클라우드 네이티브 GCP 상호 연결 기술을 활용하여 프라이빗 애플리케이션에 고대역폭 서비스 연결을 제공합니다. 모니터링 > 데이터 센터 > 서비스 연결로 이동하여 클라우드 상호 연결을 통해 하이브리드 클라우드 및 본부 데이터 센터에 대한 개인 연결을 확인하고 모니터링합니다.

Strata Cloud Manager 및 **Panorama**에서 **Prisma Access,** 데이터플레인**,** 애플리케이션 및 위협 콘텐츠 버전 보기

지원 대상**:** Prisma Access (Managed by Strata Cloud Manager) 5.2 Preferred 및 Innovation

Prisma Access(Strata Cloud Manager에서 관리됨) 구축에 대한 자세한 정보를 얻을 수 있도록 Strata Cloud Manager의 개요 페이지(관리 > 구성 > **NGFW** 및 **Prisma Access** > 개요)에 있는 소프트웨어 정보 영역과 Panorama의 Prisma Access 버전(**Panorama** > 클라우드 서비스 > 구성 > 서비스 설정)은 다음 정보를 제공합니다.

- Prisma Access 버전
- PAN-OS 데이터플레인 버전
- 릴리즈 유형(Preferred 또는 Innovation)
- 애플리케이션 및 위협 콘텐츠 버전

커밋리스 앱 온보딩을 위한 **ZTNA** 커넥터 지원

지원 대상**:** Prisma Access 5.2 Innovation

커밋리스 온보딩 개선 사을 통해 애플리케이션을 온보딩, 수정 또는 제거할 때 향상된 경험을 할 수 있습니다. 이전에 발생하던 5~10분 지연이 제거되어 프로세스 속도가 빨라집니다. 이제 애플리케이션 온보딩 시간이 1분도 채 걸리지 않으므로 애플리케이션을 빠르고 효율적으로 관리할 수 있습니다. 또한 ZTNA 커넥

터의 확장성이 향상되어 10,000개 이상의 애플리케이션을 관리하는 대규모 고객의 요구를 충족할 수 있습니다. 더 많은 애플리케이션을 온보딩할 수 있으므로 운영의 유연성과 효율성이 향상됩니다.

Prisma Access 5.2 및 5.2.1의 기본 동작에 대한 변경 사항

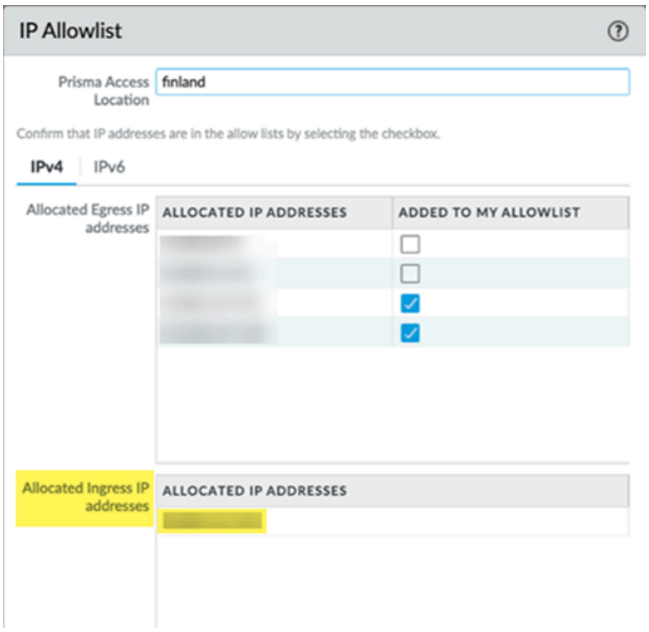
어디에서 사용할 수 있습니까?	무엇이 필요합니까?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 라이센스 ❑ Minimum Required Prisma Access Version 5.2 또는 5.2.1 Preferred 또는 Innovation

다음 섹션에서는 Prisma Access 5.2 및 Prisma Access 5.2.1 버전의 기본 동작에 대한 변경 사항을 자세히 설명합니다.

Prisma Access 5.2.1의 기본 동작에 대한 변경 사항

다음 표에서는 Prisma Access 5.2.1 버전의 기본 동작에 대한 변경 사항을 자세히 설명합니다.

구성품	변경
새로운 **Prisma Access** 구축을 위해 **IP** 최적화가 활성화됨	Prisma Access 테넌트의 더 빠른 온보딩을 가능하게 하고 IP 주소 허용 목록을 간소화하기 위해 새로운 Prisma Access 구축에는 IP 최적화가 활성화되어 있습니다. *IP* 최적화 구축은 퍼블릭*(*외부*)* 앱에 액세스하기 위해 IPv6를 지원하지 않지만 프라이빗 앱 액세스는 지원됩니다. 새로운 *Prisma Access* 구축을 위해 *IPv6*를 활성화하려면 *Palo Alto Networks* 계정 팀에 문의하십시오. 그러면 담당 계정 팀에서 요청을 수용하기 위해 *TAC* 케이스를 열어드립니다. 새로운 Prisma Access 구축을 설정하기 전에 모든 사용자가 6.1.4 이상, 6.2.3 이상 또는 6.3.0 이상의 GlobalProtect 앱 버전을 실행하고 있는지 확인하십시오. 새로운 *FedRAMP* 구축에는 *IP* 최적화가 활성화되어 있지 않습니다.
새로운 **Prisma Access(Strata Cloud Manager**에서 관리됨**)** 구축을 위해 기본 모바일 사용자 **- GlobalProtect IP** 주소 풀이 변경됨	새로운 Prisma Access(Strata Cloud Manager에서 관리됨) 모바일 사용자 - GlobalProtect 구축에는 새로운 기본 IP 주소 풀인 100.92.0.0/16이 있습니다. 이는 100.127.0.0/16의 기본 IP 주소 풀을 사용했던 이전 구축과 다른 점입니다. 이 RFC6598 풀은 모바일 사용자를 위한 프라이빗 앱 액세스를 포함한 대부분의 사용 사례에 사용할 수 있습니다. 더 많은 IP 주소가 필요하면 Prisma Access UI에서 추가할 수 있습니다.

구성품	변경
IP 최적화로 마이그레이션된 구축에 대한 **IP** 주소 통합	기존 Prisma Access에서 하나 이상의 지역이 IP 최적화로 마이그레이션되었고 Prisma Access 허용 목록을 사용하는 경우, 허용 목록에 추가한 일부 IP 주소가 Prisma Access의 할당된 송신 **IP** 주소 영역에서 할당된 수신 **IP** 주소 영역으로 이동되었습니다. 이러한 변경은 Prisma Access 5.2.1 인프라 업그레이드의 일환으로 IP 주소 통합이 이루어진 결과입니다. 네트워크는 여전히 이러한 IP 주소에 접근할 수 있으며 더 이상 이를 허용 목록에 추가할 필요가 없습니다. 

Prisma Access 5.2의 기본 동작에 대한 변경 사항

구성품	변경
PAN-OS 10.2.10 데이터플레인에 대한 업그레이드 고려 사항	Palo Alto Networks에서 Prisma Access 5.2 Preferred 기능을 지원하기 위해 PAN-OS 10.2.10으로 데이터플레인을 업그레이드하도록 선택한 경우, 업그레이드를 예약하기 전에 다음의 10.2 관련 변경 사항 및 업그레이드 고려 사항을 알고 있어야 합니다. • 기본 동작에 대한 변경 사항 • 업그레이드/다운그레이드 고려 사항 • PAN-OS 10.2.10 및 기타 PAN-OS 10.2 릴리즈의 해결된 문제
PAN-OS 11.2.3 데이터플레인에 대한 업그레이드 고려 사항	Palo Alto Networks에서 Prisma Access 5.2 Innovation 기능을 지원하기 위해 PAN-OS 11.2.3으로 데이터플레인을 업그레이드하도록 선택한 경

구성품	변경
	우, 업그레이드를 예약하기 전에 다음의 11.2 관련 변경 사항 및 업그레이드 고려 사항을 알고 있어야 합니다. • 기본 동작에 대한 변경 사항 • 업그레이드/다운그레이드 고려 사항 • PAN-OS 11.2.2 및 기타 PAN-OS 11.2 릴리즈의 해결된 문제
Prisma Access 5.1의 웹 인터페이스 변경 사항	최대 25,000개의 원격 네트워크를 지원하기 위해 일부 Prisma Access (Managed by Strata Cloud Manager) 웹 인터페이스가 Prisma Access 5.1에서 변경되었습니다. 자세한 내용은 25,000개의 원격 네트워크 및 50,000개의 IKE 게이트웨이 지원을(를) 참조하십시오.

Prisma Access 알려진 문제

어디에서 사용할 수 있습니까?	무엇이 필요합니까?
• Prisma Access (Managed by Panorama)	❑ Prisma Access 라이센스 ❑ Minimum Required Prisma Access Version 5.2 또는 5.2.1 Preferred 또는 Innovation

Prisma Access에는 다음과 같은 알려진 문제가 있습니다.

문제 ID	설명
AIOPS-11286	Colo-Connect를 활성화한 경우 멀티테넌트 환경의 서브테넌트에서 교차 연결 및 연결 관련 정보가 최신 상태가 아닐 수 있습니다.
CYR-47139	ZTNA 커넥터 애플리케이션 블록 또는 커넥터 블록이 명시적 프록시 주소와 충돌하는 RFC6598 주소로 구성된 경우 ZTNA 커넥터 - 명시적 프록시 통합에서 ZTNA 커넥터가 비활성화됩니다. 해결 방법: ZTNA 커넥터를 명시적 프록시와 통합한 경우 "100.64.0.0/15", "100.72.0.0/15" 또는 "100.88.0.0/15" 서브넷을 다음에 대해 사용하지 마십시오. • ZTNA 커넥터 애플리케이션 블록 • ZTNA 커넥터 커넥터 블록 • 애플리케이션과 연결한 ZTNA 커넥터에 구성된 IP 서브넷
CYR-46759	DNS 쿼리에 대한 UDP 설정이 명시적 프록시에서 적용되지 않습니다.
CYR-46627	서비스 연결을 통한 기본 경로 수락이 활성화된 경우 명시적 프록시가 지원되지 않습니다.
CYR-46445	NAT 디바이스에서 처리된 포트 6081과 관련된 일시적인 오류로 인해 ZTNA 커넥터가 정지되었습니다.

문제 ID	설명
	해결 방법: ZTNA 커넥터 트래픽이 NAT 디바이스를 통과하는 경우 NAT 세션이 포트 6081에 매핑되지 않았는지 확인합니다.
CYR-46349	중국에서 트래픽 스티어링으로 명시적 프록시가 있는 원격 네트워크를 사용하는 경우 URL 범주를 사용하여 트래픽 스티어링 규칙을 구성하지 마십시오.
CYR-46191	프라이빗 애플리케이션 액세스가 활성화된 상태로 명시적 프록시가 구성되고 ZTNA 커넥터가 구성에 추가되면 Panorama 또는 Strata Cloud Manager에서 다른 커밋이 필요할 수 있습니다. 해결 방법: Prisma Access를 관리하는 Panorama 또는 Strata Cloud Manager에서 명시적 프록시 구성을 약간 수정하고 변경 사항을 푸시합니다.
CYR-46170	DDNS를 활성화하고 나중에 모바일 사용자에게 서비스 서브넷 변경 사항을 푸시하는 경우 DDNS가 변경 사항을 선택할 수 있도록 모바일 사용자 게이트웨이에서 DDNS 플러그인도 다시 시작해야 합니다. 해결 방법: 다음 명령을 입력합니다. **`debug software restart process pl-ddns`**
CYR-46145	ZTNA 커넥터 및 해당 애플리케이션이 온보딩된 기존 Prisma Access 테넌트에 대해 Prisma Access 자율 시스템 번호 또는 Prisma Access 인프라 서브넷이 업데이트되면 업데이트 후 약 5분 동안 중단이 발생합니다.
CYR-46093	구축에서 최대 25,000개의 원격 네트워크와 50,000개의 IKE 게이트웨이를 지원하는 기능을 구현한 경우 집계 대역폭 사용 통계에 사용 통계 대신 `No data for the specified time period`가 표시됩니다.
CYR-45440	관리자 역할을 구성할 때 액세스 정보가 항상 올바르게 저장되는 것은 아닙니다. 해결 방법: 관리자 역할 영역에서 플러그인/클라우드 서비스 플러그인을 두 번 이상 클릭하여 액세스 정보가 올바르게 저장되었는지 확인합니다. 확인을 클릭하고 열기를 다시 클릭하여 변경 사항이 저장되었는지 확인합니다.

문제 **ID**	설명
CYR-45415	클라우드 서비스 플러그인에 대한 읽기 전용 또는 비활성화된 액세스 권한이 있는 관리자는 템플릿, 디바이스 그룹, 클라우드 서비스 구성 제거, 클라우드 서비스 플러그인 설치 제거 및 구성 파일 로드와 같은, 클라우드 서비스 동작에 영향을 주는 클라우드 서비스 플러그인 외부의 구성을 수정할 수 있습니다.
CYR-45517	Colo-Connect 탭에서 읽기 전용 사용자는 온보딩 항목을 삭제할 수 있습니다.
CYR-45440	관리자 역할을 구성할 때 액세스 정보가 항상 올바르게 저장되는 것은 아닙니다. 해결 방법: 관리자 역할 영역에서 플러그인/클라우드 서비스 플러그인을 두 번 이상 클릭하여 액세스 정보가 올바르게 저장되었는지 확인합니다. 확인을 클릭하고 열기를 다시 클릭하여 변경 사항이 저장되었는지 확인합니다.
CYR-45415	클라우드 서비스 플러그인에 대한 읽기 전용 또는 비활성화된 액세스 권한이 있는 관리자는 템플릿, 디바이스 그룹, 클라우드 서비스 구성 제거, 클라우드 서비스 플러그인 설치 제거 및 구성 파일 로드와 같은, 클라우드 서비스 동작에 영향을 주는 클라우드 서비스 플러그인 외부의 구성을 수정할 수 있습니다.
CYR-44433	성공 상태의 원격 네트워크 작업이 성공에서 보류 중 상태로 변경될 수 있습니다.
CYR-44202	클라우드 서비스 플러그인에 대한 읽기 전용 액세스 권한이 있는 관리 사용자는 RBI 탭을 수정할 수 있습니다.
CYR-43425	서비스 연결이 RFC 6598 주소를 사용하는 경우 해당 서비스 연결에 서비스에 대한 아웃바운드 경로를 지정할 수 없습니다.
CYR-43400 **Prisma Access 5.2.0**에서 이 문제가 해결되었습니다. **Prisma Access 5.2.0** 해결된 문제의 내용을 참조하십시오.	사용자 **ID** 유지가 선택된 ZTNA 커넥터 그룹에서 온보딩된 커넥터는 내부 인터페이스에서 데이터 센터 앱으로의 작업 > 진단 > 핑**(ping)**이 작동하지 않습니다.

문제 **ID**	설명
CYR-43262 **Prisma Access 5.2.0**에서 이 문제가 해결되었습니다. **Prisma Access 5.2.0** 해결된 문제의 내용을 참조하십시오.	원격 네트워크 온보딩에 대한 원격 네트워크 API 요청은 BGP 구성이 페이로드에 포함된 경우 클라우드 서비스 플러그인에서 커밋 유효성 검사 오류를 반환합니다.
CYR-43222 **Prisma Access 5.2.0**에서 이 문제가 해결되었습니다. **Prisma Access 5.2.0** 해결된 문제의 내용을 참조하십시오.	사용자 ID 기반 ZTNA 커넥터 그룹에 할당된 애플리케이션 대상은 **icmp ping**의 프로빙 유형을 지원하지 않습니다 해결 방법: 애플리케이션 유형에 대한 프로빙 유형으로 **tcp ping** 또는 없음을 선택합니다.
CYR-43147	자동 크기 조정된 ZTNA 커넥터의 경우 축소 중에, 축소로 표시된 ZTNA 커넥터에서 처리하는 기존의 긴 수명 세션이 조기에 삭제될 수 있습니다. 축소 후 새 트래픽 세션에는 영향을 미치지 않습니다.
CYR-43132	Panorama에서 서브테넌트를 생성하는 동안 모바일 사용자 구성을 비워 두면 원격 네트워크에 대한 단위를 구성할 수 없으며 그 반대의 경우도 마찬가지입니다.
CYR-42919**Prisma Access 5.2.1**에서 이 문제가 해결되었습니다. **Prisma Access 5.2.1** 해결된 문제의 내용을 참조하십시오.	ZTNA 커넥터에서 커넥터 IP 블록을 수정하거나 삭제하려고 할 때 커밋 및 푸시 후에 변경 사항이 적용되지 않습니다. 해결 방법: 커밋 및 푸시 작업을 두 번 더 수행하여 변경 사항을 적용합니다.
CYR-42312	NAT를 통한 사용자 ID는 Colo-Connect에서 지원되지 않습니다.
CYR-42259	명시적 프록시 프라이빗 앱 액세스는 RFC6598이 활성화된 경우 작동하지 않습니다.
CYR-42244	인수 합병을 위한 비즈니스 연속성 기능의 일부로 Prisma Access 게이트웨이 이름 변경을 요청하는 경우 업데이트된 FQDN이 Strata Cloud Manager 또는 Panorama에서 표시되지 않습니다. 해결 방법: Palo Alto Networks 계정 팀에 연락하여 SRE 케이스를 열어 게이트웨이의 FQDN을 업데이트합니다.
CYR-42188	명시적 프록시 프라이빗 앱 액세스를 사용하는 경우 TCP를 통한 DNS가 작동하지 않습니다. 그러나 UDP를 통한 DNS는 올바르게 작동합니다.

문제 **ID**	설명
CYR-42130	Colo-Connect 라우팅 정보가 서비스 가용성 명령 영역에 표시되지 않습니다.
CYR-42018	IP 최적화를 활성화한 경우 GlobalProtect에 대한 TLS 1.3이 지원되지 않습니다. 해결 방법: 최대 TLS 버전 1.2를 사용합니다.
CYR-41990	IPv6-to-IPv6 또는 IPv6-to-IPv4 소스 또는 대상 트래픽은 URL 필터링 작업 계속 및 재정의를 지원하지 않습니다.
CYR-41838	원격 네트워크의 이그레스(Egress) IP 주소 - Prisma Access API를 사용하여 검색할 때 고성능 구축이 두 번 표시됩니다. 해결 방법: 중복된 IP 주소를 무시합니다.
CYR-41813	ZTNA 커넥터 온보딩은 스위스, 프랑스, 카타르 또는 대만 위치에서 지원되지 않습니다. 해결 방법은 없습니다.
CYR-41228	IP 최적화를 활성화한 경우 SP 상호 연결 기능을 사용할 수 없습니다.
CYR-41067	UI의 Prisma Access 버전 영역에 잘못된 Prisma Access 버전이 표시됩니다. Strata Cloud Manager에서 버전은 관리 > 구성 > **NGFW** 및 **Prisma** 액세스 > 개요 > **Prisma Access** 버전에 표시됩니다. Panorama Managed Prisma Access에서 버전은 **Panorama** > 클라우드 서비스 > 구성 > 서비스 설정 > **Prisma Access** 버전에 표시됩니다.
CYR-40503	IPv6는 남아프리카 공화국 중부 및 캐나다 서부 지역에서 지원되지 않습니다.
CYR-40404	커넥터 그룹의 일부 ZTNA 커넥터에서 애플리케이션에 액세스할 수 없는 경우 커넥터 그룹에 대해 와일드카드와 일치하는 FQDN 대상이 검색되지 않을 수 있습니다. 지정된 그룹의 모든 커넥터는 DNS를 사용하여 애플리케이션을 확인하고 애플리케이션이 그룹에서 자동으로 검색되도록 애플리케이션에 액세스할 수 있어야 합니다. 해결 방법: 애플리케이션 개체를 Strata Cloud Manager에서 필요한 커넥터 그룹에 연결합니다.

문제 **ID**	설명
CYR-39930	Cortex Data Lake 로그는 IP 최적화 기능이 활성화된 테넌트에서 내보내지지 않습니다.
CYR-39795	클라우드 서비스 플러그인을 설치한 후에는 명시적 프록시가 활성화되지 않은 경우에도 __cloud_services 사용자가 명시적 프록시 Kerberos 서버 프로파일(default_server_profile)을 설치합니다. 해결 방법: 변경 사항을 무시합니다.
CYR-39551	인증 유형 TSIG로 Prisma Access 동적 DNS를 설정하는 경우 TSIG 키 파일에 대한 .key 파일을 업로드해야 합니다. 키 파일은 콘텐츠에 ASCII가 아닌 문자가 있는 경우 유효하지 않은 것으로 간주됩니다. ASCII가 아닌 문자로 TSIG 인증을 위한 .key 파일을 제공하고 확인을 클릭하면 #### `.key#` ### ####### `.` 오류가 표시됩니다. 해결 방법: 유효한 tsig 키 파일을 제공하십시오.
CYR-39153	ZTNA 커넥터 그룹으로 업그레이드를 수행할 때 업그레이드 작업 중에 간헐적으로 오류가 발생할 수 있습니다. 예를 들어, 영향을 받는 커넥터 중 일부가 나중에 성공적으로 업그레이드되더라도 업그레이드 상태는 `partial_success` 또는 `failed`로 표시됩니다. 해결 방법: 나중에 커넥터 그룹 업그레이드를 다시 시도합니다. ZTNA 커넥터는 커넥터 그룹의 적절한 상태를 다시 확인하고 제공합니다.
CYR-39148	Colo-Connect를 구성할 때 Colo Connect 디바이스 그룹에 대한 커밋 및 푸시 작업이 간헐적으로 실패할 수 있습니다. 해결 방법: Colo-Connect 디바이스 그룹에 대한 커밋 및 푸시 작업을 재시도합니다.
CYR-39028	ZTNA 커넥터를 4.1에서 그 이상의 Prisma Access 버전으로 업그레이드하고 ZTNA 커넥터 애플리케이션 풀이 RFC6598 주소 공간(100.64.0.0/16 및 100.65.0.0/16) 내에 구성된 경우 MU-SPN에서 ZTNA 커넥터 트래픽이 차단될 수 있습니다. 해결 방법: Prisma Access 팀에 문의하여 모든 Prisma Access 테넌트의 SaaS 에이전트 버전을 업데이트하십시오.

문제 **ID**	설명
CYR-38619	스위스와 프랑스에서 온보딩된 테넌트는 ZTNA 커넥터를 사용할 수 없습니다.
CYR-38120	사용 가능한 모든 위치가 모바일 사용자 - 명시적 프록시 설정 페이지의 목록 보기에 표시되지는 않습니다. 해결 방법: 맵 뷰를 사용하여 누락된 위치를 선택합니다.
CYR-38076	올바른 EBGP 라우터 주소가 원격 네트워크 세부 정보 페이지(원격 네트워크 설정 > 원격 네트워크 > **EBGP** 라우터)에 표시되지 않고, 대신 원격 네트워크의 루프백 IP 주소를 표시합니다.
CYR-37983	모바일 사용자(GlobalProtect 사용자)에 대해 IPv6를 활성화한 경우 HIP 보고서를 검색하면 충돌이 발생합니다. 해결 방법: GlobalProtect 클라이언트가 IPv6를 사용하는 경우 클라이언트의 IPv6 주소를 사용하여 HIP 보고서를 실행합니다. GlobalProtect 클라이언트가 IPv4 전용인 경우 클라이언트의 IPv4 주소를 사용하여 HIP 보고서를 실행합니다.
CYR-37923	새 URL 범주 또는 보안 규칙 또는 EDL을 생성한 후 RBI 보안 규칙 연결에서 해당 개체를 사용하기 전에 로컬 Panorama 커밋이 필요합니다.
CYR-37906	기존 와일드카드 개체에 대한 포트를 업데이트할 때 포트 사이에 공백을 넣으면 `500 internal server` 오류가 표시됩니다. 해결 방법: 포트 사이에 공백을 두지 마십시오. 예를 들어, **`1-2, 80, 100-300`** 대신, **`1-2,80,100-300`**을 사용하십시오.
CYR-37887	30일 평가판의 일부로 ZTNA 커넥터를 사용 중이고 라이센스를 구매하지 않은 경우 **ZTNA** 커넥터 활성화 버튼을 클릭하면 `Something went wrong` 메시지가 표시되면서 온보딩이 실패할 수 있습니다. 해결 방법: UI를 새로 고쳐 ZTNA 커넥터 기능의 온보딩을 완료합니다.
CYR-37826	둘 이상의 ZTNA 커넥터 애플리케이션에 동일한 FQDN이 있는 경우 `Application Custom rule conflict` 메시지가 SD-WAN 포털에 표시될 수 있습니다.

문제 **ID**	설명
	해결 방법: 이 메시지는 가짜이며 무시할 수 있습니다.
CYR-37797	상태 페이지는 플러그인 업그레이드 후 일회성 암호(OTP)를 요청합니다. 해결 방법: 만료된 라이센스 키를 삭제하고, Panorama 인증서를 삭제하고, 라이센스를 검색하고, 라이센스 검색 후 라이센스 키가 유효한지 확인합니다. 그런 다음 OTP를 생성하여 확인합니다.
CYR-37755	ZTNA 커넥터에서 와일드카드 대상을 구성하고 해당 대상의 결과로 검색되어 FQDN 대상에 추가된 애플리케이션의 포트를 변경하려고 하면 이름이 너무 길다는 오류가 표시됩니다. 해결 방법: 애플리케이션 이름은 최대 32자까지 가능하지만 포트 번호를 변경하면 ZTNA 커넥터 인프라에서 이름이 너무 길어집니다. 이 오류가 발생하면 애플리케이션에 더 짧은 이름을 지정해 보십시오.
CYR-37706	명시적 프록시를 사용하는 경우 과도한 양의 위협 로그가 표시됩니다. 해결 방법: 위협 로그를 무시합니다. 이러한 로그는 명시적 프록시 기능에 영향을 주지 않습니다.
CYR-37673	**Panorama** > 클라우드 서비스 > 상태 > 상태 > 원격 브라우저 격리 > 활성 격리 세션 링크를 클릭하면 Prisma Access Cloud Management 또는 Strata Cloud Manager의 모니터 > 구독 사용 페이지가 열리지 않습니다.
CYR-37500	원격 네트워크에 대해 IPv6를 활성화한 경우 에지 로케이션에 대해 공용 IPv6 주소가 표시되지 않습니다.
CYR-37466	Colo-Connect를 활성화하는 경우 VLAN에서 BFD(양방향 포워딩 감지)를 활성화하지 마십시오.
CYR-37356	라이센스의 유예 기간을 포함하여, 만료된 앱 가속 라이센스를 갱신하는 경우 갱신이 즉시 적용되지 않습니다. 해결 방법: 라이센스 갱신 후 약 1시간 정도 기다렸다가 앱 가속을 사용하십시오.
CYR-37290	ZTNA 커넥터를 온보딩할 때 `declaim requested by root` 오류를 수신합니다.

문제 **ID**	설명
	해결 방법: 오류가 발생한 커넥터를 삭제하고 새 커넥터를 만듭니다.
CYR-37227	그룹이 없어도, IP 서브넷 기반 커넥터 그룹 생성이 `group already exists` 메시지와 함께 실패하는 경우가 있습니다. 해결 방법: IP 서브넷 기반 커넥터 그룹에 다른 이름을 사용합니다.
CYR-37208	Prisma Access Clean Pipe를 사용할 때 네트워크 세부 정보 페이지(**Panorama** > 클라우드 서비스 > 상태 > 상태 > 네트워크 세부 정보)에 Clean Pipe 항목이 표시되지 않습니다.
CYR-36749	Netflow와 관련된 ZTNA 커넥터 플로우 로그는 Strata Cloud Manager 로그 뷰어에 표시되지 않을 수 있습니다.
CYR-35506	테넌트에 대해 IPv6를 활성화한 경우 테넌트를 삭제해도 할당된 IPv6 접두사가 해제되지 않으며 해당 접두사를 다시 사용할 수 없습니다. 해결 방법: IPv6를 활성화한 테넌트를 삭제하지 마십시오.
CYR-34999	Panorama Prisma Access 테넌트의 경우 ZTNA 커넥터가 온보딩되면 서비스 연결에 대한 프로비저닝 진행 상황(**Panorama** > 클라우드 서비스 > 상태 > 상태 > 서비스 연결 > 프로비전 진행 상황)에 ZTNA 커넥터 및 서비스 연결 모두에 대한 프로비저닝 진행 상황이 표시됩니다.
CYR-34770	모바일 사용자 - GlobalProtect 구축을 위한 Prisma Access에서 여러 개의 포털을 구성하는 경우 모든 포털의 클라이언트 인증에서 인증 프로파일을 구성해야 합니다. 하나 이상의 인증 프로파일을 구성하지 않으면 인증 쿠키가 생성되지 않고 다중 포털 기능이 원하는 대로 작동하지 않습니다.
CYR-34720	10.1.x를 실행하는 Panorama를 사용하여 클라우드 서비스 플러그인으로 Prisma Access를 관리할 때 GlobalProtect DDNS 기능이 작동하지 않습니다.
CYR-33877	명시적 프록시 설정 중에 인증 건너뛰기를 선택하여 주소 개체에 대한 인증을 건너뛴 다음, 해당 주소 개체에 대해 인증 건너뛰기를 선택 해제하여 인증을 활성화하려는 경우, 변경

문제 **ID**	설명
	후 변경 사항을 커밋 및 푸시하는 데 최대 24시간이 걸릴 수 있습니다.
CYR-33471	멀티테넌시를 활성화하는 경우 새 서브테넌트를 생성하고, 모바일 사용자-GlobalProtect, 원격 네트워크 및 Colo-Connect 디바이스 그룹을 구성한 다음, Colo-Connect 서브넷 및 VLAN을 구성하고, 부분 커밋을 수행하면 `Unable to retrieve last in-sync configuration for the device` 오류와 함께 실패합니다. 해결 방법: Colo-Connect를 처음 구성할 때 부분 커밋 대신 커밋 및 푸시 작업을 수행합니다.
CYR-33454	멀티테넌트 구축에서 Prisma Access를 구성하고 커밋 및 푸시를 수행한 다음, Colo-Connect를 구성하면 변경 사항을 커밋 및 푸시하는 선택 항목이 회색으로 표시됩니다. 해결 방법: 커밋 > **Panorama**에 커밋을 클릭한 다음, 커밋 > 디바이스에 푸시 및 선택 수정을 클릭하고 **Colo-Connect**가 푸시 범위에서 선택되어 있는지 확인한 후, 커밋 및 푸시 작업을 재시도합니다.
CYR-33199	Kerberos 인증 사용자에 대해 현재 사용자 수 및 90일 사용자 수가 올바르지 않습니다.
CYR-33145	모든 서비스 유형에 대한 Prisma Access 라이센스가 만료되면 모두 커밋 작업이 일반 `Commit Failed` 오류 메시지와 함께 실패합니다. 해결 방법: 커밋을 수행하기 전에 모든 Prisma Access 라이센스가 만료되지 않았는지 확인하십시오.
CYR-32687	에이전트 또는 Kerberos 인증이 명시적 프록시와 함께 사용되는 경우, EDL, **IP** 와일드카드 마스크 및 **FQDN** 유형의 주소 개체, 동적 주소 그룹이 암호 해독 정책에서 작동하지 않습니다. 해결 방법: 암호 해독 정책에서 IP 넷마스크, IP 범위 또는 주소 그룹의 주소 개체를 사용합니다.
CYR-32666	Colo-Connect 구성이 포함된 이전에 저장된 Panorama 구성을 가져오거나 이전에 저장한 구성에서 되돌릴 때 다음 조건이 있는 경우 오류가 발생합니다.

문제 **ID**	설명

	• Colo-Connect 서비스 연결이 구성된 구성을 로드하려고 합니다.
	• 비어 있는 Prisma Access 구성을 로드하려고 합니다.
	• 이전에 저장한 구성에서 되돌리려고 하며, 다음과 같은 조건이 있습니다.
	  • Colo-Connect 구성(서비스 연결 포함)이 현재 구성에 있으며 되돌리려는 구성에는 Colo-Connect 구성이 없습니다.
	  • Colo-Connect 구성이 현재 구성에 없으며 되돌리려는 구성에는 Colo-Connect 구성(서비스 연결 포함)이 있습니다.
	  • Colo-Connect 구성(서비스 연결 포함)이 현재 구성에 있으며 되돌리려는 구성에도 있습니다.
	해결 방법: 해당 VLAN이 활성 상태가 아니면 Colo-Connect 서비스 연결을 온보딩할 수 없습니다. Panorama 이미지를 내보내거나 되돌리기 전에 Colo-Connect 서비스 연결을 삭제합니다. 그런 다음, 새 이미지를 가져온 후 Colo-Connect 서비스 연결을 다시 만듭니다.

CYR-32661	GlobalProtect가 프록시 모드 또는 터널 및 프록시 모드로 연결된 경우 사용자 로그인은 모바일 사용자 - 명시적 프록시에서 지난 90일 동안 로그인한 사용자 수 또는 현재 사용자 수에 포함되지 않습니다.
CYR-32564	ZTNA 커넥터 앱 트래픽은 기본 URL 범주를 사용하는 경우 위협으로 감지되고 Prisma Access 클라우드 관리를 위해 삭제됩니다. 해결 방법: 필요에 따라 다음 단계 중 하나 이상을 수행합니다. **1.** 사용자 정의 URL 범주를 만들고 ZTNA 커넥터에 대해 온보딩된 애플리케이션에 대한 애플리케이션 FQDN을 추가합니다. **2.** 기본 프로파일 그룹을 사용하는 경우 새 그룹을 복제하고 1단계에서 만든 사용자 정의 URL 범주를 연결합니다. 사용자 정의 프로파일 그룹을 사용하는 경우 1단계에서 만든 사용자 정의 URL 범주를 연결합니다. **3.** 복제된 프로파일 그룹 또는 사용자 정의 프로파일 그룹(2단계에서)을 ZTNA 커넥터 애플리케이션으로 향하

문제 **ID**	설명
	는 트래픽 허용을 위해 생성한 보안 정책에 연결해야 합니다.
CYR-32511	IPv6를 사용하지 않도록 설정한 경우에도 IPv6 DNS 주소를 구성할 수 있습니다.
CYR-32431	명시적 프록시를 구성할 때 인증 설정에서 신뢰할 수 있는 소스 주소 값을 추가하고 다른 설정을 구성한 다음, 인증 설정 탭으로 돌아가면 신뢰할 수 있는 소스 주소가 올바르게 표시되지 않을 수 있습니다. 해결 방법: Prisma Access를 관리하는 Panorama를 새로 고친 다음, 인증 설정 탭으로 돌아가 주소를 확인합니다.
CYR-32191	ZTNA 커넥터는 멀티테넌트 환경에서 지원되지 않습니다.
CYR-32004	현재 Prisma Access에서 지원되는 IPSec 프로파일 수의 제한으로 인해 ZTNA 커넥터를 배포할 때 테넌트당 최대 100개의 커넥터 VM을 온보딩할 수 있습니다.
CYR-31603	두 개의 인터페이스가 있는 ZTNA 커넥터는 AWS Auto Scale에 대해 활성화된 커넥터 그룹에서 지원되지 않습니다. 이는 두 인터페이스를 동일한 서브넷에 연결하는 AWS Auto Scale 그룹 제한 때문입니다. 자세한 내용은 이 기사의 내용을 참조하십시오. 해결 방법**:** 두 개의 인터페이스가 있는 ZTNA 커넥터는 AWS Auto Scale에 대해 활성화되지 않은 커넥터 그룹에서 지원됩니다. 두 개의 인터페이스가 있는 모든 ZTNA 커넥터가 AWS Auto Scale에 대해 활성화되지 않은 커넥터 그룹에 포함되어 있는지 확인합니다.
CYR-31187	상시 접속된 인터넷 보안 기능을 위해 GlobalProtect에서 Prisma Access 명시적 프록시 연결을 사용하려는 경우 모바일 사용자 - GlobalProtect 및 모바일 사용자 - 명시적 프록시 모두에 커밋 및 푸시를 수행하지 않으면 기본 PAC 파일 URL이 제대로 채워지지 않습니다. 해결 방법: 커밋 및 푸시하려는 경우, GlobalProtect에서 Prisma Access Explicit Proxy 연결을 구성할 때 푸시 범위에서 모바일 사용자 - GlobalProtect 및 모바일 사용자 - 명시적 프록시를 모두 선택해야 합니다.

문제 **ID**	설명

CYR-30414	테넌트가 하나뿐인 멀티테넌트 구축에서 여러 포털을 활성화한 다음, 해당 단일 테넌트에서 여러 포털 기능을 비활성화하면 UI에서 두 포털을 모두 볼 수 있습니다.
	
	해결 방법: Prisma Access를 관리하는 Panorama에서 CLI 세션을 열고 다음 명령을 입력한 다음, Panorama에서 로컬 커밋을 수행합니다.
	
	`set plugins cloud_services multi-tenant tenants` <*tenant_name*> `mobile-users multi-portal-multi-auth no`
	
	`request plugins cloud_services gpcs multi-tenant tenant-name` <*tenant_name*> `multi_portal_on_off`

CYR-30044	사전정의된 EDL이 새 명시적 프록시 구축의 블록 설정 목록에 채워지지 않습니다. 해결 방법: 명시적 프록시 구축을 온보딩하고, 커밋 및 푸시 작업을 수행한 다음, 돌아가서 블록 설정에서 EDL을 업데이트합니다.
CYR-29964	CSR(인증서 서명 요청)을 재사용하여 인증서를 생성하려고 하면 `"Requested entity already exists"` 오류가 표시됩니다. 해결 방법: CSR을 재사용하지 마십시오.
CYR-29933	**`verdicts:all -X "DELETE"`** API 호출을 시간당 두 번 이상 사용하려고 하면 `{"code" :8, "message" : "Too many requests"` 오류가 표시됩니다. 해결 방법: 이 API 호출을 시간당 두 번 이상 사용하지 마십시오.
CYR-29700	멀티테넌트 Prisma Access Panorama Managed 멀티테넌트 구축에서 여러 GlobalProtect 포털을 구성하는 경우, 사용자 이름별로 변경 사항을 커밋하면 실패하고 `"global-protect-portal-8443 should have the value "GlobalProtect_Portal_8443" but it is [None"` 오류가 표시됩니다.

문제 **ID**	설명
	해결 방법: 여러 GlobalProtect 포털을 활성화했고 Prisma Access 멀티테넌트 구축이 있는 경우 사용자별로 커밋하는 대신 모두 커밋 작업을 수행합니다.
CYR-29160	Prisma Access를 관리하는 파노라마가 FIPS 모드로 구성되어 있고 **GlobalProtect** 앱 로그 수집 및 자율 **DEM**을 위한 인증서 생성을 선택하면 인증서가 다운로드되지 않습니다. 해결 방법: Prisma Access 데이터 플레인이 10.2.4로 업그레이드되기 전까지는 FIPS 모드의 Panorama 어플라이언스에서 이 기능을 사용할 수 없습니다.
CYR-26112	Net Interconnect 라이센스가 없는 경우 극장의 모든 원격 네트워크는 완전히 메시되지만 극장에서 서비스 연결을 온보딩하지 않은 경우 다른 극장의 원격 네트워크에서 원격 네트워크에 연결할 수 없습니다. 해결 방법: Net Interconnect 라이센스를 구입하거나 극장에서 서비스 연결을 온보딩하여 원격 네트워크가 다른 극장과 통신하도록 합니다.

동적 권한 액세스에 대한 알려진 문제

문제 **ID**	설명
PANG-4881	사용자가 Prisma Access 에이전트를 인증하는 데 사용한 웹 브라우저가 열려 있으면 웹 브라우저에서 Prisma Access 에이전트로의 트래픽이 포워딩 프로파일이 구성되는 방식에 관계없이 터널을 통해 전송됩니다.
PANG-4870	Prisma Access 에이전트가 설치된 macOS 디바이스에서 Prisma Access 에이전트의 보안 확장에 대한 전체 디스크 액세스 권한을 제거하면(이전에 전체 디스크 액세스 권한을 부여한 후) Prisma Access 에이전트가 비활성화 모드에서 멈춥니다. 해결 방법**:** 시스템 설정 > 개인정보 보호 및 보안 > 전체 디스크 접근 권한을 선택하고 앱 목록에서 **securityExtension**을 활성화하여 보안 확장에 액세스 권한을 부여합니다.

문제 **ID**	설명
PANG-4825	포워딩 프로파일을 구성할 때 소스 애플리케이션, 대상 도메인 및 IP 주소(경로)에 대해 많은 수의 포워딩 규칙을 구성하면 CPU 사용률이 높아질 수 있는 문제가 있습니다. 해결 방법: 소스 애플리케이션, 대상 도메인 및 IP 주소에 대해 100개를 초과하는 포워딩 규칙을 구성하지 마십시오.
NETVIS-1363	Strata Cloud Manager에 대한 Insights에서 사용자 세부 정보 페이지의 프로젝트 연결 내역 보기에는 프로젝트 이름만 표시되며 Prisma Access 에이전트 사용자가 연결된 경우 다른 세부 정보는 표시되지 않습니다. 사용자가 연결되지 않은 경우 프로젝트 연결 내역은 비어 있습니다.
NETVIS-1293	Insights에서 시간 범위가 **3**시간 경과, **1**시간 경과 및 **15**분 경과로 설정되면 프로젝트 연결 내역이 올바른 데이터를 표시하지 않습니다.
NETVIS-1263	Insights에서 프로젝트 탭에 나열된 연결된 사용자 수가 정확하지 않을 수 있습니다. 경우에 따라 프로젝트 탭의 연결된 사용자 수가 사용자 탭의 사용자 수와 일치하지 않을 수 있습니다. 예를 들어, 동일한 사용자가 서로 다른 디바이스의 두 프로젝트에 연결된 경우 프로젝트 탭의 연결된 사용자 수가 사용자 탭의 사용자 수와 일치하지 않습니다.
NETVIS-1207	Insights의 프로젝트 탭에는 프로젝트에 대해 구성된 IP 풀이 모두 표시되지는 않습니다. 사용 중인 IP 풀만 표시됩니다.
EPM-1589	포워딩 프로파일을 구성할 때 Strata Cloud Manager가 와일드카드 문자로 IP 주소를 구성하도록 허용해도 **`10.*.*.*`**와 같은 대상 IP 주소의 와일드카드 문자 사용은 포워딩 프로파일에서 동작 불일치를 유발하므로 지원되지 않습니다.
EPM-1399	Strata Cloud Manager의 동적 권한 액세스 페이지의 프로젝트 탭에 있는 프로젝트 이름 변경이 현재 지원되지 않습니다. 해결 방법**:** 프로젝트 이름을 바꾸려면 기존 프로젝트를 삭제하고 액세스 에이전트 푸시 구성을 수행한 다음, 프로젝트를 새 이름으로 만들고 액세스 에이전트 푸시 구성을 수행합니다.

문제 **ID**	설명
EPM-646	동적 권한 액세스가 활성화된 Prisma Access 테넌트에서 먼저 프로젝트를 구성하지 않고 Prisma Access 에이전트 인프라 구성을 푸시하려고 하면 구성 푸시가 실패합니다. 해결 방법: 푸시 구성을 수행하기 전에 하나 이상의 프로젝트를 구성합니다.
DRS-4691	텍스트 검색 옵션을 사용하여 Cloud Identity Engine 또는 Strata Cloud Manager에서 사용자 그룹을 검색할 때 사용자 그룹 이름을 큰따옴표로 묶습니다. 예를 들어, EXAMPLE.User_Group이라는 사용자 그룹을 검색하는 경우 "EXAMPLE.User_Group"을 입력합니다.
DRS-4406	Strata Cloud Manager에서 프로젝트를 구성할 때 사용자 그룹 이름을 부분적으로 입력하면 사용자 그룹을 검색할 수 없습니다. 해결 방법**:** 사용자 그룹을 검색하려면 전체 사용자 그룹 이름을 입력합니다.
DOCS-5681	동적 권한 액세스 활성화 테넌트에서 ZTNA 커넥터를 활성화하는 것은 Prisma Access 5.2에서 지원되지 않습니다. 동적 권한 액세스 활성화 테넌트에서 ZTNA 커넥터를 활성화하면 라우팅에 문제가 발생할 수 있습니다. Strata Cloud Manager는 생성된 ZTNA 커넥터의 삭제를 지원하지 않기 때문에 서비스가 영향을 받을 수도 있습니다.
DOCS-5611	동적 권한 액세스에 대한 Cloud Identity Engine에서 사용자 그룹 매핑을 승인할 때 Prisma Access에서 인증에 사용할 SAML 속성을 선택하는 경우 **/identity/claims/name**을 포함하는 사용자 이름 속성을 선택해야 합니다. 잘못된 사용자 이름 속성을 선택하면 사용자가 프로젝트에 대해 인증할 수 없습니다.
DOCS-5463	**HIP** 데이터 수집 옵션이 에이전트 설정 페이지에서 활성화되어 있지 않은 경우 임의 터널 연결 해제가 발생할 수 있는 문제가 있습니다. 그러므로 액세스 에이전트 설정 페이지의 호스트 정보 프로파일(HIP) 섹션에서 **HIP** 데이터 수집을 비활성화하지 마십시오.

문제 **ID**	설명
DOCS-3650	동적 권한 액세스 활성화 Prisma Access 테넌트에서 Cloud Identity Engine 인증이 작동하려면 사용자 그룹이 ID 제공자(IdP)의 여러 SAML 애플리케이션에 매핑되지 않아야 합니다. 여러 앱이 사용자 그룹에 매핑된 경우 고유한 매핑이 없기 때문에 Cloud Identity Engine은 인증 중에 연결할 SAML 앱을 판별할 수 없습니다.
ADI-33262	동적 권한 액세스가 활성화된 Prisma Access 테넌트에서, 먼저 Strata Cloud Manager에서 프로젝트를 구성하지 않으면 모바일 사용자 컨테이너 > 액세스 에이전트 구성 푸시가 실패합니다. 해결 방법: 푸시 구성을 수행하기 전에 하나 이상의 프로젝트를 구성합니다.
ADI-31750	프로젝트당 지원되는 IP 풀의 수는 50개입니다. 프로젝트당 IP 풀 수가 50개를 초과하는 경우 성능에 영향을 미칩니다. 해결 방법: 프로젝트당 50개 이하의 IP 풀을 할당합니다.
ADI-31601	동적 권한 액세스가 활성화된 테넌트에서 Strata Cloud Manager를 사용하면 일반 오류와 함께 푸시 구성이 실패하더라도 프로젝트당 100개를 초과하는 IP 풀을 구성할 수 있습니다. 해결 방법: 프로젝트당 100개를 초과하는 IP 풀을 구성하지 마십시오.
ADI-31538	포워딩 프로파일을 설정할 때 포워딩 프로파일 유형이 "Prisma Access 에이전트" 대신 "ZTNA 에이전트"로 표시되는 문제가 있습니다. 또한, 포워딩 프로파일 추가를 선택하면 드롭다운에 "Prisma Access 에이전트" 대신 "ZTNA 에이전트"가 표시됩니다. 해결 방법: 없음. 향후 포워딩 프로파일 유형이 "Prisma Access 에이전트"로 변경될 예정입니다.
ADI-31523	특수 문자가 포함된 설명으로 스니펫을 만들지 마십시오. **! ~ @ # $ % ^ & * ( ) _ +**와 같은 특수 문자가 포함된 스니펫 설명은 지원되지 않습니다.

문제 **ID**	설명
ADI-31306	포워딩 프로파일을 설정할 때 포워딩 프로파일 페이지의 트래픽 적용 섹션에 있는 모든 옵션이 기본적으로 활성화되어 있는 문제가 있습니다. 기본적으로 이러한 옵션을 모두 활성화하면 예기치 않은 동작 또는 바람직하지 않은 동작이 발생할 수 있습니다. 해결 방법**:** 동적 권한 액세스에 대해 이러한 옵션을 비활성화합니다.
ADI-31305	포워딩 프로파일을 설정할 때 터널 **DNS** 서버를 사용하여 **FQDN DNS** 확인 적용 및 터널에서 할당한 **DNS** 서버를 사용하여 모든 **FQDN** 확인**(Windows** 에이전트만 해당**)** 옵션이 포워딩 프로파일 페이지의 트래픽 적용 섹션에 표시되는 문제가 있습니다. 이러한 옵션의 의도된 기능은 포워딩 프로파일 규칙을 사용하여 구성할 수 있으므로 이 두 옵션이 표시되어서는 안 됩니다.
ADI-30902	Strata Cloud Manager는 동적 권한 액세스 프로젝트 구성, Prisma Access 에이전트 설정, 보안 정책 및 단계적 롤아웃 구성과 같은 여러 구성에서 Cloud Identity Engine 디렉토리의 사용자 및 사용자 그룹 정보를 사용합니다. 이러한 구성을 작성한 후 Cloud Identity Engine에서 디렉토리를 삭제하지만 해당 사용자 및 사용자 그룹을 참조하는 Strata Cloud Manager 구성을 삭제하지 않으면 "500 Internal Server Error"와 같은 예기치 않은 오류가 발생할 수 있습니다. 해결 방법: Cloud Identity Engine에서 디렉토리를 제거할 때 해당 디렉토리의 사용자 및 사용자 그룹을 참조하는 Strata Cloud Manager 구성도 삭제해야 합니다.
ADI-30468	Strata Cloud Manager의 액세스 에이전트 > 인프라 설정 페이지에, **Prisma Access** 관리 및 **OnPrem DHCP** 서버 옵션 모두가 클라이언트 IP 풀 할당 섹션에 나타나는 문제가 있습니다. 동적 권한 액세스가 활성화된 일반 가용성 Prisma Access 테넌트에서 사용자를 프로비저닝하는 경우 구성을 저장한 후에는 되돌릴 수 없으므로 **OnPrem DHCP** 서버를 선택하지 마십시오. **OnPrem DHCP** 서버는 동적 권한 액세스 일반 가용성 테넌트에 대해 지원되지 않으며 Strata Cloud

문제 **ID**	설명
	Manager의 향후 릴리스에서 제거될 예정입니다. **OnPrem DHCP** 서버를 선택하는 경우 테넌트는 기본 동적 권한 액세스 워크플로에 사용할 수 없게 렌더링됩니다.
ADI-29665	프로젝트 이름에 특수 문자를 사용하지 마십시오. 그렇지 않으면 프로젝트 구성을 저장하려고 할 때 Strata Cloud Manager에서 "잘못된 형식의 요청" 오류 메시지를 발행합니다.
ADI-29434	Strata Cloud Manager의 에이전트 설정 페이지에서 세션 타임아웃에 권장되는 값은 7일입니다.
ADI-29272	스니펫을 만들 때 개체 이름에 접두사 추가 옵션을 비활성화하는 경우, 예기치 않은 동작이 발생하지 않도록 두 개의 서로 다른 스니펫에서 중복된 에이전트 설정 이름을 사용하지 마십시오.
ADI-26493	Strata Cloud Manager의 액세스 에이전트 > 인프라 설정에서 클라이언트 IP 풀 할당 섹션의 **OnPrem DHCP** 서버 옵션은 선택할 수 없습니다. **OnPrem DHCP** 서버는 동적 권한 액세스에 대해 지원되지 않으므로 이 동작은 의도된 동작입니다. 기존 동적 권한 액세스 활성화 Prisma Access 테넌트가 올바르게 작동하도록 이 옵션의 이름이 **OnPrem DHCP** 서버**(**미리 보기 전용**)**로 변경될 것입니다.
ADI-24562	프로젝트가 서로 다른 구성 스니펫으로부터 구성된 경우 동일한 도메인 및 사용자 그룹으로 둘 이상의 프로젝트를 만들 수 있는 문제가 있습니다. 일부 Strata Cloud Manager 워크플로에서 예기치 않은 동작이 발생할 수 있으므로 이 구성을 사용하지 마십시오. 해결 방법: 동일한 도메인 및 사용자 그룹을 사용하여 서로 다른 프로젝트를 구성하지 마십시오.

Prisma Access 5.2.1의 알려진 문제

문제 **ID**	설명
CYR-47139	애플리케이션에 연결하는 데 사용되는 ZTNA 커넥터 애플리케이션 블록, 커넥터 블록 또는 IP 서브넷이 명시적 프록시

문제 **ID**	설명
	주소와 충돌하는 RFC6598 주소로 구성된 경우 ZTNA 커넥터 - 명시적 프록시 통합에서 ZTNA 커넥터가 비활성화됩니다. 해결 방법: 명시적 프록시와 함께 사용하도록 ZTNA 커넥터를 구성할 때 애플리케이션 또는 커넥터 블록에 대해 100.64.0.0/15, 100.72.0.0/15 또는 100.88.0.0/15 서브넷을 사용하지 마십시오.
CYR-46759	DNS 쿼리에 대한 UDP 설정이 명시적 프록시에서 적용되지 않습니다.
CYR-46627	서비스 연결을 통한 기본 경로 수락이 활성화된 경우 명시적 프록시가 지원되지 않습니다.
CYR-46349	중국에서 트래픽 스티어링으로 명시적 프록시가 있는 원격 네트워크를 사용하는 경우 URL 범주를 사용하여 트래픽 스티어링 규칙을 구성하지 마십시오.
CYR-46191	프라이빗 애플리케이션 액세스가 활성화된 상태로 명시적 프록시가 구성되고 ZTNA 커넥터가 구성에 추가되면 Panorama 또는 Strata Cloud Manager에서 다른 커밋이 필요할 수 있습니다. 해결 방법: Prisma Access를 관리하는 Panorama 또는 Strata Cloud Manager에서 명시적 프록시 구성을 약간 수정하고 변경 사항을 푸시합니다.

Prisma Access 해결된 문제

어디에서 사용할 수 있습니까?	무엇이 필요합니까?
• Prisma Access (Managed by Panorama)	❑ Prisma Access 라이센스 ❑ Minimum Required Prisma Access Version 5.2 또는 5.2.1 Preferred 또는 Innovation

다음 항목에서는 Prisma Access 5.2 및 Prisma Access 5.2.1에서 해결된 문제를 설명합니다.

Prisma Access 5.2.1 해결된 문제

문제 ID	설명
CYR-45847	서비스 서브넷이 변경되면 Prisma Access GlobalProtect 게이트웨이에서 업데이트되었지만 NAT가 제대로 구현되지 않아 GlobalProtect 터널이 다운되는 문제를 수정했습니다.
CYR-45341	Colo-Connect 디바이스 그룹에 대한 커밋 및 푸시 작업의 제한 시간이 초과되어 VLAN이 삭제되지 않는 문제를 수정했습니다.
CYR-44391	중국의 명시적 프록시 구축이 인증에 클라우드 ID 엔진 또는 SAML을 사용하는 것을 지원하지 않는 문제를 수정했습니다.
CYR-43690	ZTNA 커넥터에서 커넥터 IP 블록을 수정하거나 삭제하려고 할 때 커밋 및 푸시 후에 변경 사항이 적용되지 않았던 문제를 수정했습니다.
CYR-42919	ZTNA 커넥터에서 커넥터 IP 블록을 수정하거나 삭제하려고 할 때 커밋 및 푸시 후에 변경 사항이 적용되지 않는 문제를 수정했습니다.

Prisma Access 5.2.0-h14 해결된 문제

문제 ID	설명
CYR-46782	GlobalProtect DDNS 기능에서 nsupdate 명령을 처리하는 동안 비ASCII 문자가 포함되어 있고 Panorama 캐시에 있는 도메인 이름으로 인해 오류가 발생하는 문제를 수정했습니다.
CYR-46358	Colo-Connect 변경 사항이 있는 클라우드 서비스 플러그인으로 업그레이드하는 동안 Prisma Access 에디션이 아닌 테넌트에서 #### ### ## ## 오류가 발생하는 문제를 수정했습니다.
CYR-45949	UI가 Prisma Access 인프라에 액세스할 수 없는 경우 모바일 사용자 - 명시적 프록시 온보딩 위치 탭이 로드되지 않고 버퍼링이 계속되는 문제를 수정했습니다.
CYR-45932	다음 오류로 인해 일회성 푸시(OTP) 확인이 실패하는 문제를 수정했습니다. `[get-panorama-cert.py:288] <class 'AttributeError'> ("'Pan_Plugin_Client' object has no attribute 'whitelist_keys'`
CYR-44969	역할 기반 관리자를 사용하여 생성한 사용자가 UI에서 클라우드 서비스 구성을 볼 수 없었던 문제를 수정했습니다.
CYR-44766	일반 API를 사용한 IKE 및 IPsec 암호화 프로파일 삭제에 실패하고 프로파일이 구성에서 삭제되지 않는 문제를 수정했습니다.

Prisma Access 5.2.0 해결된 문제

문제 ID	설명
CYR-45112	클라우드 서비스 플러그인을 5.1.0 이상 버전으로 업그레이드할 때 외부 게이트웨이 구성이 회색으로 표시되는 문제를 수정했습니다.

문제 **ID**	설명
CYR-44598	Panorama 관리형 Prisma Access 구축의 Strata 로깅 서비스 상태가 `Exception` <*customer-id*> 오류를 표시하는 문제를 수정했습니다.
CYR-43673	API의 모든 잘못된 구성이 GET 호출을 통해 시스템 관리자에게 다시 전달되는 문제를 수정했습니다.
CYR-43400	사용자 **ID** 유지가 선택된 ZTNA 커넥터 그룹에서 온보딩된 커넥터에서 내부 인터페이스에서 데이터 센터 앱으로의 작업 > 진단 > 핑**(ping)**이 작동하지 않는 문제를 수정했습니다.
CYR-43280	잘못된 base64 데이터 오류로 인해 변경 사항이 있더라도 DSP가 diff를 생성하지 못하는 문제를 수정했습니다.
CYR-43262	BGP 구성이 페이로드에 포함되어 있을 때 원격 네트워크 온보딩에 대한 원격 네트워크 API 요청이 플러그인에서 커밋 유효성 검사 오류를 발생시키는 문제를 수정했습니다.
CYR-43222	사용자 ID 기반 ZTNA 커넥터 그룹에 할당된 애플리케이션 대상이 **icmp ping**의 프로빙 유형을 지원하지 않는 문제를 수정했습니다.
CYR-42377	원격 문제 해결 및 업데이트를 위한 동적 DNS 등록 지원을 구성할 때 인증 유형이 **Kerberos**인 경우 Prisma Access를 관리하는 Panorama에 암호화되지 않은 Kerberos 키 파일을 업로드할 수 없는 문제를 수정했습니다. 플러그인 5.2.0 버전 이상을 사용하여 Panorama 관리형 구축을 실행 중이고 Kerberos 인증 유형을 선택하는 경우, DNS 서버에서 검색한 Kerberos 키의 base64 인코딩 문자열이 있는 .key 파일을 통해 인증 키를 업로드하십시오. 예를 들면 다음과 같습니다. `"ABCDEFGHIJKLMNOPQRSTUV5WXYZOUy5DT00ADUFabcD` 플러그인 5.1.0 버전 미만을 사용하여 Panorama 관리형 구축을 실행 중이고 Kerberos 인증 유형을 선택하는 경우, DNS 서버에서 검색한 인코딩되지

문제 ID	설명
	않은 Kerberos 키탭 파일이 있는.key 파일을 통해 인증 키를 업로드하십시오.
CYR-42191	동적 DNS 지원을 설정할 때 유효한 Kerberos 파일이 제대로 업로드되지 않아 시스템 구성에 저장되지 않는 문제를 수정했습니다.
CYR-41740	짧은 기간 동안 동일한 지역에 100개 이상의 커넥터가 온보딩된 경우 일부 ZTNA 커넥터를 통한 프라이빗 앱 액세스가 작동하지 않을 수 있는 문제를 수정했습니다.
CYR-38418	IPv6을 활성화한 후 Prisma Access 데이터플레인을 10.2.8-h1에서 10.2.8-h2로 업그레이드하지 못하는 문제를 수정했습니다.
CYR-38386	자동 크기 조정 작업으로 인해 더 많은 모바일 사용자 게이트웨이가 생성된 후 커밋 및 푸시 작업이 실패하는 문제를 수정했습니다.
CYR-37913	컴퓨팅에서 트래픽 복제를 비활성화한 다음 동일한 컴퓨팅에서 다시 활성화한 경우 트래픽 복제 기능이 영향을 받아 모바일 사용자 또는 원격 네트워크 트래픽이 복제되지 않고 커밋 없음 또는 구성 실패가 표시되는 문제를 수정했습니다.
CYR-37791	사용자가 한 프로젝트에서 다른 프로젝트로 전환하고 동일한 Prisma Access 위치에 연결한 후 Strata Cloud Manager의 모니터 > 사용자 페이지에 사용자가 3시간, 24시간, 7일 및 30일의 시간 범위 동안 전환한 올바른 프로젝트 이름이 반영되지 않는 문제를 수정했습니다.
CYR-36930	GlobalProtect 모바일 사용자가 이중 스택(IPv4 및 IPv6)을 활성화하고 IPv6이 활성화된 Prisma Access GlobalProtect 위치에 연결했다가 나중에 해당 위치에 대해 IPv6이 비활성화된 경우 이중 스택 사용자가 해당 위치에 연결할 수 없는 문제를 수정했습니다.

문제 ID	설명
CYR-27734	사용하지 않는 규칙 사용 통계에 대한 정책 최적화 프로그램이 원격 네트워크 디바이스 그룹의 Panorama에서 보이지 않는 문제를 수정했습니다.

Prisma Access 5.2 및 5.2.1에 대한 Panorama 지원

어디에서 사용할 수 있습니까?	무엇이 필요합니까?
• Prisma Access (Managed by Panorama)	❑ Prisma Access 라이센스 ❑ Minimum Required Prisma Access Version 5.2 또는 5.2.1 Preferred 또는 Innovation

Prisma Access (Managed by Panorama) 릴리즈 5.2 및 5.2.1에서는 **Cloud Services Plugin 5.2** 클라우드 서비스 플러그인을 사용합니다. Prisma Access 5.2.1은 5.2 플러그인의 핫픽스 버전을 사용하여 활성화됩니다. Panorama를 사용하여 Prisma Access를 관리하고 5.2 플러그인으로 업그레이드해야 하는 경우 다음을 수행해야 합니다.

1. Prisma Access 5.2 Preferred 및 Innovation을 지원하기 위해 Panorama에 필요한 소프트웨어 버전 검토
2. 클라우드 서비스 플러그인에 대해 따라야 할 업그레이드 경로 결정
3. 클라우드 서비스 플러그인 업그레이드

Panorama 관리형 Prisma Access 5.2 및 5.2.1을 위한 필수 소프트웨어 버전 및 권장 소프트웨어 버전

어디에서 사용할 수 있습니까?	무엇이 필요합니까?
• Prisma Access (Managed by Panorama)	❑ Prisma Access 라이센스 ❑ Minimum Required Prisma Access Version 5.2 또는 5.2.1 Preferred 또는 Innovation

Prisma Access 5.2.1 Preferred 및 Innovation을 위한 권장 소프트웨어 버전

Prisma Access 5.2.1 버전은 두 가지가 있습니다.

- 5.2.1 Preferred는 PAN-OS 10.2.10 데이터플레인을 실행합니다. 구축에서 하위 데이터플레인 버전을 실행하는 경우 5.2.1 Preferred 기능을 구현하려면 PAN-OS 10.2.10으로 데이터플레인을 업그레이드해야 합니다.
- 5.2.1 Innovation은 PAN-OS 11.2.4 데이터플레인을 실행합니다. 5.2 Innovation 기능을 구현하려면 PAN-OS 11.2.4로 업그레이드해야 합니다.

새로운 Prisma Access 5.2.1 Innovation 기능의 경우, Prisma Access에서는 플러그인을 설치하기 전에 **Prisma Access**를 다음 버전으로 업그레이드할 것을 권장합니다.

Prisma Access 버전	클라우드 서비스 플러그인 버전	**5.2.1**용 필수 데이터플레인 버전	권장 **GlobalProtect** 버전	권장 **Panorama** 버전
5.2.1	5.2.0 핫픽스	PAN-OS 10.2.10(5.2.1 Preferred에 필요) PAN-OS 11.2.4(5.2.1 Innovation에 필요)	6.0.7+ 6.1.3+ 6.2.1+	10.2.10+ 11.0.1+ 11.1.0 11.2.4

Prisma Access 5.2 Preferred 및 Innovation을 위한 권장 소프트웨어 버전

Prisma Access 5.2 버전은 두 가지가 있습니다.

- 5.2 Preferred는 PAN-OS 10.2.10 데이터플레인을 실행합니다. 구축에서 하위 데이터플레인 버전을 실행하는 경우 5.2 Preferred 기능을 구현하려면 PAN-OS 10.2.10으로 데이터플레인을 업그레이드해야 할 수 있습니다. 기존 고객인 경우 Prisma Access 5.2.1 Preferred 및 Innovation 기능에 대한 인프라, 플러그

인 및 데이터플레인 종속성을 참조하여 Prisma Access 5.2 기능에 데이터플레인 업그레이드가 필요한지 확인하십시오.

- 5.2 Innovation은 PAN-OS 11.2.3 데이터플레인을 실행합니다. 5.2 Innovation 기능을 구현하려면 PAN-OS 11.2.3으로 업그레이드해야 합니다.

새로운 Prisma Access 5.2 Innovation 기능의 경우, Prisma Access에서는 플러그인을 설치하기 전에 **Prisma Access**를 다음 버전으로 업그레이드할 것을 권장합니다.

Prisma Access 버전	클라우드 서비스 플러그인 버전	**5.2**용 필수 데이터플레인 버전	권장 **GlobalProtect** 버전	권장 **Panorama** 버전
5.2	5.2	PAN-OS 10.2.10(5.2 Preferred에 필요) PAN-OS 11.2.3(5.2 Innovation에 필요)	6.0.7+ 6.1.3+ 6.2.1+	10.2.10+ 11.0.1+ 11.1.0 11.2.3

Panorama 관리 Prisma Access에 대한 업그레이드 고려 사항

어디에서 사용할 수 있습니까?	무엇이 필요합니까?
• Prisma Access (Managed by Panorama)	❑ Prisma Access 라이센스 ❑ Minimum Required Prisma Access Version 5.2 또는 5.2.1 Preferred 또는 Innovation

클라우드 서비스 플러그인을 Prisma Access 5.2 또는 5.2.1로 업그레이드하려면 다음 업그레이드 경로 중 하나를 사용하십시오. Panorama에서 현재 플러그인 버전을 찾으려면 **Panorama** > 클라우드 서비스 > 구성 > 서비스 설정을 선택하고 플러그인 알림 영역에서 플러그인 버전을 확인하십시오.

업그레이드 중에 각 플러그인 버전에 대해 최소 Panorama 버전을 따르십시오.

설치된 클라우드 서비스 플러그인 버전	대상 버전	플러그인 업그레이드 경로
5.1	5.2 또는 5.2.1	플러그인을 Prisma Access 5.1에서 Prisma Access 5.2로 업그레이드하고 변경 사항을 커밋 및 푸시합니다.
5.0	5.2 또는 5.2.1	**1.** 플러그인을 Prisma Access 5.0에서 Prisma Access 5.1로 업그레이드하고 변경 사항을 커밋 및 푸시합니다. **2.** 플러그인을 Prisma Access 5.1에서 Prisma Access 5.2로 업그레이드하고 변경 사항을 커밋 및 푸시합니다.
4.1 및 4.2	5.2 또는 5.2.1	**1.** 플러그인을 Prisma Access 4.1에서 Prisma Access 5.0으로 업그레이드하고 변경 사항을 커밋 및 푸시합니다. **2.** 플러그인을 Prisma Access 5.0에서 Prisma Access 5.1로 업그레이드하고 변경 사항을 커밋 및 푸시합니다. **3.** 플러그인을 Prisma Access 5.1에서 Prisma Access 5.2로 업그레이드하고 변경 사항을 커밋 및 푸시합니다.
4.0	5.2 또는 5.2.1	**1.** 플러그인을 Prisma Access 4.1로 업그레이드하고 변경 사항을 커밋 및 푸시합니다. **2.** 플러그인을 Prisma Access 5.0으로 업그레이드하고 변경 사항을 커밋 및 푸시합니다. **3.** 플러그인을 Prisma Access 5.0에서 Prisma Access 5.1로 업그레이드하고 변경 사항을 커밋 및 푸시합니다.

설치된 클라우드 서비스 플러그인 버전	대상 버전	플러그인 업그레이드 경로
		4. 플러그인을 Prisma Access 5.1에서 Prisma Access 5.2로 업그레이드하고 변경 사항을 커밋 및 푸시합니다.
3.0, 3.1 및 3.2 Preferred	5.2 또는 5.2.1	1. (3.0 플러그인만 해당) 플러그인을 Prisma Access 3.1로 업그레이드하고 변경 사항을 커밋 및 푸시합니다. 2. (3.1 플러그인만 해당) 플러그인을 Prisma Access 3.2 또는 3.2.1로 업그레이드하고 변경 사항을 커밋 및 푸시합니다. 3. 플러그인을 Prisma Access 3.2 또는 3.2.1로 업그레이드하고 변경 사항을 커밋 및 푸시합니다. 4. 플러그인을 Prisma Access 4.0으로 업그레이드하고 변경 사항을 커밋 및 푸시합니다. 5. 플러그인을 Prisma Access 4.1로 업그레이드하고 변경 사항을 커밋 및 푸시합니다. 6. 플러그인을 Prisma Access 5.0으로 업그레이드하고 변경 사항을 커밋 및 푸시합니다. 7. 플러그인을 Prisma Access 5.0에서 Prisma Access 5.1로 업그레이드하고 변경 사항을 커밋 및 푸시합니다. 8. 플러그인을 Prisma Access 5.1에서 Prisma Access 5.2로 업그레이드하고 변경 사항을 커밋 및 푸시합니다.
2.2 Preferred	5.2 또는 5.2.1	1. 플러그인을 Prisma Access 3.0으로 업그레이드하고 변경 사항을 커밋 및 푸시합니다. 2. 플러그인을 Prisma Access 3.1로 업그레이드하고 변경 사항을 커밋 및 푸시합니다. 3. 플러그인을 Prisma Access 3.2 또는 3.2.1로 업그레이드하고 변경 사항을 커밋 및 푸시합니다. 4. 플러그인을 Prisma Access 4.0으로 업그레이드하고 변경 사항을 커밋 및 푸시합니다. 5. 플러그인을 Prisma Access 4.1로 업그레이드하고 변경 사항을 커밋 및 푸시합니다. 6. 플러그인을 Prisma Access 5.0으로 업그레이드하고 변경 사항을 커밋 및 푸시합니다. 7. 플러그인을 Prisma Access 5.0에서 Prisma Access 5.1로 업그레이드하고 변경 사항을 커밋 및 푸시합니다.

설치된 클라우드 서비스 플러그인 버전	대상 버전	플러그인 업그레이드 경로
		8. 플러그인을 Prisma Access 5.1에서 Prisma Access 5.2로 업그레이드하고 변경 사항을 커밋 및 푸시합니다.
2.2 이전 Preferred 릴리스	5.2 또는 5.2.1	**1.** 플러그인을 Prisma Access 2.2로 업그레이드하고 변경 사항을 커밋 및 푸시합니다. 구축이 2.2 Preferred 이전 버전의 Prisma Access인 경우 3.2로 업그레이드하기 전에 먼저 2.2로 업그레이드해야 합니다. Prisma Access 2.0 또는 2.1 버전에서의 업그레이드는 지원되지 않습니다. **2.** 플러그인을 Prisma Access 3.0으로 업그레이드하고 변경 사항을 커밋 및 푸시합니다. **3.** 플러그인을 Prisma Access 3.1로 업그레이드하고 변경 사항을 커밋 및 푸시합니다. **4.** 플러그인을 Prisma Access 3.2 또는 3.2.1로 업그레이드하고 변경 사항을 커밋 및 푸시합니다. **5.** 플러그인을 Prisma Access 4.0으로 업그레이드하고 변경 사항을 커밋 및 푸시합니다. **6.** 플러그인을 Prisma Access 4.1로 업그레이드하고 변경 사항을 커밋 및 푸시합니다. **7.** 플러그인을 Prisma Access 5.0으로 업그레이드하고 변경 사항을 커밋 및 푸시합니다. **8.** 플러그인을 Prisma Access 5.0에서 Prisma Access 5.1로 업그레이드하고 변경 사항을 커밋 및 푸시합니다. **9.** 플러그인을 Prisma Access 5.1에서 Prisma Access 5.2로 업그레이드하고 변경 사항을 커밋 및 푸시합니다.

클라우드 서비스 플러그인 업그레이드

어디에서 사용할 수 있습니까?	무엇이 필요합니까?
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 라이센스 ❑ Minimum Required Prisma Access Version 5.2 또는 5.2.1 Preferred 또는 Innovation

다음 절차에 따라 클라우드 서비스 플러그인을 업그레이드합니다.

Prisma Access는 Panorama의 클라우드 서비스 플러그인을 사용하여 기능을 활성화합니다.

Prisma Access에서 지원되는 Panorama 소프트웨어 버전 목록은 Palo Alto Networks 호환성 매트릭스에서 필요한 최소 Panorama 소프트웨어 버전의 내용을 참조하십시오.

플러그인을 업그레이드하기 전에 Prisma Access 템플릿 스택에서 Prisma Access가 아닌 템플릿을 제거하여 업그레이드 후 커밋 유효성 검사 오류를 방지하고 Prisma Access를 관리하는 Panorama가 지원되는 PAN-OS 버전을 실행하고 있는지 확인하십시오.

다음 작업 중 하나를 사용하여 클라우드 서비스 플러그인을 다운로드하여 설치합니다.

HA 구축만 해당 - 고가용성(HA) 모드에서 두 개의 *Panorama* 어플라이언스가 구성된 경우 먼저 기본 *HA* 쌍에 플러그인을 설치한 다음, 보조 *HA* 쌍에 설치합니다.

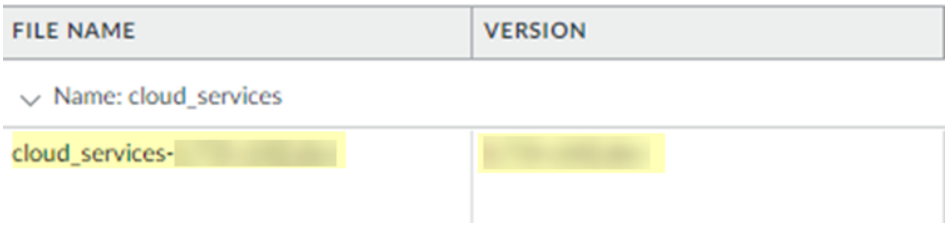
STEP 1 | 업그레이드하려는 플러그인에 대해 업그레이드 경로를 결정합니다.

일부 업그레이드 경로의 경우 플러그인을 순차적으로 업그레이드해야 합니다. 예를 들어, 3.0 Preferred 플러그인에서 5.2 플러그인으로 업그레이드하려면 5.2로 업그레이드하기 전에 먼저 3.1, 4.0, 4.1, 5.0 및 5.1로 중간 업그레이드를 수행해야 합니다.

STEP 2 | 필요한 클라우드 서비스 플러그인 버전을 다운로드하여 설치합니다.

- 고객 지원 포털에서 클라우드 서비스 플러그인을 다운로드하여 설치하려면 다음 단계를 완료하십시오.
  1. 고객 지원 포털에 로그인하고 소프트웨어 업데이트를 선택합니다.
  2. Panorama 통합 플러그인 섹션에서 클라우드 서비스 플러그인을 찾아 다운로드합니다.

     플러그인 파일의 이름을 바꾸지 마십시오. 이름을 바꾸면 *Panorama*에 설치할 수 없습니다.
  3. Prisma Access와 함께 사용하도록 라이센스를 받은 Panorama의 Panorama 웹 인터페이스에 로그인하고 **Panorama** > 플러그인 > 업로드 및 찾아보기를 통해 고객 지원 포털에서 다운로드한 플러그인 파일을 선택합니다.
  4. 플러그인을 설치합니다.
- Panorama에서 직접 클라우드 서비스 플러그인의 새 버전을 다운로드하고 설치하려면 다음 단계를 완료하십시오.
  1. **Panorama** > 플러그인을 선택하고 지금 확인을 클릭하여 최신 클라우드 서비스 플러그인 업데이트를 표시합니다.

  2. 설치하려는 플러그인 버전을 다운로드합니다.
  3. 플러그인을 다운로드 한 후, 설치합니다.

STEP 3 | (3.2 이전 버전에서 3.2 이상 버전으로 업그레이드) 커밋 > **Panorama**에 커밋을 선택하여 Prisma Access를 관리하는 Panorama에 로컬로 변경 사항을 저장합니다.

3.2 이전 버전의 클라우드 서비스 플러그인에서 3.2 이상인 플러그인으로 업그레이드하는 경우에만 Panorama에 로컬 커밋을 수행해야 합니다. 3.2 이후 버전에서 업그레이드하는 경우 로컬 커밋이 필요하지 않습니다.

도움 받기

어디에서 사용할 수 있습니까?	무엇이 필요합니까?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 라이센스 ❑ Minimum Required Prisma Access Version 5.2 Preferred 및 Innovation

다음 항목에서는 이 릴리즈에 대한 자세한 내용을 확인하고 지원을 요청하는 방법에 대한 정보를 제공합니다.

- 관련 문서
- 지원 요청

관련 문서

다음 문서를 사용하여 Prisma Access 구축을 설정하고 구현하십시오.

- Prisma Access 관리자 가이드를 사용하여 Prisma Access를 계획, 설치, 설정 및 구성하여 네트워크를 보호하십시오.
- Prisma Access 통합 가이드의 공급업체별 작업을 활용하여 Prisma Access를 통해 모바일 사용자 인증을 구성하고 퍼블릭 클라우드 및 타사 SD-WAN 구축을 보호하십시오.
- Strata 로깅 서비스 시작하기 가이드를 사용하여 Strata Logging Service(이전의 Cortex Data Lake) 구축 방법을 알아보고 온프레미스 방화벽에서 Cortex Data Lake로 로그 전달을 시작하십시오.

https://docs.paloaltonetworks.com을 방문하여 당사 제품에 대한 자세한 정보를 알아보십시오.

지원 요청

지원 팀에 문의하거나, 지원 프로그램에 대한 정보를 얻거나, 계정이나 디바이스를 관리하거나, 지원 케이스를 열려면 https://support.paloaltonetworks.com으로 이동하십시오

문서에 대한 피드백을 제공하려면 documentation@paloaltonetworks.com으로 이메일을 보내주십시오.

연락처 정보

본사**:**

Palo Alto Networks

3000 Tannery Way

Santa Clara, CA 95054

https://www.paloaltonetworks.com/company/contact-support

Palo Alto Networks, Inc.

www.paloaltonetworks.com