paloalto TECHDOCS

Prisma Accessリリース ノート

5.2.0-h14 and 5.2.1

docs.paloaltonetworks.com

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リリース情報

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessライセンス ❑ Minimum Required Prisma Access Version 5.2または5.2.1のPreferred (推奨)またはInnovation (革新)

Prisma Accessリリース アップデートについて

Prisma Accessのリリースとアップデートにより、常に最新の状態を維持し、ユーザーを保護することができます。Prisma Accessインフラなど一部のアップデートはPalo Alto Networksが管理しており、それに対応するための詳細な通知がお客様に送信されます。一部のアップデートはお客様の責任で行ってください。コンテンツ アップデートおよびソフトウェア アップデートの指定されたバージョンをスケジュールする必要があります。Prisma Accessの管理に（Prisma Access Cloud Managementではなく）Panoramaを使用している場合は、プラグインがPanoramaに対して新たに有効にする機能を利用するために、最新のプラグイン バージョンにアップグレードするタイミングを決定します。

Panoramaが管理するPrisma Accessを使用する場合、PanoramaとこのPanoramaが管理するリリースのプラグインの要件を表示します。

Prisma Accessで使用するサポート対象の**GlobalProtect**バージョン

EoL（サポート終了)以外のGlobalProtectバージョンは、Prisma Accessでの使用がサポートされています。ただし、Prisma Access 5.2には、GlobalProtectの推奨ソフトウェアバージョンと必要なバージョンもあります。

ここでは、Prisma Accessに付属または統合されている製品およびサービスの最新アップデートについての詳細を知ることができます。

最新の**Prisma Access**リリース アップデート	以前の**Prisma Access**リリース バージョン	**Prisma Access**でサポートされているサービスとアドオンのアップデート
• Prisma Access5.2および5.2.1の新機能 • Prisma Access Cloud Managementの新機能	• Prisma Accessバージョン5.1 • Prisma Accessバージョン5.0 • Prisma Accessバージョン4.2	• Prisma Access Insights • 自律型 DEM • SaaS セキュリティ • Enterprise DLP • グローバルプロテクト

最新の**Prisma Access**リリースアップデート	以前の**Prisma Access**リリースバージョン	**Prisma Access**でサポートされているサービスとアドオンのアップデート
	• Prisma Accessバージョン4.1 • Prisma Accessバージョン4.0 • Prisma Accessバージョン3.2 PreferredとInnovation • Prisma Accessバージョン3.1 PreferredとInnovation • Prisma Accessバージョン3.0 PreferredとInnovation • Prisma Accessバージョン2.2 Preferred • 2.2 Preferredより前のPrisma Accessのリリース	• Prisma SASEマルチテナント クラウド管理プラットフォーム • Prisma SD-WAN

Prisma Access5.2および5.2.1の新機能

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessライセンス ❑ Minimum Required Prisma Access Version5.2または5.2.1のPreferred (推奨)またはInnovation (革新)

このセクションでは、Prisma Access5.2および5.2.1のPreferred (優先)およびInnovation (革新)の新機能のリストと、使用する必要のある推奨および必須のソフトウェア バージョンを示します。

この文書にはロードマップの情報が含まれており、情報提供および計画の目的でのみ共有されています。拘束力のあるコミットメントではなく、変更される可能性があります。

- Prisma Access5.2.1のPreferred (推奨)とInnovation (革新)の推奨ソフトウェア バージョン
- Prisma Access5.2.1 Preferred機能とInnovation機能のインフラストラクチャ、プラグイン、およびデータプレーンの依存関係
- Prisma Access 5.2.1の機能

Prisma Access5.2.1のPreferred (推奨)とInnovation (革新)の推奨ソフトウェア バージョン

Prisma Access5.2.1には2つのバージョンがあります。

- 5.2.1 Preferred (推奨)はPAN-OS 10.2.10データプレーンを実行します。デプロイメント環境で下位のデータプレーン バージョンを実行している場合、5.2.1の Preferred (推奨)機能を実装するには、PAN-OS 10.2.10へのデータプレーンのアップグレードが必要です。
- 5.2.1 Innovation (革新)はPAN-OS 11.2.4データプレーンを実行します。5.2 Innovation機能を実装するには、PAN-OS 11.2.4へのアップグレードが必要です。

5.2.1 Innovationの新Prisma Access機能については、 Prisma Accessではプラグインをインストールする前に **Prisma Access**を以下のバージョンにアップグレードすることをお勧めします 。

Prisma Accessバージョン	クラウドサービスプラグインのバージョン	**5.2.1**に必要なデータプレーンのバージョン	**GlobalProtect**の推奨バージョン	推奨**Panorama**バージョン
5.2.1	5.2.0のホット	PAN-OS 10.2.10（5.2.1	6.0.7+	10.2.10+

Prisma Accessバージョン	クラウドサービスプラグインのバージョン	5.2.1に必要なデータプレーンのバージョン	GlobalProtectの推奨バージョン	推奨Panoramaバージョン
	フィックス	Preferred (優先)に必要） PAN-OS 11.2.4（5.2.1 Innovation (革新)に必要）	6.1.3+ 6.2.1+	11.0.1+ 11.1.0 11.2.4

Prisma Access 5.2 Preferred (推奨)とInnovation (革新)の推奨ソフトウェア バージョン

Prisma Access 5.2には2つのバージョンがあります。

- 5.2 Preferred (推奨)はPAN-OS 10.2.10データプレーンを実行します。デプロイメント環境で下位のデータプレーン バージョンを実行している場合、5.2 Preferred (優先)機能を実装するには、PAN-OS 10.2.10へのデータプレーン アップグレードが必要になることがあります。既存のお客様は、Prisma Access 5.2の機能にデータプレーンのアップグレードが必要かどうかについて、Prisma Access5.2.1 Preferred機能とInnovation機能のインフラストラクチャ、プラグイン、およびデータプレーンの依存関係を参照してください。
- 5.2 Innovation (革新)は11.2.3のPAN-OSデータプレーンを実行します。5.2 Innovation機能を実装するには、PAN-OS 11.2.3へのアップグレードが必要です。

5.2 Innovationの新Prisma Access機能については、 Prisma Accessではプラグインをインストールする前に **Prisma Access**を以下のバージョンにアップグレードすることをお勧めします 。

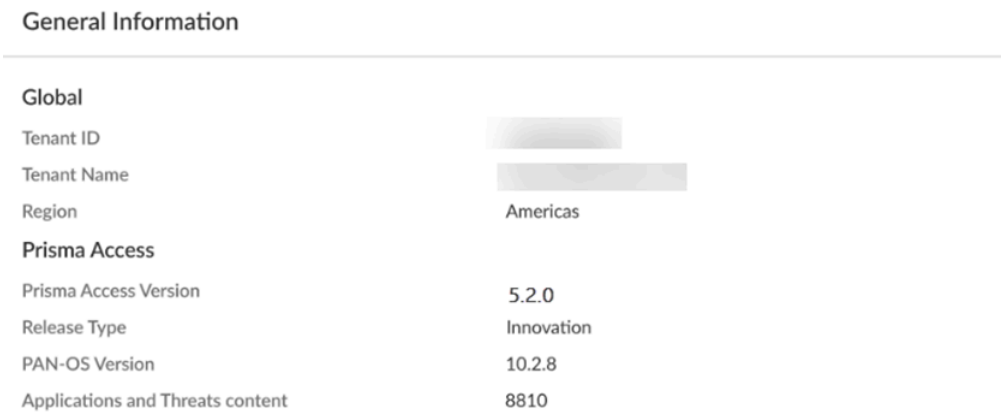
Prisma Accessバージョン	クラウドサービスプラグインのバージョン	5.2に必要なデータプレーンのバージョン	GlobalProtectの推奨バージョン	推奨Panoramaバージョン
5.2	5.2	PAN-OS 10.2.10（5.2 Preferredに必要） PAN-OS 11.2.3（5.2 Innovationに必要）	6.0.7+ 6.1.3+ 6.2.1+	10.2.10+ 11.0.1+ 11.1.0 11.2.3

Prisma Access5.2.1 Preferred機能とInnovation機能のインフラストラクチャ、プラグイン、およびデータプレーンの依存関係

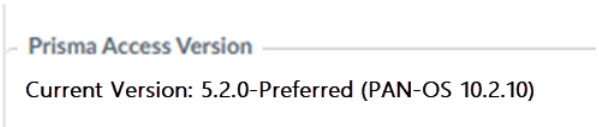
Prisma Access5.2.1の機能が機能するには、以下のコンポーネントのうち1つ以上が必要です:

- インフラのアップグレード—インフラストラクチャには、基盤となるサービス バックエンド、オーケストレーション、および監視インフラストラクチャが含まれます。Prisma Accessは、Prisma Accessリリースの一般提供(GA)日より前にインフラをアップグレードします。

  インフラのアップグレードだけでロックを解除できる機能は、バージョンに関係なく、インフラのアップグレード時にすべてのPrisma Accessデプロイメントで有効になります。
- プラグインのアップグレード(**Prisma AccessPanoramaが管理するデプロイメントのみ**): プラグインをインストールすると、そのリリースで使用できる機能がアクティベートされます。Prisma Accessを管理するPanoramaにプラグインをダウンロードしてインストールします。
- データプレーン アップグレード—データプレーンにより、ネットワークおよびユーザー トラフィックに対するトラフィック検査とセキュリティ ポリシーの適用が可能になります。
  - Prisma Access (Managed by Strata Cloud Manager)については、**[Manage (管理)]** > **[Configuration (設定)]** > **[NGFW and Prisma Access (NGFWとPrisma Access)]** > **[Overview (概要)]**。

  - Prisma Access (Managed by Panorama)デプロイメントの場合、データプレーンのバージョンを表示するには、**[Panorama]** > **[Cloud Services (クラウド サービス)]** > **[Configuration (設定)]** > **[Service Setup (サービス セットアップ)]**に移動し、**Prisma Access[Version (バージョン)]**を表示します。Prisma Access 5.2.1 PreferredはPAN-OS 10.2.10を実行し、Prisma Access InnovationはPAN-OS 11.2.4を実行します。

*5.2.1 Innovation*へのデータプレーンのアップグレードはオプションです。データプレーンのアップグレードが必要な機能を利用する場合だけ、アップグレードが必要です。

これらの機能は、インフラのアップグレードでPrisma Accessに対してのみアクティベートされます。

- ハイパフォーマンスなブランチ サイトの可視化
- Prisma Access Agentの観測性
- 新しいPrisma Access (Managed by Strata Cloud Manager)デプロイメント用のRFC6598モバイル ユーザー アドレス プール
- ブランチ サイトおよびサービス接続でのルート テーブルの可視性
- ZTNAコネクタの表示と監視の更新
- エージェントベースの明示型プロキシの表示
- イスラエルとサウジアラビアのStrata Logging Serviceのリージョン サポート
- 既存のPrisma Accessデプロイメントのための IPv6ネイティブ サポート

これらの機能には、インフラストラクチャとプラグインのアップグレードが必要ですが、データプレーンのアップグレードは必要ありません。ただし、これらの機能には、10.2.4以上のデータペイン バージョンが必要です。

- Colo-Connectの明示型プロキシのサポート
- DNSプロキシの明示型プロキシのサポート
- ZTNAコネクタとの明示型プロキシ統合
- ワイルドカードFQDNによるZTNAコネクタ ポリシー設定の更新
- 明示型プロキシのサードパーティ製エンタープライズ ブラウザとの統合

以下の5.2.1の機能を使用するには、インフラとプラグインのアップグレードが必要です。また、PAN-OS 10.2.10の最小データプレーン バージョンが必要です。そうすることで、Prisma Access 5.2.1のPreferred機能になります:

- オンボーディング アプリケーション向けZTNAコネクタの機能拡張
- なし

以下の5.2の機能は、PAN-OS 11.2.4へのインフラストラクチャ、プラグイン、データプレーンをアップグレードしてPrisma Access 5.2.1 Innovationの機能とする必要があります。

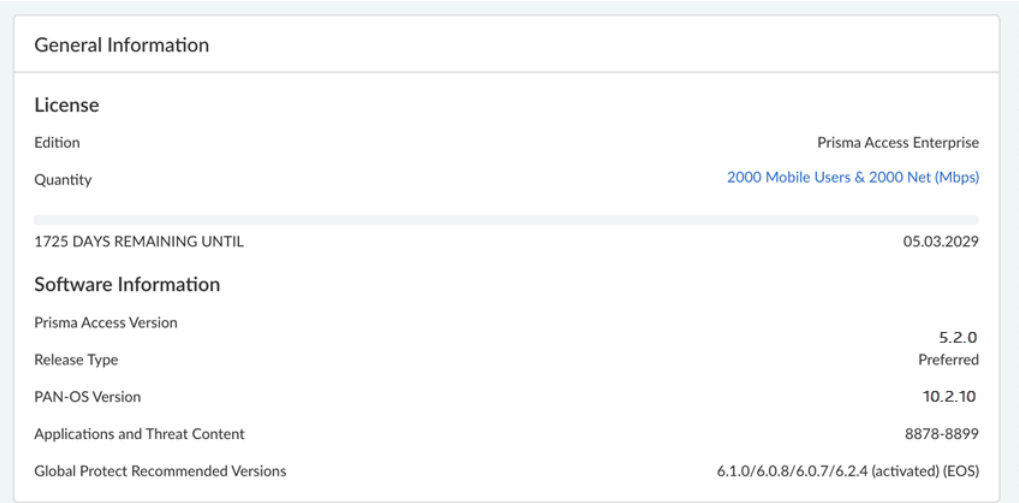
- リモート ネットワーク—高性能プライベート アプリ アクセスのサポート
- モバイル ユーザー向けの静的IPアドレスの拡張
- モバイル　ユーザー向けの静的IPアドレス割り当ての表示

Prisma Access 5.2 Preferred機能とInnovation機能のインフラ、プラグイン、およびデータプレーンの依存関係

Prisma Access 5.2の機能を使用するには、次のコンポーネントのうち1つ以上が必要です。

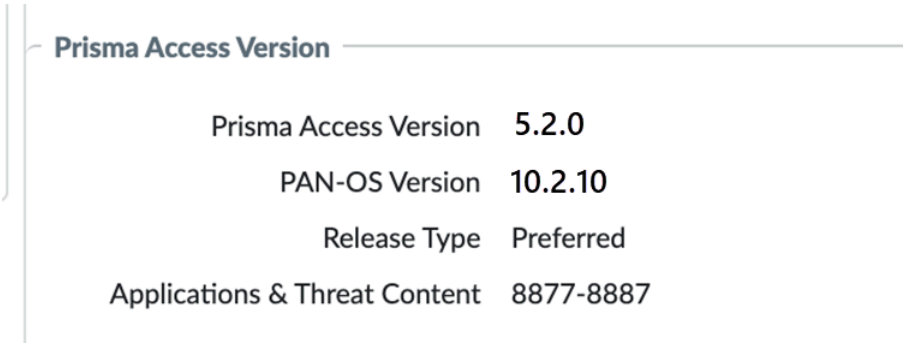
- インフラのアップグレード—インフラストラクチャには、基盤となるサービス バックエンド、オーケストレーション、および監視インフラストラクチャが含まれます。Prisma Accessは、Prisma Accessリリースの一般提供(GA)日より前にインフラをアップグレードします。

  インフラのアップグレードだけでロックを解除できる機能は、バージョンに関係なく、インフラのアップグレード時にすべてのPrisma Accessデプロイメントで有効になります。
- プラグインのアップグレード(**Prisma AccessPanoramaが管理するデプロイメントのみ**): プラグインをインストールすると、そのリリースで使用できる機能がアクティベートされます。Prisma Accessを管理するPanoramaにプラグインをダウンロードしてインストールします。
- データプレーン アップグレード—データプレーンにより、ネットワークおよびユーザー トラフィックに対するトラフィック検査とセキュリティ ポリシーの適用が可能になります。
  - Prisma Access (Managed by Strata Cloud Manager)については、**[Manage (管理)]** > **[Configuration (設定)]** > **[NGFW and Prisma Access (NGFWとPrisma Access)]** > **[Overview (概要)]**。

  - Prisma Access (Managed by Panorama)デプロイメントの場合、データプレーンのバージョンを表示するには、**[Panorama]** > **[Cloud Services (クラウド サービス)]** > **[Configuration (設定)]** > **[Service Setup (サービス セットアップ)]**に移動し、**Prisma Access[Version (バージョ**

ン)]を表示します。Prisma Access 5.2 PreferredはPAN-OS 10.2.10を実行し、Prisma Access InnovationはPAN-OS 11.2.3を実行します。



5.2 Innovation へのデータプレーンのアップグレードはオプションです。データプレーンのアップグレードが必要な機能を利用する場合だけ、アップグレードが必要です。

これらの機能は、インフラのアップグレードでPrisma Accessに対してのみアクティベートされます。

- エンドポイントDLP
- モバイル ユーザー向けのIP最適化と明示型プロキシのデプロイメントでPrisma Access SaaS接続を簡素化
- TLS 1.3とPubSubによるトラフィック レプリケーションのサポート
- Colo-Connectの表示と監視

これらの機能には、インフラとプラグインのアップグレードが必要ですが、データプレーンのアップグレードは必要ありません。

- 25,000のリモート ネットワークと50,000のIKEゲートウェイのサポート
- エージェント ベースのプロキシ トラフィックに対するプライベートIPアドレスの可視化と適用
- 明示型プロキシ ユーザーのためのIPアドレス最適化-プロキシのデプロイメント
- クラウド サービス プラグイン向けRBACのサポート
- シンプルなPrisma Accessプライベート アプリ接続 にも5.2 SaaS-Agentのアップグレードが必要です
- AWS向けSPバックボーン統合サポート
- Strata Cloud ManagerでPrisma Access、データプレーン、アプリケーションおよび脅威のコンテンツバージョンを表示する

以下の5.2.1の機能を使用するには、インフラとプラグインのアップグレードが必要です。また、PAN-OS 10.2.10の最小データプレーン バージョンが必要です。そうすることで、Prisma Access5.2.1のPreferred機能になります:

- リモート ネットワーク—ハイ パフォーマンス

以下の5.2の機能は、Prisma Access 11.2.3へインフラ、プラグイン、データプレーンをアップグレードしてPrisma Access 5.2.1 Innovationの機能とする必要があります。

- CIAMによる動的な特権アクセスに対してSC-NATがサポートされたことで、
- ZTNA コネクタによるコミットレス アプリ オンボーディングのサポート

Prisma Access 5.2.1の機能

以下の表に、Prisma Access 5.2.1で一般に提供される新機能を示します。

Colo-Connectの明示型プロキシのサポート

サポート対象:Prisma Access5.2.1 PreferredとInnovation

コロケーション施設に直接接続できる大規模なデータセンターでは、Prisma Access明示型プロキシを介して接続できるようになり、プライベート アプリケーションへの高速アクセスが可能になります。強化により、リージョンあたり最大20Gbpsのスループットが得られます。

Colo-ConnectとExplicit Proxy明示型プロキシの統合には、以下のような利点があります。

- 明示型プロキシは、最も近いPrisma Accessコンピューティング ロケーションに自動的に接続し、可能な限り最高のレイテンシーを提供します。
- ネットワークとルーティングの依存関係を排除し、プライベート アプリケーション向けにセキュア トンネル管理とルーティングを自動化します。
- Colo-Connectは、重複ネットワーク内のプライベート アプリケーションの取得をサポートし、柔軟性とアクセシビリティを確保します

DNSプロキシの明示型プロキシのサポート

サポート対象:Prisma Access (Managed by Strata Cloud Manager)5.2.1 PreferredとInnovation

明示型プロキシは、DNS Proxyのカスタマイズを含むようにサポートを拡張します。明示型プロキシは、地域DNS、カスタムDNSなどのDNS設定をサポートしています。また、サードパーティのDNSリゾルバーやオンプレミスのDNSリゾルバーを使用してパブリック アプリとプライベート アプリを解決し、FQDNごとに使用することができます。この機能は現在、でのみサポートされています。

明示型プロキシによるサードパーティ製エンタープライズ ブラウザの安全な統合

サポート対象:Prisma Access5.2.1 PreferredとInnovation

Prism Accessでは、サードパーティ製のエンタープライズ ブラウザを介してプライベート アプリケーションへの安全なアクセスが可能になりました。今回の機能強化により、サードパーティーのエンタープライズ ブラウザとPrisma Accessの間でユーザー情報を安全かつ透過的に交換できるようになり、Prisma Access内でユーザーIDベースのポリシー ルールを適用することが可能となります。これにより、エンド ユーザーがサードパーティ製のエンタープライズ ブラウザにすでにログインしている場合に、Prisma Accessで再認証する必要がなくなります。

ZTNAコネクタとの明示型プロキシ統合

サポート対象:Prisma Access5.2.1 PreferredとInnovation

ZTNAコネクタを介してプライベート アプリケーションに接続するユーザーは、Prisma Access明示型プロキシを介して接続を確立できるようになりました。この統合は、Prisma Access BrowserとAgent Proxy向けに最大10Gbpsの容量を持つZTNAコネクタをサポートします。

その他のメリットとして、次のようなものがあります。

- 明示型プロキシは、明示型プロキシを使用して最も近いPrisma Accessコンピューティング ロケーションに自動的に接続し、最適なレイテンシーを確保します。
- ネットワークとルーティングの依存関係を排除し、プライベート アプリケーションのセキュア トンネル管理とルーティングを自動化します。
- ZTNAコネクタは、プライベート アプリケーションの自動検出を可能にするCIE（Cloud Identity Engine）をサポートしています。
- ZTNAコネクタは、重複ネットワーク内のプライベート アプリケーションの取得をサポートし、柔軟性とアクセス性を確保します。

ハイパフォーマンスなブランチ サイトの可視化

サポート対象:Prisma Access5.2.1 PreferredとInnovation

Prisma Accessの高性能ブランチ (RN-HP) は、従来のブランチとは一線を画す特徴を持っており、顧客環境内では両者が共存することになります。管理システムは、ネットワーク管理者がトラブルシューティングを行う際に役立つように、新しいRN-HPブランチ タイプに対応する必要があります。

既存のPrisma Accessデプロイメントに対するIPv6のネイティブサポート

サポート対象: Prisma Access すべてのデプロイメントに対する5.2.1 PreferredおよびInnovation（IPv6による新規デプロイメントのサポートはPrisma Access 5.1.1以降。既存のデプロイメントのサポートはPrisma Access 5.2.1で追加）

Prisma Accessは、プライベート アプリケーションからのIPv6 サポートを拡張し、モバイル ユーザー、リモート ネットワーク、サービス接続に対する包括的なエンドツーエンドのIPv6 サポートを網羅し、既存のPrisma Accessデプロイメントにネイティブ IPv6サポートを追加します。

ネイティブIPv6サポートの利点の1つは、IPv6のみのエンドポイントを使用するモバイル ユーザーが、GlobalProtectを使用してIPv6接続経由でPrisma Accessとの接続を確立できることです。さらに、このサポートにより、特に宛先でIPv6接続が必要な場合に、インターネット経由でパブリックSaaSアプリケーションにアクセスしやすくなります。

IPv6はIPv4に比べてアドレス空間が広く、ほぼ無制限の数の固有のIPアドレスを収容できます。Prisma Accessはネイティブ IPv6サポートを通じて、IPv6とデュアルスタック接続の両方と互換性を持つように設計されており、IPv4からIPv6への移行プロセスを容易にします。この互換性により、下位互換性が保証され、組織はクラウドベースおよびIPv6対応ネットワークに移行しやすくなります。

Prisma Accessエージェントの観測性

サポート対象:Prisma Access5.2.1 PreferredとInnovation

Prisma Access Agentは、Prisma Accessを使用してモバイル ワーカーのセキュリティを確保できる次世代モバイル アクセス エージェントです。今日のハイブリッド ワーク環境向けに構築されたPrisma Access Agentは、エンタープライズ アプリケーションとインターネットの両方への安全で便利なアクセスを提供し、組織のネットワーク、IT、セキュリティ運用を簡素化します。Strata Cloud Managerで、**[Insights (インサイト)]** > **[Activity Insights (アクティビティ インサイト)]** > **[Users (ユーザー)]**に移動し、Prisma Access Agentのデプロイメントに関する情報を表示します。

リモート ネットワーク—高性能プライベート アプリケーション アクセスのサポート

サポート対象:Prisma Access5.2.1 PreferredとInnovation

Prisma Accessリモート ネットワーク—ハイ パフォーマンスは、インターネットへの出口に対する既存のサポートに加えて、プライベート アプリへのアクセス サポートを追加します。このサポートにより、次のことが可能になります。

- 高パフォーマンス リモート ネットワークで接続されたブランチからプライベート アプリを取得する
- サービス接続を使用して別のブランチと通信する(ブランチ間トラフィック)
- サービス接続を使用してモバイルユーザーと通信する（モバイル ユーザーからブランチへのトラフィック）

ブランチ サイトおよびサービス接続でのルート テーブルの可視性

サポート対象:Prisma Access5.2.1 PreferredとInnovation

モバイル ユーザー向けの静的IPアドレスの拡張

サポート対象:Prisma Access5.2.1 Innovation

Prisma Accessでは、モバイル ユーザー向けの静的IPアドレス機能に加え、Prisma Accessシアターまたはユーザー IDに基づいてユーザーに静的IPアドレスを割り当てることができます。

モバイル ユーザーのIPアドレス割り当てを強化するため、シアターやユーザーIDに加えて、ロケーション グループやユーザー グループを基準として使用できるようになりました。

さらに、サポートされるIPアドレス プール プロファイル数が10,000に増加しました。

新しいPrisma Access (Managed by Strata Cloud Manager)デプロイメント用のRFC6598モバイル ユーザー アドレス プール

サポート対象:Prisma Access (Managed by Strata Cloud Manager)5.2.1 PreferredとInnovation

すべてのPrisma Accessデプロイメントには、モバイル ユーザー アドレスIPプールが必要です。Prisma Accessは、このプールからGlobalProtectで接続された各デバイスにIPアドレスを割り当てます。GlobalProtectモバイル ユーザーのオンボーディングを簡素化するために、Palo Alto NetworksはRFC6598からデフォルトのIPアドレス プールを備えた新しいPrisma Access（Strata Cloud Managerによって管理）デプロイメントを提供しています。IPプールは100.92.0.0/16です。より多くのアドレスが必要な場合、または独自のアドレスを使用する場合は、このプールを変更するか、削除して独自のIPアドレス プールを追加できます。

イスラエルとサウジアラビアのStrata Logging Serviceのリージョン サポート

サポート対象:Prisma Access5.2.1 PreferredとInnovation

Prisma Accessは、イスラエルとサウジアラビアのStrata Logging Serviceリージョンをサポートしています。

ZTNAコネクタの表示と監視の更新

サポート対象:Prisma Access5.2.1 PreferredとInnovation

ゼロ トラスト ネットワーク アクセス (ZTNA) コネクタは、すべてのアプリケーションのプライベート アプリケーション アクセスを簡素化します。環境内のZTNAコネクタVMは、プライベート アプリケーションとの間に自動的にトンネルを形成します。Prisma Access 5.2.1以降、ZTNAコネクタ ページの外観を見直して使いやすくし、ワイルドカード、FQDN、IPサブネット ターゲットの詳細を示す表を追加しました。

エージェントベースの明示型プロキシの表示

サポート対象:Prisma Access5.2.1 PreferredとInnovation

説明待ちです。

モバイル　ユーザー向けの静的IPアドレス割り当ての表示

サポート対象:Prisma Access5.2.1 Innovation

静的IPプールを監視するには、**[Insights (インサイト)]** > **[Activity Insights (アクティビティ インサイト)]** > **[Users (ユーザー)]**に移動し、**[IP Pool Utilization (IP プール使用率)]**ウィジェットで静的IPプールを監視します。静的IP割り当て機能を使用すると、Prisma Accessモバイル ユーザーに固定IPアドレスを割り当てることができます。これは、ネットワーク デプロイメントにおいて、ネットワークおよびアプリケーションの設計の一環としてIPアドレスを使用してリソースへのユーザー アクセスを制限する場合に役立ちます。この機能を使用すると、シアターとユーザーに基づいてIPプールを定義できます。

ZTNAコネクタにおけるセキュリティポリシーのワイルドカードFQDN設定

サポート対象:Prisma Access5.2.1 PreferredとInnovation

セキュリティ ポリシー ルールでのワイルドカード FQDNの使用は、現在、プロトコルの制限事項によって制限されています。そのため、現時点では、セキュリティ ポリシー ルールのワイルドカードFQDNではHTTPおよびHTTPSプロトコルのみがサポートされています。

この機能強化により、次のことが可能になります。

- ワイルドカード アプリケーションFQDNに基づいてセキュリティ ポリシーを設定できます。
- 同じワイルドカードFQDNを共有する検出されたすべてのアプリケーションに同じセキュリティ ポリシーが適用されます。
- ワイルドカードFQDNに一致する新しいアプリケーションが検出されると、新しいコミットを必要とせずにトラフィックを通過できます。

オンボーディング アプリケーション向けZTNAコネクタの機能拡張

サポート対象:Prisma Access5.2.1 PreferredとInnovation

エンタープライズのユーザーが多数のプライベート アプリケーションにアクセスする場合、インフラ内のアプリケーションの数が15000を超えると、ZTNAコネクタでスケーラビリティの問題が発生する可能性があります。

ZTNAコネクタは、スケーラビリティを向上させる拡張機能を提供し、ユーザーによる以下のオンボーディングを可能にします。

- テナントあたり20,000アプリケーション、コネクタ グループあたり4,000アプリケーション。
- テナント全体で400個のコネクタがあり、コンピューティング リージョンあたり16Gbpsの帯域幅。

オンボーディング アプリケーション用ZTNAコネクタ

サポート対象:Prisma Access5.2.1 PreferredとInnovation

エンタープライズのユーザーが多数のプライベート アプリケーションにアクセスする場合、インフラ内のアプリケーションの数が15000を超えると、ZTNAコネクタでスケーラビリティの問題が発生する可能性があります。

ZTNAコネクタは、スケーラビリティを向上させる拡張機能を提供し、ユーザーによる以下のオンボーディングを可能にします。

- テナントあたり20,000アプリケーション、コネクタ グループあたり4,000アプリケーション。
- テナント全体で400個のコネクタがあり、コンピューティング リージョンあたり16Gbpsの帯域幅。

ワイルドカードFQDNによるZTNAコネクタ ポリシー設定の更新

サポート対象:Prisma Access5.2.1 PreferredとInnovation

セキュリティ ポリシー ルールでのワイルドカード FQDNの使用は、現在、プロトコルの制限事項によって制限されています。そのため、現時点では、セキュリティ ポリシー ルールのワイルドカードFQDNではHTTPおよびHTTPSプロトコルのみがサポートされています。

この機能強化により、次のことが可能になります。

- ワイルドカード アプリケーションFQDNに基づいてセキュリティ ポリシーを設定できます。
- 同じワイルドカードFQDNを共有する検出されたすべてのアプリケーションに同じセキュリティ ポリシーが適用されます。

- ワイルドカードFQDNに一致する新しいアプリケーションが検出されると、新しいコミットを必要とせずにトラフィックを通過できます。

Prisma Access 5.2 の機能

このセクションでは、Prisma Access 5.2で使用できる新機能について説明します。

25,000のリモート ネットワークと**50,000**の**IKE**ゲートウェイのサポート

サポート対象:Prisma Access 5.2 PreferredとInnovation

この機能を実装するには、Palo Alto Networksのアカウントチームに連絡し、SREケースをオープンして要求に対応します。

エージェント ベースのプロキシ トラフィックに対するプライベート**IP**アドレスの可視化と適用

サポート対象:Prisma Access 5.2 PreferredとInnovation

ブランチからGlobalProtectエージェントを介してPrisma Access明示型プロキシに接続するユーザーは、エンドポイントのプライベートIPアドレスをログに利用したり、IPアドレス ベースの実施を適用したりできます。

明示型プロキシ ユーザーのための**IP**アドレス最適化**-**プロキシのデプロイメント

サポート対象:Prisma Access 5.2 PreferredとInnovation

IPアドレス最適化は、デプロイメント環境におけるIPアドレスの全体的な数を削減するアーキテクチャ上の拡張機能のセットです。これにより、許可リスティング ワークフローが簡素化されると同時に、耐障害性が向上し、Prisma Accessテナントの迅速なオンボーディングが可能になります。

IPアドレスの持続性

IPアドレスの持続性により、ユーザー セッションを必要とするSaaSアプリやウェブサイトをセキュリティ保護し、ユーザー セッション全体を通じてPrisma Accessの出力IPアドレスを同じに保つことができます。

SaaSアプリケーションのオンボーディングを簡素化

Prisma Accessロケーションを追加するか、既存のPrisma Accessロケーションでスケーリング イベントが発生すると、明示型プロキシのデプロイメントに新しいIPアドレスが割り当てられる可能性があります。ベストプラクティスは、新しい出力およびゲートウェイのIPアドレスを取得し、SaaSアプリケーションの許可リストに追加することです。IPアドレスの最適化により、大規模なデプロイメントで管理しなければならないIPアドレスの数を減らすことができます。

エンドポイントDLP

サポート対象:Prisma Access 5.2 PreferredとInnovation

Prisma Access Agentが必要です。

エンドポイントDLPを使用すると、セキュリティ管理者は周辺機器の使用を許可またはブロックして周辺機器の使用を制御したり、組織内のエンドポイントに周辺機器が接続されたときにセキュリティ管理者に警告したりすることができます。周辺機器への機密データの流出を防ぐには、高度な検出方法、および独自のトラフィック一致条件を定義するカスタム データ プロファイル、または事前定義済みMLベースおよび正規表現のデータ プロファイル。

保護するエンドポイント上でをインストールすると、エンドポイントと周辺機器間のファイルの移動を検出し、ファイルの移動を検出したときにエンドポイントDLPポリシー ルールを評価して適用します。必要に応じて、はトラフィックをに転送して検査および判決を下します。はその後判決をに伝達し、その後、エンドポイントDLPポリシー ルールで設定されたアクションが実行されます。さらに、はまた、DLP インシデントを生成したときにエンド ユーザーに通知を表示する役割も担います。

を使用したエンドポイントの検査は以下の通りです。これは、が正常にインストールされ、エンドポイントDLPポリシー ルールが設定されたことを想定しています。

1. 組織内のユーザーがラップトップに周辺機器を接続します。
2. ユーザーはエンドポイントから接続された周辺機器にファイルを移動します。
3. はユーザーがエンドポイントから周辺機器にファイルを移動しようとしたことを記録し、エンドポイント DLP ポリシー ルールベースを評価します。
   - ポリシー ルールの一致なし-エンドポイントDLPポリシー ルールの一致が特定されない場合は、周辺機器の接続が許可され、エンドポイントには周辺機器に対する完全な読み取りおよび書き込みアクセス権限が付与されます。
   - 周辺機器制御ポリシー ルール—アクセスを制御するために周辺機器制御ポリシー ルールを作成した場合、はポリシー ルールで設定された許可またはブロック アクションを実行します。

     たとえば、エンドポイントDLPポリシー ルールが周辺機器への接続をブロックする場合、は周辺機器への書き込み権限を取り消します。この場合、エンドポイントは周辺機器にファイルをアップロードできません。

     逆に、エンドポイントDLPポリシー ルールが周辺機器への接続を許可している場合は、はエンドポイントに周辺機器への書き込みアクセス権限を付与します。この場合、エンドポイントは周辺機器にファイルをアップロードできます。
   - 移動中のデータ ポリシー ルール—周辺機器への接続が許可されます。がエンドポイントから周辺機器へのファイル移動を検出すると、ファイルはに転送され、検査および判決を

下します。また、はfileSHAなどの重要なファイル メタデータも転送します。これは、によって転送された各ファイルを識別するために使用されます。

がその後判決をに送り、機密データが検出された場合は、がエンドポイント DLP ポリシー ルール アクションを実行します。がfileSHAに基づいてすでに検査されたファイルであることを検出した場合は、 は既存の判決をに返します。は同じファイルを2回検査しません。

4. は周辺機器制御または移動中のデータ ポリシー ルールのいずれかで設定されたエンドポイントDLPポリシー ルール アクションを適用します。
5. 適切な場合にDLPインシデントが生成されます。エンド ユーザー コーチングを設定している場合は、エンドポイントに通知が表示され、ユーザーに警告されます。

明示型プロキシの中国サポート

サポート対象:Prisma Access 5.2 PreferredとInnovation

Prisma Accessは、中国での明示型プロキシのデプロイメントをサポートしています。

クラウド サービス プラグイン向け**RBAC**のサポート

サポート対象:Prisma Access (Managed by Panorama) 5.2 PreferredとInnovation

---

リモート ネットワーク—ハイ パフォーマンス

サポート対象:Prisma Access 5.2 PreferredとInnovation

Prisma Accessは、大規模サイトのサポート、自動ロード バランシング、簡素化されたオンボーディング、地域冗長性、単一出口IP管理、Prisma SD-WANを含むさまざまなSD-WANソリューションとの互換性など、高帯域幅IPSec終端のための包括的なソリューションを提供します。これらの機能によって、リモート サイト接続のスケーラビリティ、パフォーマンス、信頼性が総合的に強化されます。

ビジネスの規模が拡大し、オフィスの場所が地理的に分散するようになった場合、Prisma Accessパフォーマントのリモート ネットワーク(別名リモートネットワーク—高パフォーマンス)を使用して、高帯域幅のブランチ サイトを素早くオンボードできます。これらのネットワークには、以下のような利点があります。

- サービスIPアドレスまたはサービス エンドポイント アドレスあたり最大3Gbpsの総帯域幅をサポートし、IPSecトンネル終端に使用するIPアドレスまたはFQDNの数を削減できます。
- 可用性とフォールト トレランスを向上させるための地域冗長性を備えています。
- NATを使用してパブリック出口IPアドレスを削減します。

- 地理的な可用性に基づいて場所を選択する製品内の推奨事項により、オンボーディングを簡素化します。
- Prisma SD-WANがパブリックおよびプライベート トランスポート上のセキュア ファブリックVPNパスとプライベートWANアンダーレイ パスを積極的にプローブすることでリンク品質を決定するリンク品質指標（LQM）のサポートを含みます。プローブは、ジッタ、遅延、パケット損失などのネットワーク パフォーマンス メトリックを常時測定します。これらのメトリックは、アプリケーション固有のパフォーマンス メトリックおよびレイヤー1 からレイヤー7までの到達可能性とともに、新規および既存のアプリケーション フローのトラフィック転送決定内容を通知します。

動的な特権アクセスのルート要約

サポート対象:Prisma Access (Managed by Strata Cloud Manager) 5.2 Innovation

---

動的な特権アクセス対応Prisma Accessテナントでは、オンプレミス ネットワークにモバイル ユーザー（MU）ルートを通知するときにルートを集約できます。ルート集約は、基本的なクラウド ルーターなどの容量が限られているオンプレミス機器を持つエンタープライズにとって有益です。ルートの集約は、これらのデバイスの需要を減らすことで、デバイスがデータセンターと通信する際に経路容量を超えないようにします。

ルート集約を有効にするには、複数のプロジェクトで使用できる大きなIPプールのリストで構成されるグローバル集約プールを設定します。次に、Prisma Accessサービス接続でルート集約を有効にします。ユーザーがPrisma Access Agentを使用して、設定されたグローバル サマリー プールの範囲内にIPアドレスを持つプロジェクトに接続すると、サービス接続は、より小さいプロジェクトレベルのルートの代わりにグローバル サマリー プールを通知します。これにより、ネットワークに送信されるルートの数を減らすことができます。

CIAMによる動的な特権アクセスのための**SC-NAT**サポート

サポート対象:Prisma Access 5.2 Innovation

DPAを使用しており、データセンターまたは本社のプライベート アプリケーションにアクセスするためのサービス接続を作成している場合は、動的な特権アクセス（DPA）のSC-NATサポートを使用してください。インフラ サブネットのIPアドレスが重複すると、DPA環境内の複数のプロジェクトでIPアドレスが枯渇する可能性があります。この問題を解決するために、Prisma Accessは次のようなIPアドレス用の送信元NAT (SNAT) を実装できます。

- サービス接続を使用してプライベート アプリにアクセスするモバイル ユーザーの単一IPアドレスをPrisma Accessにマップさせます
- 簡単にルーティングできるSNATを提供
- IPプールの重複を排除
- Prisma Accessとデータセンターまたは本社の間のIPプールのIPv4枯渇を解消します

Prisma Accessプライベートアプリ接続の簡素化

サポート対象:Prisma Access 5.2 PreferredとInnovation

プライベート アプリにアクセスする1つの方法は、サービス接続を使用する方法です。サービス接続-企業アクセスノード(SC-CAN)とも呼ばれます。サービス接続を使用してプライベート アプリに接続するのが難しい場合があります。その理由は、以下のとおりです:

- SC-CANの障害によるプライベート アプリケーションのスループットの不確定性
- 不正な中継ホップによる遅延
- SC-CANのデプロイにおける運用の複雑さ

Prisma Accessは、この問題を解決するために、ルーティング インフラストラクチャのルーティング機能を強化しました。この機能強化は、以下のことに役立ちます:

- 内部ネットワークの改善によりSC-CANの障害を解消
- 必要に応じてアンカーSC-CANをオーケストレーションし、不正なトランジット ホップや非効率的なルーティングを防止

この設計には以下のような利点があります:

- よりデプロイしやすいルーティング セットアップ
- 簡単なゼロデイ セットアップ
- 特定のSC-CANからプライベート アプリのあるデータセンターまたは本社の場所までの1Gbpsの帯域幅が確定的

モバイル ユーザー向けの**IP**最適化と明示型プロキシのデプロイメントで**Prisma Access SaaS**接続を簡素化

サポート対象:Prisma Access 5.2 PreferredとInnovation

Prisma Accessは、IP最適化機能をモバイルユーザー—GlobalProtectだけでなく、明示型プロキシにも提供することにより、IP最適化機能を拡張します。

モバイル ユーザー—GlobalProtectデプロイメントの場合、多数のユーザーがロケーションからGlobalProtectゲートウェイにアクセスすると、Prisma Accessによってロケーションがオートスケールされ、別のGlobalProtectゲートウェイが追加されます。IP最適化はNATレイヤーを使用するため、オートスケールされたゲートウェイは以前に割り当てられたIPアドレスと同じIPアドレスを使用するので、組織の許可リストに余分なIPアドレスを追加する必要がありません。

Prisma AccessはNATレイヤーを明示型プロキシのセキュリティ処理ノード（SPN）だけでなく、モバイルユーザーSPNにも拡張し、明示型プロキシのデプロイメントでリストのIPアドレスを許可する必要性を軽減します。この明示型プロキシNATレイヤーは、プロキシ モードまたはトン

ネルとプロキシ モードでモバイル ユーザーと明示型プロキシのデプロイメントをセットアップする場合に便利です。

AWS向け**SP**バックボーン統合サポート

サポート対象:Prisma Access 5.2 PreferredとInnovation

この機能を実装するには、Palo Alto Networksのアカウントチームに連絡し、SREケースをオープンして要求に対応します。

Prisma Accessバージョン5.2から、お客様(サービスプロバイダー)は、顧客のパブリック クラウド出口トラフィックに対してAWSとGCPを柔軟に選択できるようになりました。ライセンスのアクティベーションには追加のリージョンが表示され、接続とIPアドレス プールにはGCPとAWSの異なるタブが表示され、パブリック クラウドを個別に監視することもできます。

TLS 1.3と**PubSub**によるトラフィック レプリケーションのサポート

サポート対象:Prisma Access 5.2 PreferredとInnovation

トラフィック レプリケーションを使用している大規模な組織では、デプロイと使用において以下のような課題が生じる可能性があります。

- パケット キャプチャ（PCAP）ファイルを消費するツールは、大量のPCAPファイルに対応するためにバケットの頻繁なクエリを必要とします。ツールはバケットにオーバーヘッドを発生させ、クラウド プロバイダーによって使用が制限される可能性があります。
- フォレンジック解析にPCAPファイルを使用する場合、SSL復号化されたトラフィックにアクセスすると、より高い効果が得られます。また、トラフィックのかなりの量がTLS 1.3で暗号化されます。

Prisma Accessでは、これらの問題を解決するために、サードパーティ ツールをより効率的かつ容易に拡張できる以下の拡張機能を提供しています。

- 公開/サブ通知—Prisma Accessは、新しいPCAPファイルがストレージ バケットにアップロードされると、公開/サブ通知をプロアクティブに送信します。新しいPCAPファイルにPub/Sub通知を使用すると、バケットに新しいファイルがあると通知するツールを開発する必要がなくなります。
- **TLS 1.3**復号化サポート—Prisma AccessはPCAPファイルを復号化する際にTLS 1.3を使用するため、トラフィックを詳細に可視化できます。このサポートは、PCAPファイルでSSL/TLS復号ポリシー ルールの使用を有効にしているリモート ネットワーク デプロイメントに適用されます。

Colo-Connectの表示と監視

サポート対象:Prisma Access 5.2 PreferredとInnovation

Colo-Connectは、Coloベースのパフォーマンス ハブの概念に基づいて構築されており、既存のパフォーマンス ハブからPrisma Accessへのレイヤー2/3接続とともに、高帯域幅のプライベート接続を提供します。Colo-Connectは、クラウド ネイティブのGCPインターコネクト技術を活用して、プライベート アプリケーションへの高帯域幅サービス接続を提供します。**[Monitor (監視)]** > **[Data Centers (データセンター)]** > **[Service Connections (サービス接続)]**に移動して、クラウド相互接続を介してハイブリッド クラウドおよびオンプレミス データセンターへのプライベート接続を表示および監視します。

Strata Cloud Managerと**Panorama**で**Prisma Access**、データプレーン、アプリケーションおよび脅威のコンテンツのバージョンを表示する

サポート対象:Prisma Access (Managed by Strata Cloud Manager) 5.2 PreferredとInnovation

Prisma Access (Strata Cloud Manager で管理)のデプロイメントに関する詳細情報を得るために、[Overview (概要)]ページ(Strata Cloud Managerの**[Manage (管理)]** > **[Configuration (構成)]** > **[NGFW and Prisma Access (NGFWと**Prisma Access**)]** > **[Overview (概要)]**)の[Software Infirnation (ソフトウェア情報)]領域と、PanoramaのPrisma Access バージョン (**[Panorama]** > **[Cloud Services (クラウド サービス)]** > **[Configuration (設定)]** > **[Service Setup (サービス セットアップ)]**) に以下の情報が表示されます。

- Prisma Accessバージョン
- PAN-OSデータプレーンのバージョン
- リリース タイプ(PreferredまたはInnovation)
- アプリケーションおよび脅威コンテンツのバージョン

ZTNA コネクタによるコミットレス アプリ オンボーディングのサポート

サポート対象:Prisma Access 5.2 Innovation

コミットレスなオンボーディングの強化により、アプリケーションのオンボーディング、変更、削除時の操作性が向上します。従来の5〜10分の遅延がなくなり、より迅速な処理が可能になります。アプリケーション オンボーディングにかかる時間が1分未満になり、アプリケーションを迅速かつ効率的に管理できるようになります。さらに、拡張されたZTNAコネクタは、10,000以上のアプリケーションを管理する大規模顧客のニーズに対応します。より多くのアプリケーションをオンボードできるため、運用の柔軟性と効率性が向上します。

Prisma Access5.2および5.2.1のデフォルトの動作の変更

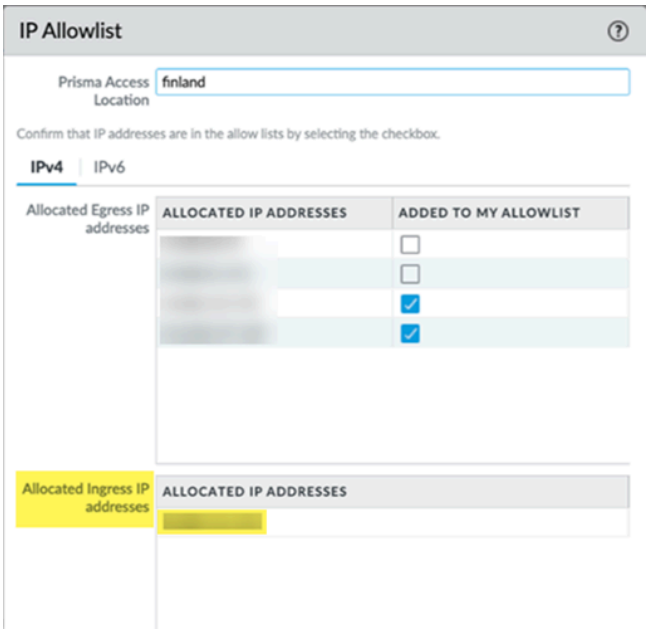
どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessライセンス ❑ Minimum Required Prisma Access Version5.2または5.2.1の推奨または革新

以下のセクションでは、Prisma Accessバージョン5.2およびPrisma Access5.2.1のデフォルト動作の変更について詳しく説明します。

Prisma Access5.2.1のデフォルト動作の変更

以下の表に、Prisma Accessバージョン5.2.1のデフォルト動作の変更の詳細を示します。

コンポーネント	変更
IPの最適化を新しい**Prisma Access**デプロイメントで可能に	Prisma Accessテナントの迅速なオンボーディングを可能にし、IPアドレス許可リストを簡素化するために、新しいPrisma AccessデプロイメントではIP最適化が有効になっています。 *IP*最適化デプロイメントでは、パブリック*(*外部*)*アプリへのアクセスにIPv6はサポートされていません。プライベート アプリへのアクセスはサポートされています。新しい*Prisma Access*デプロイメントで*IPv6*を有効にするには、*Palo Alto Networks*アカウント チームに連絡し、*TAC*ケースを開いて要求に対応します。 新しいPrisma Accessデプロイメントをセットアップする前に、すべてのユーザーがGlobalProtectアプリケーションのバージョン6.1.4以降、6.2.3以降、または6.3.0以降を実行していることを確認してください。 新しい*FedRAMP*デプロイメントでは、*IP*最適化が有効になっていません。
デフォルトのモバイル ユーザー—新しい**PrismaAccess**（**Strata**	新しいPrisma Access（Strata Cloud Managerで管理）モバイル ユーザー—GlobalProtectデプロイメントには、以下の新しいデフォルトのIPアドレス プールがあります:100.92.0.0/16これは、デフォ

コンポーネント	変更
Cloud Managerで管理）デプロイメントのために**GlobalProtect IP**アドレス プールを変更	ルトのIPアドレス プール100.127.0.0/16を使用していた以前のデプロイメントからの変更です。このRFC6598プールは、モバイル ユーザーのプライベート アプリ アクセスなど、ほとんどのユース ケースで使用できます。IPアドレスがさらに必要な場合は、Prisma Access UIで追加できます。
IP最適化に移行したデプロイメントの**IP**アドレス統合	IP最適化に移行したリージョンが1つ以上ある既存のPrisma Accessで、Prisma Access許可リストを使用している場合、リスト表示を許可した一部のIPアドレスが、Prisma AccessUIの割り当て済み出口**IP**アドレス領域から割り当て済み入口**IP**アドレス領域に移動しました。この変更は、Prisma Access 5.2.1インフラストラクチャのアップグレードの一環としてIPアドレスが統合された結果です。ネットワークはこれらのIPアドレスに到達でき、リストを許可する必要がなくなりました。 

Prisma Access5.2のデフォルトの動作の変更

コンポーネント	変更
PAN-OS 10.2.10データプレーンのアップグレードに関する考慮事項	Palo Alto NetworksにデータプレーンをPAN-OS 10.2.10にアップグレードしてPrisma Access 5.2 Preferred (優先)機能をサポートすることを選択した場合は、アップグレードのスケジュールを設定する前に、以下の10.2固有の変更点とアップグレードに関する考慮事項を確認してください。

コンポーネント	変更
	• デフォルト動作 • のアップグレード/ダウングレードに関する考慮事項の変更 • PAN-OS 10.2.10およびその他のPAN-OS 10.2リリースで対処された問題
PAN-OS 11.2.3データプレーンのアップグレードに関する考慮事項	Palo Alto NetworksにデータプレーンをPAN-OS 11.2.3にアップグレードしてPrisma Access 5.2 Innovation (革新)機能をサポートすることを選択した場合は、アップグレードのスケジュールを設定する前に、以下の11.2固有の変更点とアップグレードに関する考慮事項を確認してください。 • デフォルト動作 • のアップグレード/ダウングレードに関する考慮事項の変更 • PAN-OS 11.2.2およびその他のPAN-OS 11.2リリースで対処された問題
Prisma Access5.1での**Web**インターフェースの変更	Prisma Access5.1では、最大25,000のリモート ネットワークをサポートするように、Prisma Access (Managed by Strata Cloud Manager)Webインターフェースの一部が変更されました。詳細は 25,000のリモート ネットワークと50,000のIKEゲートウェイのサポート を参照してください。

Prisma Accessの既知の問題

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	❑ Prisma Accessライセンス ❑ Minimum Required Prisma Access Version5.2または5.2.1のPreferred (推奨)またはInnovation (革新)

Prisma Accessには以下の既知の問題があります。

問題 ID	詳説
AIOPS-11286	Colo-Connectを有効にしている場合、マルチテナント環境のサブテナントでクロスコネクトおよび接続関連情報が最新にならないことがあります。
CYR-47139	ZTNAコネクタ アプリケーション ブロックまたはコネクタ ブロックが、明示型プロキシ アドレスと競合するRFC6598アドレスで設定されている場合、ZTNAコネクタ-明示型プロキシ統合でZTNAコネクタが無効になります。 回避策:ZTNAコネクタを明示型プロキシと統合している場合、以下の用途には「100.64.0.0/15」、「100.72.0.0/15」、「100.88.0.0/15」サブネットを使用しないでください。 • ZTNAコネクタ-アプリケーション ブロック • ZTNAコネクタのコネクタ ブロック • アプリケーションに関連付けたZTNAコネクタで設定したIPサブネット
CYR-46759	DNSクエリのUDP設定は、明示型プロキシでは適用されません。
CYR-46627	[**Accept Default Route over Service Connection (**サービスコネクション経由のデフォルト ルートを受け入れる**)]**が有効になっている場合、明示型プロキシはサポートされません。

問題 ID	詳説
CYR-46445	NATデバイスで処理されたポート6081に関連する一時的なエラーにより、ZTNAコネクタがダウンしました。 回避策:ZTNAコネクタのトラフィックがNATデバイスを通過するときは、NATセッションがポート6081にマッピングされていないことを確認してください。
CYR-46349	リモート ネットワークをトラフィック ステアリング付きの明示型プロキシで中国で使用する場合、URLカテゴリでトラフィック ステアリング ルールを設定しないでください。
CYR-46191	Explicit Proxyがプライベート アプリケーション アクセスを有効にして設定されており、ZTNAコネクタが設定に追加されている場合、PanoramaまたはStrata Cloud Managerからの別のコミットが必要になることがあります。 回避策:Prisma Accessを管理するPanoramaまたはStrata Cloud Managerの明示型プロキシ設定に小さな修正を加え、変更をプッシュします。
CYR-46170	DDNSを有効にしていて、後でモバイル ユーザーにサービス サブネットの変更をプッシュする場合、DDNSが変更を拾うためにモバイル ユーザー ゲートウェイのDDNSプラグインも再起動する必要があります。 回避策:以下のコマンドを入力します。 デバッグ ソフトウェア再起動プロセス**pl-ddns**
CYR-46145	ZTNAコネクタと対応するアプリケーションがオンボードされている既存のPrisma Accessテナントの Prisma Access自律システム番号またはPrisma Accessインフラ サブネットが更新された場合、更新後5分程度停止が発生します。
CYR-46093	デプロイメント環境で、最大25,000のリモートネットワークと50,000の IKE ゲートウェイをサポートする機能を実装している場合、帯域幅使用量の統計情報の集計では、使用量の統計情報の代わりに"No data for

問題 ID	詳説
	the specified time period (指定された期間のでーたがありません)"と表示されます。
CYR-45440	管理者ロールを設定すると、アクセス情報が正しく保存されないことがあります。 回避策:[Admin Roles (管理者ロール)]領域で[Plugins/Cloud Services Plugins (プラグイン/クラウド サービス プラグイン)]を2回以上クリックして、アクセス情報が正しく保存されていることを確認します。[OK]をクリックし、もう一度[Open (開く)]」をクリックして、変更が保存されるかどうかを確認します。
CYR-45415	クラウド サービス プラグインへの読み取り専用または無効のアクセス権を持つ管理者は、テンプレート、デバイスグループ、クラウド サービス設定の削除、クラウド サービス プラグインのアンインストール、設定ファイルのロードなど、クラウドサービスの動作に影響を与えるクラウド サービス プラグイン以外の構成を変更できます。
CYR-45517	［Colo-Connect］タブでは、読み取り専用ユーザーがオンボーディング エントリを削除できます。
CYR-45440	管理者ロールを設定すると、アクセス情報が正しく保存されないことがあります。 回避策:[Admin Roles (管理者ロール)]領域で[Plugins/Cloud Services Plugins (プラグイン/クラウド サービス プラグイン)]を2回以上クリックして、アクセス情報が正しく保存されていることを確認します。**[OK]**をクリックして、もう一度**[Open (開く)]**をクリックし、変更が保存されているかどうかを確認します。
CYR-45415	クラウド サービス プラグインへの読み取り専用または無効のアクセス権を持つ管理者は、テンプレート、デバイスグループ、クラウド サービス設定の削除、クラウド サービス プラグインのアンインストール、設定ファイルのロードなど、クラウドサービスの動作に影響を与えるクラウド サービス プラグイン以外の構成を変更できます。

問題 ID	詳説
CYR-44433	成功したリモート ネットワーク ジョブのステータスが[Success (成功)]から[Pending (保留)]に変わることがあります。
CYR-44202	クラウド サービス プラグインへの読み取り専用アクセスを持つ管理ユーザーは 、 ［RBI］タブを変更できます。
CYR-43425	サービス接続でRFC 6598アドレスが使用されている場合、サービス接続のアウトバウンド ルートを指定することはできません。
CYR-43400 この問題は**Prisma Access5.2.0**で解決されました。**Prisma Access5.2.0**で解決された問題を参照してください。	**[Preserve User ID (ユーザーID**を保持**)]**がオンになっているZTNAコネクタ グループにオンボードされているコネクタの場合、内部インターフェースからデータセンターアプリへの**[Action (**アクション**)]** > **[Diagnostics (**診断**)]** > **ping** が機能しません。
CYR-43262 この問題は**Prisma Access5.2.0**で解決されました。**Prisma Access5.2.0**で解決された問題を参照してください。	リモート ネットワーク オンボーディングのリモート ネットワークAPI要求は、BGP設定がペイロードに含まれている場合、クラウ ドサービス プラグイン上でコミット検証エラーを返します。
CYR-43222 この問題は**Prisma Access5.2.0**で解決されました。**Prisma Access5.2.0**で解決された問題を参照してください。	ユーザーIDベースのZTNAコネクタ グループに割り当てられたアプリケーション ターゲットは、プローブタイプの**icmp ping**をサポートしていません。 回避策:アプリケーションの**[Probint Type (**プローブタイプ**)]**を**[none (**なし**)]**または**[tcp ping]**にします。
CYR-43147	オートスケールされたZTNAコネクタの場合、スケールイン中に、既存の長寿命セッションが途中でドロップされることがあります。これは、スケールイン用にマークされたZTNAコネクタによって処理されます。スケール後の新しいトラフィック セッションには影響がないはずです。
CYR-43132	Panoramaでサブテナントを作成する際、[Mobile Users (モバイルユーザー)]の設定を空白のままにしておくと、[Remote Networks (リモートネットワーク)]のユニットを設定できません。その逆も同様です。

問題 ID	詳説
CYR-42919この問題は**Prisma Access5.2.1**で解決されました。**Prisma Access 5.2.1**で解決された問題を参照してください。	ZTNAコネクタでコネクタIPブロックを変更または削除しようとすると、コミットとプッシュ後に変更が適用されません。 回避策:さらに2回コミットとプッシュの操作を実行して変更を適用します。
CYR-42312	NAT を介したユーザーID は、Colo-Connectではサポートされていません。
CYR-42259	RFC6598が有効になっている場合、明示型プロキシのプライベート アプリ アクセスは機能しません。
CYR-42244	合併および買収のビジネス継続性機能の一環としてPrisma Accessゲートウェイ名の変更を要求している場合、更新されたFQDNがStrata Cloud ManagerまたはPanoramaに表示されません。 回避策:Palo Alto Networksのアカウント チームに連絡し、SREケースを開いてゲートウェイのFQDNを更新します。
CYR-42188	明示型プロキシのプライベート アプリ アクセスを使用する場合、TCP経由のDNSは機能しません。ただし、UDP経由のDNSは正しく機能します。
CYR-42130	Colo-Connectのルーティング情報がServiceabilityコマンド領域に表示されません。
CYR-42018	IP最適化を有効にしている場合、GlobalProtectのTLS 1.3サポートはサポートされません。 回避策:TLSの最大バージョン1.2を使用します。
CYR-41990	IPv6からIPv6、またはIPv6からIPv4の送信元または宛先トラフィックは、URLフィルタリング アクションの［**Continue (**続行**)**］および［**Override (**オーバーライド**)**］をサポートしません。
CYR-41838	Prisma Access APIを使用して取得すると、リモート ネットワーク - ハイ パフォーマンス デプロイメントの出口IPアドレスが2回表示されます。 回避策:IPアドレスの重複は無視してください。

問題 ID	詳説
CYR-41813	ZTNAコネクタのオンボーディングが、スイス、フランス、カタール、台湾の拠点ではサポートされていません。回避策はありません。
CYR-41228	IP最適化を有効にしている場合、SPインターコネクト機能は使用できません。
CYR-41067	UIのPrisma Access Versionエリアに誤ったPrisma Accessのバージョンが表示されます。Strata Cloud Managerでは、バージョンは**[Manage (管理)]** > **[Configuration (設定)** > **[NGFW and Prisma Access (NGFWと**Prisma Access)]** > **[Overview (概要)]** > **[Prisma Access Version (Prisma Access**バージョン)]]Panoramaが管理するPrisma Accessでは、バージョンは [**Panorama (パノラマ)]** > **[Cloud Services (**クラウド サービス)]** > **[Configuration (設定)]** > **[Service Setup (**サービス セットアップ)** > **[Prisma Access Version (Prisma Access**バージョン)]**に表示されます。
CYR-40503	IPv6は南アフリカ中部およびカナダ西部ではサポートされていません。
CYR-40404	アプリケーションがコネクタ グループ内の一部のZTNAコネクタからアクセスできない場合、ワイルドカードに一致するFQDNターゲットがコネクタ グループに対して検出されないことがあります。 特定のグループ内のすべてのコネクタは、、グループ内で自動検出されるアプリケーションに対して、DNSを使用してアプリケーションを解決し、アプリケーションにアクセスできる必要があります。 回避策:Strata Cloud Managerからアプリケーション オブジェクトを必要なコネクタグループに関連付けます。
CYR-39930	Cortex Data Lakeのログは、IP最適化機能が有効になっているテナントからはエクスポートされません。
CYR-39795	Cloud Servicesプラグインのインストール後、明示型プロキシが有効になっていないにもかかわらず、__cloud_servicesユーザーによって明示型プロキシKerberosサーバ プロファイル（default_server_profile）がインストールされます。

問題 ID	詳説
	回避策:変更は無視してください。
CYR-39551	Prisma AccessダイナミックDNSの認証タイプをTSIGにセットアップしている場合は、TSIGキー ファイルの.keyファイルをアップロードする必要があります。キー ファイルの内容に非ASCII文字が含まれる場合、有効ではないと見なされます。TSIG認証用の.keyファイルを非ASCII文字で提供して［**OK**］をクリックすると、「`Please upload a file with the .key extension (.key`拡張子のファイルをアップロードしてください)」というエラーが表示されます。 回避策:有効なtsigキー ファイルを提供します。
CYR-39153	ZTNAコネクタ グループへのアップグレードを実行すると、アップグレード操作中に断続的に障害が発生することがあります。たとえば、影響を受けたコネクタのいくつかが後で正常にアップグレードされたにもかかわらず、アップグレードステータスは`partial_success`または`failed`と表示されます。 回避策:後でコネクタ グループのアップグレードを再試行してください。ZTNAコネクタが再チェックを行い、コネクタ グループの適切なステータスが表示されます。
CYR-39148	Colo-Connectを設定すると、Colo Connectデバイス グループへのコミットおよびプッシュ操作が断続的に失敗する場合があります。 回避策:Colo-Connectデバイス グループに対してコミットとプッシュ操作を再試行します。
CYR-39028	ZTNAコネクタを4.1からそれ以降のPrisma Accessバージョンにアップグレードし、ZTNAコネクタのアプリケーション プールがRFC6598アドレス空間（100.64.0.0/16および100.65.0.0/16）内で設定されている場合、MU-SPNでZTNAコネクタのトラフィックがブロックされることがあります。

問題 ID	詳説
	回避策:すべてのPrisma AccessテナントのSaaSエージェント バージョンの更新については、Prisma Accessチームにお問い合わせください。
CYR-38619	スイスとフランスでオンボードされているテナントは、ZTNAコネクタを使用できません。
CYR-38120	使用可能なすべてのロケーションが、モバイルユーザー—明示型プロキシのセットアップ ページのリストビューに表示されません。 回避策:マップ ビューを使用して、見つからない場所を選択します。
CYR-38076	正しいEBGPルーターのアドレスは、[Remote Networks Network Details (リモート ネットワークのネットワーク詳細)]ページ(**[Remote Networks Setup (**リモート ネットワークのセットアップ**)]** > **[Remote Networks (**リモート ネットワーク**)** > **[EBGP Router (EBGP**ルーター**)]**)には表示されず、代わりにリモート ネットワークのループバックIPアドレスが表示されます。
CYR-37983	モバイル ユーザー—GlobalProtectユーザーに対してIPv6を有効にしている場合、HIPレポートを取得するとクラッシュします。 回避策:GlobalProtectクライアントがipv6に対応している場合は、クライアントのIPv6アドレスを使用してHIPレポートを実行します。GlobalProtectクライアントがIPv4のみの場合は、クライアントのipv4アドレスを使用してHIPレポートを実行します。
CYR-37923	新しいURLカテゴリまたはセキュリティ ルールまたはEDLを作成した後、RBIセキュリティ ルール アソシエーションでそのオブジェクトを使用する前に、ローカルPanoramaコミットが必要です。
CYR-37906	既存のワイルドカード オブジェクトのポートを更新するときに、ポート間にスペースを入れると、`500`内部サーバーエラーが表示されます。

問題 ID	詳説
	回避策:ポートの間にスペースを入れないでください。たとえば、**1-2,80,100-300**の代わりに、**1-2,80,100-300**を入れます。
CYR-37887	ZTNAコネクタを30日間の試用期間で使用していて、ライセンスを購入していない場合、［**Enable ZTNA Connector (ZTNA**コネクタを有効にする**)]**ボタンをクリックすると、オンボーディングが失敗し、何か問題が発生したことを示すメッセージが表示されることがあります。 回避策:UIを更新して、ZTNAコネクタ機能のオンボーディングを完了します。
CYR-37826	2つ以上のZTNAコネクタ アプリケーションに同じFQDNがある場合、SD-WANポータルにアプリケーション カスタム ルールの競合メッセージが表示される可能性があります。 回避策:このメッセージは偽のものなので無視してかまいません。
CYR-37797	ステータス ページでは、プラグインのアップグレード後にワンタイム パスワード（OTP）の入力を求められます。 回避策:期限切れのライセンス キーを削除し、パノラマ証明書を削除し、ライセンスを取得して取得後にライセンス キーが有効かどうかを確認します。その後、OTPを生成して確認します。
CYR-37755	ZTNAコネクタでワイルドカード ターゲットを設定し、そのターゲットの結果として検出され、FQDNターゲットに追加されたアプリケーションのポートを変更しようとすると、名前が長すぎるというエラーが表示されます。 回避策:アプリケーション名は最大32文字まで指定できますが、ポート番号を変更すると、ZTNAコネクタ インフラストラクチャで名前が長くなりすぎます。このエラーが発生した場合は、アプリケーションの名前を短くしてください。

問題 ID	詳説
CYR-37706	明示型プロキシを使用すると、脅威ログが過剰に表示されます。 回避策:脅威ログは無視してください。これらのログは明示型プロキシ機能には影響しません。
CYR-37673	**[Panorama]** > **[Cloud Services (**クラウド サービス**)]** > **[Status (**ステータス**)]** > **[Status (**ステータス**)]** > **[Remote Browser Isolation (**リモート ブラウザ分離**)]** > **[Active Isolated Session (**アクティブ分離セッション**)]**リンクをクリックしても、Prisma Access Cloud ManagementまたはStrata Cloud Managerの**[Monitor (**監視**)]** > **[Subscription Usage (**使用**)**ページが開きません。
CYR-37500	リモート ネットワークでIPv6を有効にしている場合、エッジ ロケーションのパブリックIPv6アドレスは表示されません。
CYR-37466	Colo-Connectを有効にする場合は、VLANで双方向転送検出（BFD）を有効にしないでください。
CYR-37356	有効期限が切れた後（ライセンスの猶予期間を含む）にアプリ アクセラレーション ライセンスを更新した場合、更新はすぐには有効になりません。 回避策:ライセンス更新後、約1時間待ってからアプリ アクセラレーションをご利用ください。
CYR-37290	ZTNAコネクタをオンボーディングすると、ルートエラーによって要求されたクレームが表示されます。 回避策:エラーが発生したコネクタを削除して、新しいコネクタを作成します。
CYR-37227	IPサブネットベースのコネクタ グループの作成に失敗すると、グループが存在しないにもかかわらず、「グループが既に存在します」というメッセージが表示されることがあります。 回避策:IPサブネットベースのコネクタ グループに別の名前を使用します。
CYR-37208	Prisma Access Clean Pipeを使用する場合、 **[Network Details (**ネットワークの詳細**)]**ページ([**[Panorama]** >

問題 ID	詳説
	[Cloud Services (クラウド サービス**]** > **[Status (**ステータス**)]** > **[Status (**ステータス**)]** > **[Network Details (**ネットワークの詳細**)]**)にClean Pipeエントリが表示されません。
CYR-36749	NetFlowに関連するZTNAコネクタのフロー ログがStrata Cloud Managerのログ ビューアーで表示されない場合があります。
CYR-35506	テナントでIPv6を有効にしている場合、そのテナントを削除しても、そのテナントに割り当てられていたIPv6プレフィックスは解放されず、それらのプレフィックスは再度使用できません。 回避策:IPv6が有効になっているテナントは削除しないでください。
CYR-34999	Panorama Prisma Accessテナントの場合、ZTNAコネクタがオンボードされていると、サービス接続のプロビジョニング進捗（**[Panorama]** > **[Cloud Services (**クラウド サービス**)]** > **[Status (**ステータス**)]** > **[Status (**ステータス**)]** > **[Service Connections (**サービス コネクション**)]** > **[Provision Progress (**プロビジョニング進捗**)]**）にZTNAコネクタとサービス接続の両方のプロビジョニング進捗が表示されます。
CYR-34770	モバイル ユーザー向けのPrisma Access—GlobalProtectデプロイメントで複数のポータルを設定する場合、すべてのポータルでクライアント認証の下に認証プロファイルを設定する必要があります。認証プロファイルを少なくとも1つ設定しないと、認証クッキーが生成されず、マルチポータル機能は期待どおりに動作しません。
CYR-34720	GlobalProtect DDNS機能は、10.1.xを実行しているPanoramaを使用してクラウドサービスプラグインでPrisma Accessを管理する場合、機能しません。
CYR-33877	明示型プロキシのセットアップ中に、アドレス オブジェクトの認証をスキップするために**[Skip authentication (**認証をスキップ**)]**を選択し、後でそのアドレス オブジェクトの**[Skip authentication (**認証を

問題 ID	詳説
	スキップ)]の選択を解除して認証を有効にする場合、変更を行ってから変更をコミットおよびプッシュして変更が有効になるまで最大24時間かかることがあります。
CYR-33471	マルチテナンシーを有効にした場合は、新しいサブ テナントを作成し、モバイル ユーザー—GlobalProtect、リモート ネットワーク、およびColo-Connectデバイス グループを設定してから、Colo-Connectサブネットおよび VLANを設定すると、「`Unable to retrieve last in-sync configuration for the device` (デバイスの最終同期設定を取得できません)」エラーで部分的にコミットが失敗します。 回避策:Colo-Connectを初めて設定するときは、部分コミットではなくコミットとプッシュの操作を実行します。
CYR-33454	マルチテナント デプロイメントでPrisma Accessを設定し、コミットとプッシュを実行してからColo-Connectを設定すると、変更をコミットしてプッシュする選択肢がグレー表示されます。 回避策:**[Commit (コミット)]** > **[Commit to Panorama (パノラマにコミット)]**をクリックし、**[Commit (コミット)]** > **[Push to Devices (デバイスにプッシュ)]**ををクリックし、**[Edit Selections (選択範囲の編集)]**をクリックして、**[Push Scope (スコープのプッシュ)]**で**[Colo-Connect]**が選択されていることを確認し、コミットとプッシュ操作を再試行します。
CYR-33199	Kerberos認証済みユーザーの場合、現在のユーザー数と90日間のユーザー数が正しくありません。
CYR-33145	いずれかのサービス タイプのPrisma Accessライセンスが期限切れになると、[Commit All (すべてコミット)]操作は失敗し、一般的なコミット失敗のエラーメッセージが表示されます。 回避策:コミットを実行する前に、すべてのPrisma Accessライセンスが期限切れになっていないことを確認してください。

問題 ID	詳説
CYR-32687	明示型プロキシでエージェントまたはKerberos認証を使用する場合、EDL、**IP**ワイルドカード マスクと**FQDN**タイプのアドレス オブジェクト、およびダイナミック アドレス グループが復号化ポリシーで機能しません。 回避策:復号化ポリシーでIPネットマスク、IP範囲、またはアドレス グループのアドレスオブジェクトを使用します。

CYR-32666	Colo-Connect設定を含む以前に保存したPanorama設定をインポートする場合、または以前に保存した設定から元に戻す場合、以下の条件があるとエラーが表示されます。
	
	• Colo-Connectサービス接続が設定されている設定をロードしています。
	• 空のPrisma Access設定をロードしています。
	• 以前に保存した設定を復元する場合、以下の条件があります。
	  • 現在の設定にColo-Connect設定（サービス接続あり）が存在し、元に戻す設定にColo-Connect設定が存在しません。
	  • 現在の設定にColo-Connect設定がなく、元に戻す設定にColo-Connect設定（サービス接続あり）が存在します。
	  • Colo-Connect設定（サービス接続あり）が現在の設定に存在し、元に戻す設定にも存在します。
	
	回避策:Colo-Connect サービス接続は、対応するVLANがActive状態でない限りオンボードできません。Panoramaイメージをエクスポートまたは元に戻す前に、Colo-Connectサービス接続をすべて削除します。新しいイメージをインポートした後、Colo-Connectサービス接続を再作成します。

CYR-32661	GlobalProtect がプロキ シモードまたはトンネルとプロキシ モードで接続されている場合、ユーザーのログインは現在のユーザの数または過去90日間のモバイル

問題 ID	詳説
	ユーザー—明示型プロキシでログインしたユーザーの数にカウントされません。
CYR-32564	ZTNAコネクタ アプリのトラフィックは脅威として検出され、デフォルトのURLカテゴリが使用されている場合、Prisma Access Cloud Management用にドロップされます。 回避策:必要に応じて、以下の手順の1つ以上を実行します。 1. カスタムURLカテゴリを作成し、ZTNAコネクタのオンボード アプリケーション用のアプリケーションFQDNを追加します。 2. デフォルトのプロファイル グループを使用している場合は、新しいグループのクローンを作成し、手順1で作成したカスタムURLカテゴリをアタッチします。カスタム プロファイル グループを使用している場合は、手順1で作成したカスタムURLカテゴリをアタッチします。 3. ZTNAコネクタ アプリケーション宛てのトラフィックを許可するため、作成したセキュリティ ポリシーにクローン プロファイル グループまたはカスタム プロファイル グループのいずれか（手順2）をアタッチしてください。
CYR-32511	IPv6が無効になっていても、IPv6 DNSアドレスを設定できます。
CYR-32431	明示型プロキシを設定する場合、[Authentication Settings (認証設定)]で[Trusted Source Address (信頼できる送信元アドレス)]の値を追加し、他の設定を行ってから[Authentication Setting (認証設定)]タブに戻ると、信頼できる送信元アドレスが正しく表示されないことがあります。 回避策:Prisma Accessを管理しているPanoramaを更新し、[Authentication Settings (認証設定)]タブに戻ってアドレスを確認します。
CYR-32191	ZTNAコネクタはマルチテナント環境ではサポートされていません。

問題 ID	詳説
CYR-32004	Prisma Accessで現在サポートされているIPSecプロファイルの数に制限があるため、ZTNAコネクタをデプロイする場合、テナントごとに最大100個のコネクタVMをオンボードできます。
CYR-31603	AWS Auto Scaleに対応したコネクタ グループでは、2つのインターフェースを持つ ZTNAコネクタはサポートされていません。これは、両方のインターフェースを同じサブネットに結び付けるAWS Auto Scaleグループの制限によるものです。詳細については、この記事を参照してください。 回避策:2つのインターフェースを持つZTNAコネクタは、AWS Auto Scaleが有効になっていないコネクタ グループでサポートされています。2つのインターフェースを持つすべてのZTNAコネクタが、AWS Auto Scaleに対して有効になっていないコネクタ グループに含まれていることを確認します。
CYR-31187	GlobalProtect for Always-On Internet Security機能のPrisma Access明示型プロキシ接続機能を使用するには、モバイル ユーザー—GlobalProtecとモバイル ユーザー—明示型プロキシの両方にコミットしてプッシュしない限り、デフォルトのPACファイルURL が正しく入力されません。 回避策:コミットとプッシュを行う場合、GlobalProtectでPrisma Access明示型プロキシ接続を設定する際に、スコープのプッシュで[Mobile Users—GlobalProtect (モバイル ユーザー—GlobalProtect)]と[Mobile Users—Explicit Proxy(モバイル ユーザー—明示型プロキシ)]の両方を選択するようにしてください。
CYR-30414	テナントが1つだけのマルチテナント デプロイメントで複数のポータルを有効にし、その単一テナントで複数のポータル機能を無効にした場合、UIで両方のポータルを表示できます。 回避策:Prisma Accessを管理するPanoramaでCLIセッションを開き、以下のコマンドを入力します。次に、Panoramaでローカルコミットを実行します:

問題 ID	詳説

	`set plugins cloud_services multi-tenant tenants` <*tenant_name*> `mobile-users multi-portal-multi-auth no`
	
	`request plugins cloud_services gpcs multi-tenant-name` <*tenant_name*> `multi_portal_on_off`

CYR-30044	新しい明示型プロキシのデプロイメントで、事前定義済みのEDLが［Block Settings (ブロック設定)］リストに入力されていません。 回避策:明示型プロキシのデプロイメントをオンボードし、［Commit and Push (コミットしてプッシュ)］操作を実行した後、ブロックの［Settings (設定)］でEDLを更新します。
CYR-29964	証明書を生成するためのCertificate Signing Request (証明書署名要求 - CSR)を再利用しようとすると、"`Requested entity already exists (`要求されたエンティティは既に存在します`)"`という エラーが発生します。 回避策:CSRを再使用しないでください。
CYR-29933	**`verdicts:all -X "DELETE"`**APIコールを1時間に2回以上使用しようとすると、`{"code" :8 , " message" :"Too many requests (`要求が多すぎます`)"`エラーが発生します。 回避策:このAPIコールは1時間に2回以上使用しないでください。
CYR-29700	マルチテナントのPrisma Access Panoramaが管理するマルチテナント デプロイメントで複数のGlobalProtectポータルを設定する場合、ユーザー名単位での変更のコミットが`"global-protect-portal-8443 should have the value "GlobalProtect_Portal_8443" but it is [None] (global-protect-portal-8443`の値は`"GlobalProtect_Portal_8443"`であるべきですが`"None"`になっています`)"`というエラーで失敗します。

問題 ID	詳説
	回避策:複数のGlobalProtectポータルを有効にしていて、Prisma Accessのマルチテナント デプロイメントがある場合は、ユーザーごとにコミットするのではなく、[Commit All (すべてコミット)]操作を実行します。
CYR-29160	Prisma Accessを管理するPanoramaがFIPSモードで設定されていて、**[Generate Certificate for GlobalProtect App Log Collection and Autonomous DEM (GlobalProtect**アプリケーションのログ収集と自律型**DEM**の証明書の生成**)]**を選択すると、証明書がダウンロードされません。 回避策:この機能は、Prisma Accessデータプレーンが10.2.4にアップグレードされるまで、FIPSモードのPanoramaアプライアンスでは使用できません。
CYR-26112	Net Interconnectライセンスがない場合、シアター内のすべてのリモート ネットワークはフルメッシュ構造になっていますが、シアターのサービス接続をオンボードしていない場合、他のシアターのリモート ネットワークからリモート ネットワークにアクセスできません。 回避策:Net Interconnectライセンスを購入するか、シアターのサービス接続をオンボードして、リモート ネットワークが他のシアターと通信できるようにします。

動的な特権アクセスに関する既知の問題

問題 ID	詳説
PANG-4881	ユーザーがPrisma Access Agentの認証に使用したWebブラウザが開いたままの場合、WebブラウザからPrisma Access Agentへのトラフィックは、転送プロファイルの設定に関係なくトンネル経由で送信されます。
PANG-4870	Prisma Access Agent がインストールされているmacOSデバイスでは、Prisma Access Agentのセキュリティ拡張機能のフル ディスク アクセスを削除すると（以前にフル ディスク アクセスを許可した

問題 ID	詳説
	後）、Prisma Access Agent が無効モードのままになります。 回避策:［**System Settings (システム設定)]** > **[Privacy & Security (プライバシーとセキュリティ)]** >［**Full Disk Access (フル ディスク アクセス)]**を選択し、アプリのリストから［**securityExtension**］を有効にして、セキュリティ拡張機能へのアクセスを許可します。
PANG-4825	転送プロファイルを設定する場合、送信元アプリケーション、宛先ドメイン、およびIPアドレス（ルート）に大量の転送ルールを設定すると、CPU使用率が高くなる可能性があるという問題があります。 回避策:送信元アプリケーション、宛先ドメイン、およびIPアドレスには、100を超える転送ルールを設定しないでください。
NETVIS-1363	Insights on Strata Cloud Managerでは、ユーザー詳細ページの**[Project Connectivity Hisotry (プロジェクト接続履歴)]**ビューに、Prisma Access Agentユーザーが接続している場合、プロジェクト名のみが表示され、その他の詳細情報は表示されません。ユーザーが接続していないときは、[Project Connectivity Hisotry (プロジェクト接続履歴)]は空白になります。
NETVIS-1293	Insightsで、**[Time Range (時間範囲)]**が**[Past 3 Hours (過去3時間)]**、**[Past 1 Hours (過去1時間)]**、および**[Past 15 Minutes (過去15分)]**に設定されている場合、**[Project Connectivity History (プロジェクト接続履歴)]**に正しいデータが表示されません。
NETVIS-1263	Insightsで、[Project (プロジェクト)]タブに表示される接続ユーザー数が正確でない場合があります。[Project (プロジェクト)]タブの接続ユーザー数と[Users (ユーザー)]タブの接続ユーザー数が一致しない場合があります。たとえば、同じユーザーが異なるデバイス上の2つのプロジェクトに接続されている場合、［Project (プロジェクト)］タブの接続ユーザー数と［Users (ユーザー)］タブの接続ユーザー数が一致しません。
NETVIS-1207	Insightsでは、［Project (プロジェクト)］タブにプロジェクトに設定されているすべてのIPプールが表示さ

問題 ID	詳説
	れるわけではありません。使用中のIPプールだけが表示されます。
EPM-1589	転送プロファイルを設定する場合、Strata Cloud Managerではワイルドカードを使用してIPアドレスを設定することができますが、宛先IPアドレスにワイルドカード文字**10.*.*.***などを使用すると、転送プロファイルで一貫性のない動作を引き起こすため、サポートされていません。
EPM-1399	Strata Cloud Managerの［Dynamic Privilege Access (動的な特権アクセス)］ページの［**Projects (**プロジェクト**)**］タブでのプロジェクト名の変更は、現時点ではサポートされていません。 回避策**:**プロジェクトの名前を変更するには、既存のプロジェクトを削除してAccess Agentのプッシュ設定を実行した後、新しい名前でプロジェクトを作成し、Access Agentのプッシュ設定を実行します。
EPM-646	動的な特権アクセスが有効になっているPrisma Accessテナントでは、最初にプロジェクトを何も設定せずにPrisma Access Agentインフラ設定をプッシュしようとすると、設定プッシュが失敗します。 回避策:プッシュ設定を行う前に、少なくとも1つのプロジェクトを設定します。
DRS-4691	Cloud Identity EngineまたはStrata Cloud Managerでテキスト検索オプションを使用してユーザー グループを検索する場合は、ユーザー グループ名を二重引用符で囲みます。例えば、EXAMPLE.User_Groupという名前のユーザー グループを検索する場合は 、"EXAMPLE.User_Group"と入力します。
DRS-4406	Strata Cloud Managerでプロジェクトを設定する場合、**[User group (**ユーザー グループ**)]**名の一部を指定してユーザー グループを検索することはできません。 回避策**:**ユーザー グループを検索するには、完全なユーザー グループ名を入力します。

問題 ID	詳説
DOCS-5681	動的な特権アクセス対応テナントでのZTNAコネクタの有効化は、Prisma Access 5.2ではサポートされていません。 動的な特権アクセス対応テナントでZTNAコネクタを有効にすると、ルーティングに問題が発生する可能性があります。また、Strata Cloud Managerは一度作成したZTNA Connectorの削除をサポートしていないため、サービスに影響が出る可能性があります。
DOCS-5611	動的な特権アクセス用にCloud Identity Engineでユーザー グループ マッピングを許可する場合、Prisma Accessで認証に使用するSAML属性を選択するときは、必ず**/identity/claims/name**を含むユーザー名属性を選択してください。 誤ったユーザー名属性を選択すると、ユーザーはプロジェクトに対して認証できなくなります。
DOCS-5463	[Agent Settings (エージェントの設定)]ページで**[Collect HIP Data (HIP**データの収集**)]**オプションが有効になっていないと、ランダムなトンネル切断が発生する可能性があるという問題が存在します。そのため、[Access Agent Settings (Access Agentの設定)]ページの[Host Information Profile (ホスト情報プロファイル)(HIP)]セクションで**[Collect HIP Data (HIP**データの収集**)]**を無効にしないでください。
DOCS-3650	動的な特権アクセス対応のPrisma AccessテナントでCloud Identity Engine認証を機能させるには、ユーザー グループがIDプロバイダー（IdP）内の複数のSAMLアプリケーションにマップされていないことを確認します。 複数のアプリがユーザー グループにマッピングされている場合、一意のマッピングがないため、Cloud Identity Engineは認証時にどのSAMLアプリに接続するかを判断できません。
ADI-33262	動的な特権アクセスが有効になっているPrisma Accessテナントでは、最初にStrata Cloud Managerでプロジェクトを設定しないと、モバイル ユーザー コンテナ > **Access Agent**の設定プッシュが失敗します。

問題 ID	詳説
	回避策:プッシュ設定を行う前に、少なくとも1つのプロジェクトを設定します。
ADI-31750	プロジェクトごとにサポートされるIPプールの数は50です。プロジェクトあたりのIPプール数が50を超えると、パフォーマンスに影響が出ます。 回避策:プロジェクトあたり50個以下のIPプールを割り当てます。
ADI-31601	動的な特権アクセス対応テナントでは、プッシュ設定が汎用エラーで失敗することになるにもかかわらず、Strata Cloud Managerを使用してプロジェクトごとに100を超える IP プールを設定できます。 回避策:プロジェクトごとに100を超えるIPプールを設定しないでください。
ADI-31538	転送プロファイルをセットアップする際に、転送プロファイルの**[Type (種類)]**が「Prisma Access Agent」ではなく「ZTNA Agent」と表示される問題が存在します。また、**[Add Forwarding Profile (**転送プロファイルの追加**)]**を選択すると、ドロップダウンには「Prisma Access Agent」ではなく「ZTNA Agent」と表示されます。 回避策:なし。転送プロファイルの種類は今後「Prisma Access Agent」に変更される予定です。
ADI-31523	特殊文字を含む説明を含むスニペットを作成しないでください。**! ~ @ # $% ^ & * ( ) _ +** などの特殊文字を含むスニペット記述はサポートされていません。
ADI-31306	転送プロファイルをセットアップする場合、[Forwarding Profile (転送プロファイル)]ページの**[Traffic Enforement (**トラフィック適用**]**セクションのすべてのオプションがデフォルトで有効になっているという問題があります。これらのオプションをすべてデフォルトで有効にすると、予期しない動作や望ましくない動作を引き起こす可能性があります。

問題 ID	詳説
	回避策:動的な特権アクセスのこれらのオプションを無効にします。
ADI-31305	転送プロファイルをセットアップする際に、［**Enforce FQDN DNS resolution using tunnel DNS servers (**トンネル**DNS**サーバーを使用して**FQDN DNS**解決を適用する**)]**オプションと［**Resolve all FQDNs using DNS servers that are assigned by the tunnel (Windows agents only) (**トンネルによって割り当てられた**DNS**サーバーを使用してすべての**FQDN**を解決する（**Windows**エージェントのみ）］オプションが［Forwarding Profile (転送プロファイル)］ページの［**Traffic Enforcement (**トラフィックの適用**)]**セクションに表示される問題があります。 これら2つのオプションは、転送プロファイル ルールを使用して意図した機能を設定することができるため、表示しないでください。
ADI-30902	Strata Cloud Managerは、Cloud Identity Engineディレクトリのユーザーおよびユーザーグループの情報を、動的な特権アクセス プロジェクト設定、Prisma Access Agent設定、セキュリティ ポリシー、段階的ロールアウト設定など、複数の設定で使用します。これらの設定を行った後、Cloud Identity Engineからディレクトリを削除しても、それらのユーザーやユーザー グループを参照するStrata Cloud Managerの設定を削除しないと 、 「500 Internal Server Error (500内部サーバーエラー)」などの予期しないエラーが発生することがあります。 回避策:Cloud Identity Engineからディレクトリを削除する場合は、そのディレクトリ内のユーザーとユーザーグループを参照するStrata Cloud Managerの設定も削除する必要があります。
ADI-30468	Strata Cloud Managerの［**Access Agent] > [Infrastructure Settings (**インフラ設定**)]**ページで、［**Prisma Access Managed (Prisma Access**管理**)]**と**[OnPrem DHCP Server (OnPrem DHCP**サーバー**)]**の両方のオプションが［Client IP Pool Allocation］セクションに表示される問題があります。

問題 ID	詳説
	動的な特権アクセスが有効になっている一般提供Prisma Accessテナントでユーザーをプロビジョニングする場合は、**[OnPrem DHCP Server (OnPrem DHCPサーバー)]**を選択しないでください。一度設定を保存すると元に戻せないからです。動的な特権アクセスの一般提供テナントでは**OnPrem DHCP**サーバーはサポートされておらず、将来のリリースでStrata Cloud Managerから削除される予定です。**[OnPrem DHCP Server (OnPrem DHCPsa-ba-)]**を選択すると、テナントは基本的な動的な特権アクセス ワークフローで使用できなくなります。
ADI-29665	プロジェクト名に特殊文字を使用しないでください。特殊文字を使用すると、プロジェクト設定を保存しようとしたときに、Strata Cloud Managerによって「Malformed Request (不正な形式の要求)」というエラー メッセージが発行されます。
ADI-29434	Strata Cloud Managerの［Agent Settings (エージェント設定)］ページで、**[Session timeout (**セッションタイムアウト**)]**の推奨値は7日です。
ADI-29272	スニペットを作成するときに、**[Add prefix to object names (**オブジェクト名にプレフィックスを追加**)]**オプションを無効にすると、予期しない動作が発生する可能性があるため、2つの異なるスニペットでエージェント設定名を重複して使用しないようにしてください。
ADI-26493	Strata Cloud Managerの［**Access Agent]** > **[Infrastructure Settings (**インフラ設定**)**］で、［Client IP Pool Allocation (クライアントIPプールの割り当て)］セクションの［**OnPrem DHCP Server (OnPrem DHCP**サーバー**)]**オプションが選択できません。**[OnPrem DHCP Server (OnPrem DHCP**サーバー**)]**は動的な特権アクセスに対応していないため、これは意図したとおりに機能しています。 このオプションは、動的な特権アクセスが有効になっている既存のPrisma Accessテナントが正しく機能するように、**[OnPrem DHCP Server (OnPrem DHCP**サー

問題 ID	詳説
	バー)(Preview Only)(プレビューのみ)]に名前が変更されます。
ADI-24562	プロジェクトが異なる設定スニペットから設定されていた場合、同じドメインとユーザー グループを持つ複数のプロジェクトを作成できるという問題があります。一部のStrata Cloud Managerワークフローで予期しない動作を引き起こす可能性があるため、この設定は避けてください。 回避策:同じドメインとユーザー グループを使用して異なるプロジェクトを設定しないでください。

Prisma Access5.2.1の既知の問題

問題 ID	詳説
CYR-47139	ZTNAコネクタ アプリケーション ブロック、コネクタ ブロック、またはIPサブネットが、明示型プロキシ アドレスと競合するRFC6598アドレスで設定されている場合、ZTNAコネクタ-明示型プロキシ統合でZTNAコネクタが無効になります。 回避策:ZTNAコネクタを明示型プロキシで使用するように設定する場合は、アプリケーションまたはコネクタブロックに100.64.0.0/15、100.72.0.0/15、または100.88.0.0/15サブネットを使用しないでください。
CYR-46759	DNSクエリのUDP設定は、明示型プロキシでは適用されません。
CYR-46627	[**Accept Default Route over Service Connection (**サービスコネクション経由のデフォルト ルートを受け入れる**)]**が有効になっている場合、明示型プロキシはサポートされません。
CYR-46349	リモート ネットワークをトラフィック ステアリング付きの明示型プロキシで中国で使用する場合、URLカテゴリでトラフィック ステアリング ルールを設定しないでください。

問題 ID	詳説
CYR-46191	Explicit Proxyがプライベート アプリケーション アクセスを有効にして設定されており、ZTNAコネクタが設定に追加されている場合、PanoramaまたはStrata Cloud Managerからの別のコミットが必要になることがあります。 回避策:Prisma Accessを管理するPanoramaまたはStrata Cloud Managerの明示型プロキシ設定に小さな修正を加え、変更をプッシュします。

Prisma Accessで解決された問題

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	❑ Prisma Accessライセンス ❑ Minimum Required Prisma Access Version 5.2または5.2.1 PreferredまたはInnovation

以下のトピックでは、Prisma Access5.2およびPrisma Access5.2.1で対処された問題について説明します。

Prisma Access 5.2.1で解決された問題

問題 ID	詳説
CYR-45847	サービス サブネットを変更してPrisma Access GlobalProtectゲートウェイで更新されたとおりに変更した場合にNATが正しく実装されていないためにGlobalProtectトンネルがダウンする問題を修正しました。
CYR-45341	Colo-Connectデバイス グループへのコミット ジョブとプッシュ ジョブがタイムアウトし、VLANが削除されない問題を修正しました。
CYR-44391	中国での明示型プロキシのデプロイメントで、認証にCloud Identity EngineまたはSAMLの使用がサポートされていない問題を修正しました。
CYR-43690	ZTNAコネクタでコネクタIPブロックを変更または削除しようとすると、コミットとプッシュ後に変更が適用されない問題を修正しました。
CYR-42919	ZTNAコネクタでコネクタIPブロックを変更または削除しようとすると、コミットとプッシュ後に変更が適用されない問題を修正しました。

Prisma Access5.2.0-h14で解決された問題

問題 ID	詳説
CYR-46782	GlobalProtect DDNS機能において、非ASCII文字を含みPanoramaキャッシュにあるドメイン名がnsupdateコマンドの処理中にエラーを起こす問題を修正しました。
CYR-46358	Colo-Connectの変更があるクラウド サービス プラグインへのアップグレード中に、Prisma Access Edition以外のテナントでプラグイン検証失敗エラーが発生する問題を修正しました。
CYR-45949	UIがPrisma Accessインフラにアクセスできない場合、［Mobile Users (モバイル ユーザー)］-［Explicit Proxy onboarding location (明示型プロキシのオンボーディング場所)］タブが読み込まれず、バッファリングし続ける問題を修正しました。
CYR-45932	ワンタイム プッシュ(OTP)検証が以下のエラーで失敗する問題を修正しました: `[get-panorama-cert.py:288] <class 'AttributeError'>` (「`Pan_Plugin_Client`」オブジェクトに属性「`whitelist_keys`」がありません
CYR-44969	ロールベースの管理者を使用して作成されたユーザーが、UIでクラウド サービスの設定を確認できない問題を修正しました。
CYR-44766	共通APIを使用したIKEおよびIPSec暗号プロファイルの削除に失敗し、プロファイルが設定から削除されない問題を修正しました。

Prisma Access5.2.0で解決された問題

問題 ID	詳説
CYR-45112	クラウド サービス プラグインをバージョン5.1.0以降にアップグレードすると、外部

問題 ID	詳説
	ゲートウェイの設定がグレーアウトされる問題を修正しました。
CYR-44598	Panorama Managed Prisma Accessのデプロイメントで、Strata Logging Serviceのステータスに例外<*customer-id*>エラーが表示される問題を修正しました。
CYR-43673	APIからの無効な設定がすべてGETコールを介してシステム管理者にリレー バックされる問題を修正しました。
CYR-43400	**[Preserver User ID (ユーザーIDを保持)]**がオンになっているZTNAコネクタ グループにオンボードされているコネクタで、内部インターフェースからデータセンター アプリへの**[Action (アクション)]** > **[Diagnostics (診断)]** > **[ping]**が機能しない問題を修正しました。
CYR-43280	不正なbase64データ エラーにより、変更がある場合でもDSPが差分を生成できない問題を修正しました。
CYR-43262	リモート ネットワーク オンボーディングのリモート ネットワークAPI要求がペイロードにBGP設定が含まれている場合にプラグインでコミット検証エラーを投げてしまう問題を修正しました。
CYR-43222	ユーザーIDベースのZTNAコネクタ グループに割り当てられたアプリケーション ターゲットが、**icmp ping**のプローブ タイプをサポートしていなかった問題を修正しました。
CYR-42377	リモート トラブルシューティングおよび更新のダイナミックDNS登録サポートを設定する際に、**[Authentication Type (認証タイプ)]**が**[Kerberos]**の場合、Prisma Accessを管理するPanorama上で暗号化されていないKerberosキー ファイルをアップロードできない問題を修正しました。

問題 ID	詳説
	プラグイン バージョン5.2.0以上でPanoramaが管理するデプロイメントを実行しており、Kerberos認証タイプを選択した場合は、DNSサーバーから取得したKerberosキーのbase64エンコード文字列を含む.keyファイルを介して認証キーをアップロードします。次に例を示します。 "ABCDEFGHIJKLMNOPQRSTUV5WXYZOUy5DT00ADUFabcD プラグイン バージョン5.1.0未満のPanoramが管理するデプロイメントを実行しており、Kerberos認証タイプを選択した場合は、エンコードされていないKerberos keytabファイルがDNSサーバーから取得された.keyファイルを介して認証キーをアップロードします。
CYR-42191	ダイナミックDNSサポートのセットアップ時に、有効なKerberosファイルが正しくアップロードされず、システム設定に保存されない問題を修正しました。
CYR-41740	同じリージョンに短期間に100個以上のコネクタがオンボードされていた場合、一部のZTNAコネクタを介したプライベート アプリへのアクセスが機能しないことがある問題を修正しました。
CYR-38418	IPv6を有効にした後、Prisma Accessデータプレーンの10.2.8-h1から10.2.8-h2へのアップグレードに失敗する問題を修正しました。
CYR-38386	オートスケーリング操作により、より多くのモバイル ユーザー ゲートウェイが作成された後、コミットおよびプッシュ操作が失敗する問題を修正しました。
CYR-37913	コンピューティングでトラフィック レプリケーションを無効にし、同じコンピューティングで再度有効にすると、トラフィック レプリケーション機能に影響が及び、モバイル ユーザーまたはリモート ネットワーク トラ

問題 ID	詳説
	フィックが複製されず、コミットまたは設定エラーが表示されない問題を修正しました。
CYR-37791	ユーザーが別のプロジェクトに切り替えて同じPrisma Accessの場所に接続した後、Strata Cloud Managerの［Monitor (モニター)］ > ［User (ユーザー)］ページに、以下の時間範囲で切り替えた正しいプロジェクト名が反映されない問題を修正しました。3時間、24時間、7日、30日。
CYR-36930	GlobalProtectモバイル ユーザーがデュアル スタック（IPv4とIPv6）を有効にしていて、IPv6を有効にし、IPv6を有効にしたPrisma Access GlobalProtectロケーションに接続し、その後そのロケーションに対してIPv6が無効化された場合に、デュアルスタック ユーザーがその場所に接続できない問題を修正しました。
CYR-27734	リモート ネットワーク デバイス グループのPanoramaで、未使用のルール使用状況統計のポリシー オプティマイザーが表示されない問題を修正しました。

Prisma Access 5.2および5.2.1のPanoramaサポート

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	❑ Prisma Accessライセンス ❑ Minimum Required Prisma Access Version5.2または5.2.1のPreferred (推奨)またはInnovation (革新)

Prisma Access (Managed by Panorama)リリース5.2および5.2.1では、クラウド サービス プラグイン**5.2**クラウド サービス プラグインを使用します。Prisma Access5.2.1は、5.2プラグインのホットフィックス バージョンを使用してアクティベートされます。Panoramaを使用してPrisma Accessを管理していて、5.2プラグインにアップグレードする必要がある場合は、次の操作を行う必要があります。

1. PanoramaがPrisma Access 5.2 Preferred (推奨)とInnovation (革新)をサポートするために必要なソフトウェアバージョンを確認する
2. クラウド サービス プラグインに必要なアップグレード パスの決定
3. クラウド サービス プラグインのアップグレード

Panoramaが管理するPrisma Access 5.2および5.2.1に必要なソフトウェア バージョンと推奨ソフトウェア バージョン

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	❑ Prisma Accessライセンス ❑ Minimum Required Prisma Access Version5.2または5.2.1のPreferred (推奨)またはInnovation (革新)

Prisma Access5.2.1のPreferred (推奨)とInnovation (革新)の推奨ソフトウェア バージョン

Prisma Access5.2.1には2つのバージョンがあります。

- 5.2.1 Preferred (推奨)はPAN-OS 10.2.10データプレーンを実行します。デプロイメント環境で下位のデータプレーン バージョンを実行している場合、5.2.1の Preferred (推奨)機能を実装するには、PAN-OS 10.2.10へのデータプレーンのアップグレードが必要です。
- 5.2.1 Innovation (革新)はPAN-OS 11.2.4データプレーンを実行します。5.2 Innovation機能を実装するには、PAN-OS 11.2.4へのアップグレードが必要です。

5.2.1 Innovationの新Prisma Access機能については、 Prisma Accessではプラグインをインストールする前に **Prisma Access**を以下のバージョンにアップグレードすることをお勧めします 。

Prisma Accessバージョン	クラウドサービス プラグインのバージョン	**5.2.1**に必要なデータプレーンのバージョン	**GlobalProtect**の推奨バージョン	推奨**Panorama**バージョン
5.2.1	5.2.0のホットフィックス	PAN-OS 10.2.10（5.2.1 Preferred (優先)に必要） PAN-OS 11.2.4（5.2.1 Innovation (革新)に必要）	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 (推奨)とInnovation (革新)の推奨ソフトウェア バージョン

Prisma Access 5.2には2つのバージョンがあります。

- 5.2 Preferred (推奨)はPAN-OS 10.2.10データプレーンを実行します。デプロイメント環境で下位のデータプレーン バージョンを実行している場合、5.2 Preferred (優先)機能を実装するには、PAN-OS 10.2.10へのデータプレーン アップグレードが必要になることがあります。既存のお客様は、Prisma Access 5.2の機能にデータプレーンのアップグレードが必要かどうかについて、Prisma Access5.2.1 Preferred機能とInnovation機能のインフラストラクチャ、プラグイン、およびデータプレーンの依存関係を参照してください。
- 5.2 Innovation (革新)は11.2.3のPAN-OSデータプレーンを実行します。5.2 Innovation機能を実装するには、PAN-OS 11.2.3へのアップグレードが必要です。

5.2 Innovationの新Prisma Access機能については、 Prisma Accessではプラグインをインストールする前に **Prisma Access**を以下のバージョンにアップグレードすることをお勧めします 。

Prisma Accessバージョン	クラウドサービスプラグインのバージョン	**5.2**に必要なデータプレーンのバージョン	**GlobalProtect**の推奨バージョン	推奨**Panorama**バージョン
5.2	5.2	PAN-OS 10.2.10（5.2 Preferredに必要） PAN-OS 11.2.3（5.2 Innovationに必要）	6.0.7+ 6.1.3+ 6.2.1+	10.2.10+ 11.0.1+ 11.1.0 11.2.3

Panoramaが管理するPrisma Accessのアップグレードに関する考慮事項

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	❑ Prisma Accessライセンス ❑ Minimum Required Prisma Access Version5.2または5.2.1のPreferred (推奨)またはInnovation (革新)

クラウド サービス プラグインをPrisma Access 5.2または5.2.1にアップグレードするには、以下のいずれかのアップグレード パスを使用します。Panoramaで現在のプラグイン バージョンを確認するには 、 **[Panorama]** > **[Cloud Services (クラウド サービス)]** > **[Configuration (設定)]** > **[Service Setup (サービスのセットアップ)]** ］ を選択し、 **[Plugin Alert (プラグイン アラート)]**エリアでプラグイン バージョンを確認します。

アップグレードの際は、各プラグインのバージョンの最低Panoramaバージョンを必ず守ってください。

インストールされているクラウド サービス プラグインのバージョン	対象バージョン	プラグインのアップグレード パス
5.1	5.2または5.2.1	プラグインをPrisma Access 5.1からPrisma Access 5.2にアップグレードし、変更をコミットしてプッシュします。
5.0	5.2または5.2.1	1. プラグインをPrisma Access 5.0からPrisma Access 5.1にアップグレードし、変更をコミットしてプッシュします。 2. プラグインをPrisma Access 5.1からPrisma Access 5.2にアップグレードし、変更をコミットしてプッシュします。
4.1と4.2	5.2または5.2.1	1. プラグインをPrisma Access 4.1からPrisma Access 5.0にアップグレードし、変更をコミットしてプッシュします。

インストールされているクラウド サービス プラグインのバージョン	対象バージョン	プラグインのアップグレード パス
		2. プラグインをPrisma Access 5.0からPrisma Access 5.1にアップグレードし、変更をコミットしてプッシュします。 3. プラグインをPrisma Access 5.1からPrisma Access 5.2にアップグレードし、変更をコミットしてプッシュします。
4.0	5.2または5.2.1	1. プラグインをPrisma Access 4.1にアップグレードし、変更をコミットしてプッシュします。 2. プラグインをPrisma Access 5.0にアップグレードし、変更をコミットしてプッシュします。 3. プラグインをPrisma Access 5.0からPrisma Access 5.1にアップグレードし、変更をコミットしてプッシュします。 4. プラグインをPrisma Access 5.1からPrisma Access 5.2にアップグレードし、変更をコミットしてプッシュします。
3.0、3.1、3.2 Preferred	5.2または5.2.1	1. (3.0プラグインのみ)プラグインをPrisma Access 3.1にアップグレードし、変更をコミットしてプッシュします。 2. (3.1プラグインのみ)プラグインをPrisma Access 3.2または3.2.1にアップグレードし、変更をコミットしてプッシュします。 3. プラグインをPrisma Access 3.2または3.2.1にアップグレードし、変更をコミットしてプッシュします。 4. プラグインをPrisma Access 4.0にアップグレードし、変更をコミットしてプッシュします。 5. プラグインをPrisma Access 4.1にアップグレードし、変更をコミットしてプッシュします。 6. プラグインをPrisma Access 5.0にアップグレードし、変更をコミットしてプッシュします。 7. プラグインをPrisma Access 5.0からPrisma Access 5.1にアップグレードし、変更をコミットしてプッシュします。

インストールされているクラウド サービス プラグインのバージョン	対象バージョン	プラグインのアップグレード パス
		8. プラグインをPrisma Access 5.1からPrisma Access 5.2にアップグレードし、変更をコミットしてプッシュします。
2.2 Preferred	5.2または5.2.1	1. プラグインをPrisma Access 3.0にアップグレードし、変更をコミットしてプッシュします。 2. プラグインをPrisma Access 3.1にアップグレードし、変更をコミットしてプッシュします。 3. プラグインをPrisma Access 3.2または3.2.1にアップグレードし、変更をコミットしてプッシュします。 4. プラグインをPrisma Access 4.0にアップグレードし、変更をコミットしてプッシュします。 5. プラグインをPrisma Access 4.1にアップグレードし、変更をコミットしてプッシュします。 6. プラグインをPrisma Access 5.0にアップグレードし、変更をコミットしてプッシュします。 7. プラグインをPrisma Access 5.0からPrisma Access 5.1にアップグレードし、変更をコミットしてプッシュします。 8. プラグインをPrisma Access 5.1からPrisma Access 5.2にアップグレードし、変更をコミットしてプッシュします。
2.2 Preferredより前のリリースを優先	5.2または5.2.1	1. プラグインをPrisma Access 2.2にアップグレードし、変更をコミットしてプッシュします。 2.2 Preferredよりも前のバージョンのPrisma Accessにデプロイされている場合、3.2にアップグレードする前にまず2.2にアップグレードする必要があります。Prisma Accessの2.0または2.1バージョンからのアップグレードはサポートされていません。 2. プラグインをPrisma Access 3.0にアップグレードし、変更をコミットしてプッシュします。 3. プラグインをPrisma Access 3.1にアップグレードし、変更をコミットしてプッシュします。

インストールされているクラウド サービス プラグインのバージョン	対象バージョン	プラグインのアップグレード パス
		4. プラグインをPrisma Access 3.2または3.2.1にアップグレードし、変更をコミットしてプッシュします。 5. プラグインをPrisma Access 4.0にアップグレードし、変更をコミットしてプッシュします。 6. プラグインをPrisma Access 4.1にアップグレードし、変更をコミットしてプッシュします。 7. プラグインをPrisma Access 5.0にアップグレードし、変更をコミットしてプッシュします。 8. プラグインをPrisma Access 5.0からPrisma Access 5.1にアップグレードし、変更をコミットしてプッシュします。 9. プラグインをPrisma Access 5.1からPrisma Access 5.2にアップグレードし、変更をコミットしてプッシュします。

クラウド サービス プラグインのアップグレード

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Accessライセンス ❑ Minimum Required Prisma Access Version 5.2または5.2.1のPreferred (推奨)またはInnovation (革新)

クラウド サービス プラグインをアップグレードするには、以下の手順に従います。

Prisma AccessはPanoramaのクラウド サービス プラグインを使用して機能をアクティベートします。

Prisma Accessでサポートされ るPanoramaソフトウェアのバージョンの一覧は、『Palo Alto Networks Compatibility Matrix (Palo Alto Networks互換性マトリックス)』の「Minimum Required Panorama Software Versions (最低限必要なPanoramaソフトウェア バージョン)」を参照してください。

プラグインをアップグレードする前に、Prisma Accessテンプレート スタックからPrisma Access以外のテンプレートを削除して、アップグレード後のコミット検証エラーを回避し、Prisma Accessを管理するPanoramaがサポートされているPAN-OSバージョンを実行していることを確認してください。

以下のいずれかのタスクを使用して、クラウド サービス プラグインをダウンロードしてインストールします。

HAデプロイメントのみ—高可用性（HA）モードで*Panorama*アプライアンスを*2*つ設定している場合は、まずプライマリ*HA*ペアにプラグインをインストールし、次にセカンダリ*HA*ペアにプラグインをインストールします。

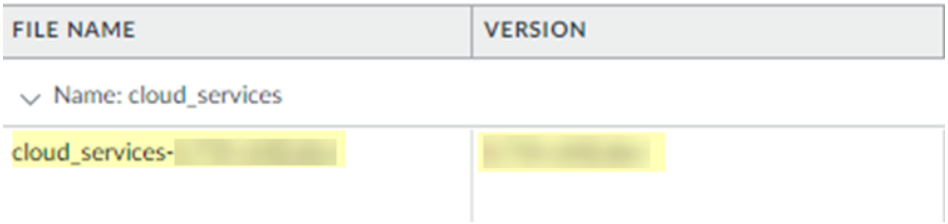
STEP 1 | アップグレードするプラグインのアップグレード パスを決定します。

アップグレード パスによっては、プラグインを順次アップグレードする必要があります。たとえば、3.0 Preferredプラグインから5.2プラグインにアップグレードするには、まず3.1、4.0、4.1、5.0、5.1への暫定アップグレードを実行してから5.2にアップグレードする必要があります。

STEP 2 | 必要なクラウド サービス プラグインのバージョンをダウンロードしてインストールします。

- カスタマーサポートポータルからCloud Servicesプラグインをダウンロードしてインストールするには、以下の手順に従ってください。
  1. カスタマーサポートポータルにログインして、**Software Updates**（ソフトウェアのアップデート）を選択します。
  2. Panorama Integration Plug Inセクションで Cloud Servicesプラグインを探して、それをダウンロードします。

     プラグインのファイル名を変更しないでください。変更すると、*Panorama*にインストールできなくなります。
  3. Prisma Accessとともに使用するライセンスを設定したPanoramaの、Panorama Webインターフェースにログインして、**[Panorama]** > **[Plugins**（プラグイン）**]** > **[Upload**（アップロード）**]**の順に選択し、カスタマーサポートポータルからダウンロードしたプラグイン**[File**（ファイル）**]**を**[Browse**（参照）**]**します。
  4. プラグインを**Install**（インストール）します。
- Panoramaから新しいバージョンのCloud Servicesプラグインを直接ダウンロード、インストールするには、以下の手順に従ってください。
  1. **Panorama** > **Plugins**（プラグイン）の順に選択し、**Check Now**（今すぐ確認）をクリックして最新のCloud Servicesプラグインアップデートを表示します。

  2. **Download**（ダウンロード）を選択して、目的のバージョンのプラグインをダウンロードします。
  3. プラグインをダウンロードしたら、それを**Install**（インストール）します。

STEP 3 | (3.2より前のバージョンから3.2以降のバージョンへのアップグレード）**[Commit (**コミット**)]** > **[Commit to Panorama (Panorama**にコミット**)]**]を選択すると、Prisma Accessを管理するPanorama上で変更がローカルに保存されます。

Panoramaへのローカル コミットは、3.2より前のクラウド サービス プラグインから3.2以降のプラグインにアップグレードする場合にのみ行う必要があります。3.2以降のバージョンからのアップグレードでは、ローカル コミットは必要ありません。

ヘルプの利用

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessライセンス ❑ Minimum Required Prisma Access Version5.2 Preferred (優先)とInnovation (革新)

以下のトピックでは、このリリースに関する詳細情報の入手先とサポート要請方法について説明します。

- 関連ドキュメント
- サポートの依頼

関連ドキュメント

Prisma Accessのデプロイメントをセットアップおよび実装するには、以下のドキュメントを参照してください。

- Prisma Access管理者ガイドを使用して、ネットワークのセキュリティ保護のためのPrisma Accessの計画、インストール、セットアップ、構成を行います。
- Prisma Access統合ガイドのベンダー固有のタスクを使用して、Prisma Accessを使用してモバイル ユーザー認証を構成し、パブリック クラウドとサードパーティのSD-WAN導入デプロイメントのセキュリティを確保します。
- Strata Logging Serviceスタート ガイドを使用して、Strata Logging Service（旧称：Cortex Data Lake）をデプロイし、オンプレミスのファイアウォールからCortex Data Lakeへのログの転送を開始する方法について説明します。

製品の詳細については、https://docs.paloaltonetworks.comをご覧ください。

サポートの依頼

サポートへの連絡、サポート プログラムに関する情報、アカウントまたはデバイスの管理、サポート ケースのオープンについては、https://support.paloaltonetworks.comを参照してください。

ドキュメントに関するフィードバックは、documentation@paloaltonetworks.comまでお送りください。

お問い合わせ先

本社：

Palo Alto Networks

3000 タネリーウェイ

サンタクララ, CA 95054

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

Palo Alto Networks, Inc.

www.paloaltonetworks.com