



TECHDOCS

Prisma Access Release Notes

6.0.0-h40 and 6.0.1

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

Palo Alto Networks, Inc.

www.paloaltonetworks.com

© 2025-2025 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.



Last Revised

November 13, 2025

Table of Contents

Prisma Access Release Information.....	5
New Features in Prisma Access 6.0 and 6.0.1.....	7
Recommended Software Versions for Prisma Access 6.0.1 Preferred and Innovation.....	7
Recommended Software Versions for Prisma Access 6.0 Preferred and Innovation.....	8
Infrastructure, Plugin, and Dataplane Dependencies for Prisma Access 6.0.1 Preferred and Innovation Features.....	9
Infrastructure, Plugin, and Dataplane Dependencies for Prisma Access 6.0 Preferred and Innovation Features.....	10
Prisma Access 6.0.1 Features.....	11
Prisma Access 6.0 Features.....	12
Changes to Default Behavior for Prisma Access 6.0 and 6.0.1.....	18
Prisma Access Known Issues.....	20
Known Issues for Dynamic Privilege Access.....	38
Prisma Access Addressed Issues.....	43
Prisma Access 6.0.1 Addressed Issues.....	43
Prisma Access 6.0.0-h40 Addressed Issues.....	43
Prisma Access 6.0.0-h25 Addressed Issues.....	44
Prisma Access 6.0.0-h22 Addressed Issues.....	45
Prisma Access 6.0.0-h11 Addressed Issues.....	46
Prisma Access 6.0.0-h9 Addressed Issues.....	46
Prisma Access 6.0.0-h3 Addressed Issues.....	47
Prisma Access 6.0.0 Addressed Issues.....	47
Panorama Support for Prisma Access 6.0.....	51
Required and Recommended Software Versions for Panorama Managed Prisma Access 6.0 and 6.0.1.....	52
Recommended Software Versions for Prisma Access 6.0.1 Preferred and Innovation.....	52
Recommended Software Versions for Prisma Access 6.0 Preferred and Innovation.....	53
Upgrade Considerations for Prisma Access 6.0.....	54
Upgrade the Cloud Services Plugin.....	57
Getting Help.....	61
Related Documentation.....	62
Requesting Support.....	63

Prisma Access Release Information

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> Prisma Access (Managed by Strata Cloud Manager) Prisma Access (Managed by Panorama) 	<ul style="list-style-type: none">  Prisma Access license  Minimum Required Prisma Access Version 6.0 Preferred or Innovation

About Prisma Access Release Updates

Prisma Access releases and updates allow you to stay up-to-date and secure your users. Some of the updates are managed by Palo Alto Networks, such as Prisma Access infrastructure updates and you will receive advance notification so you can plan around them. Some updates are your responsibility and you must schedule the specified version of the content update and software update. If you're using Panorama to manage Prisma Access (instead of Prisma Access Cloud Management), you decide when to upgrade to the latest plugin version, in order to leverage newly-available features that the plugin enables for Panorama.

If you use Panorama Managed Prisma Access, [View Panorama and plugin requirements for this Panorama Managed release](#).

Supported GlobalProtect Versions to Use with Prisma Access

Any GlobalProtect version that is not [End-of-Life \(EoL\)](#) is supported for use with Prisma Access; however, note that Prisma Access 6.0 also has [recommended software versions](#) for GlobalProtect as well as required versions.

Here's where you can learn more about the latest updates for the products and services that are included or integrate with Prisma Access:

Latest Prisma Access Release Updates	Earlier Prisma Access Release Versions	Updates for Services and Add-Ons Supported with Prisma Access
<ul style="list-style-type: none"> New Features in Prisma Access 6.0 and 6.0.1 What's New for Prisma Access Cloud Management 	<ul style="list-style-type: none"> Prisma Access Version 5.2 Prisma Access Version 5.1 Prisma Access Version 5.0 Prisma Access Version 4.2 Prisma Access Version 4.1 Prisma Access Version 4.0 Prisma Access Version 3.2 Preferred and Innovation Prisma Access Version 3.1 Preferred and Innovation 	<ul style="list-style-type: none"> Prisma Access Insights Autonomous DEM SaaS Security Enterprise DLP GlobalProtect Prisma SASE Multitenant Cloud Management Platform Prisma SD-WAN

Latest Prisma Access Release Updates	Earlier Prisma Access Release Versions	Updates for Services and Add-Ons Supported with Prisma Access
	<ul style="list-style-type: none">• Prisma Access Version 3.0 Preferred and Innovation• Prisma Access Version 2.2 Preferred• Prisma Access Releases Earlier than 2.2 Preferred	

New Features in Prisma Access 6.0 and 6.0.1

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> Prisma Access (Managed by Strata Cloud Manager) Prisma Access (Managed by Panorama) 	<ul style="list-style-type: none"> Prisma Access license Minimum Prisma Access 6.0 version required

This section provides you with a list of new features in Prisma Access 6.0 and 6.0.1 Preferred and Innovation, along with the recommended and required software versions you need to use.

- [Recommended Software Versions for Prisma Access 6.0.1 Preferred and Innovation](#)
- [Infrastructure, Plugin, and Dataplane Dependencies for Prisma Access 6.0 Preferred and Innovation Features](#)
- [Prisma Access 6.0.1 Features](#)
- [Prisma Access 6.0 Features](#)

Recommended Software Versions for Prisma Access 6.0.1 Preferred and Innovation

Prisma Access 6.0.1 Preferred and Innovation run a PAN-OS 11.2.6 dataplane.

Prisma Access (Managed by Panorama) release 6.0.1 requires a minimum Cloud Services plugin version of 6.0.0-h9.

For Prisma Access 6.0.1 features, Palo Alto Networks **recommends that you upgrade your Prisma Access to the following versions** before installing the plugin.

Prisma Access Version	Cloud Services Plugin Version	Required Dataplane Version for 6.0.1	Recommended GlobalProtect Version	Recommended Panorama Version
6.0.1	Minimum version of 6.0.0-h9	6.0.1 Preferred and Innovation: PAN-OS 11.2.6	6.0.1.7+ 6.1.3+ 6.2.1+ Minimum required versions for IPv6 Support for Public Apps for IP Optimization: <ul style="list-style-type: none"> 6.2.6 client version for Windows and macOS 	10.2.10+ 11.0.1+ 11.1.0 11.2.6 12.1.2 Before you upgrade your Panorama to 12.1.2, upgrade your Cloud Services plugin to

Prisma Access Version	Cloud Services Plugin Version	Required Dataplane Version for 6.0.1	Recommended GlobalProtect Version	Recommended Panorama Version
			<ul style="list-style-type: none"> 6.2.7 for Linux 6.1.7 for Android and IOS 	6.0.0-h22; then, upgrade your Panorama. Be sure to follow the upgrade path when upgrading your plugin.

Recommended Software Versions for Prisma Access 6.0 Preferred and Innovation

Prisma Access 6.0 Preferred and Innovation run on a PAN-OS 11.2.6 dataplane.

For Prisma Access 6.0 features, Palo Alto Networks **recommends that you upgrade your Prisma Access to the following versions** before installing the plugin.

Prisma Access Version	Cloud Services Plugin Version	Required Dataplane Version for 6.0	Recommended GlobalProtect Version	Recommended Panorama Version
6.0	6.0	PAN-OS 11.2.6 for 6.0 Preferred and Innovation	6.0.7+ 6.1.3+ 6.2.1+ Minimum required versions for IPv6 Support for Public Apps for IP Optimization: <ul style="list-style-type: none"> 6.2.6 client version for Windows and macOS 6.2.7 for Linux 6.1.7 for Android and IOS 	10.2.10+ 11.0.1+ 11.1.0 11.2.6 12.1.2 Before you upgrade your Panorama to 12.1.2, upgrade your Cloud Services plugin to 6.0.0-h22; then, upgrade your Panorama. Be sure to follow the upgrade path when upgrading your plugin.

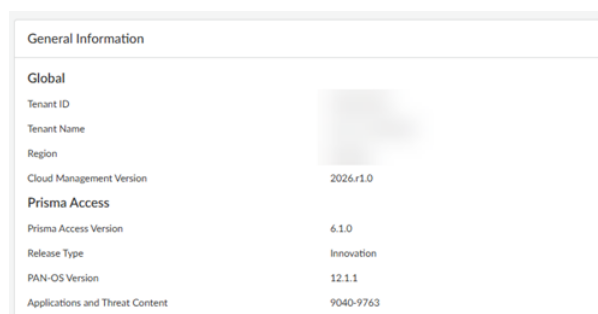
Infrastructure, Plugin, and Dataplane Dependencies for Prisma Access 6.0.1 Preferred and Innovation Features

Prisma Access 6.0.1 features require one or more of the following components to function:

- **Infrastructure Upgrade**—The infrastructure includes the underlying service backend, orchestration, and monitoring infrastructure. Prisma Access upgrades the infrastructure before the general availability (GA) date of a Prisma Access release.

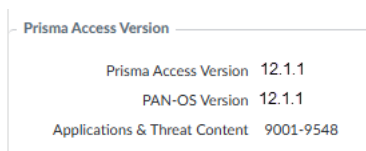
Features that require only an infrastructure upgrade to be unlocked take effect for all Prisma Access deployments, regardless of version, at the time of the infrastructure upgrade.

- **Plugin Upgrade (Prisma Access Panorama Managed Deployments Only)**—Prisma Access (Managed by Panorama) release 6.0.1 requires a minimum Cloud Services plugin version of 6.0.0-h9.
- **Dataplane Upgrade**—The dataplane enables traffic inspection and security policy enforcement on your network and user traffic.
 - For Prisma Access (Managed by Strata Cloud Manager), view your Prisma Access version and release type by going to **Manage > Configuration > NGFW and Prisma Access > Overview > Prisma Access Version.**



General Information	
Global	
Tenant ID	
Tenant Name	
Region	
Cloud Management Version	2026.r1.0
Prisma Access	
Prisma Access Version	6.1.0
Release Type	Innovation
PAN-OS Version	12.1.1
Applications and Threat Content	9040-9763

- For Prisma Access (Managed by Panorama) deployments, view your dataplane version by going to **Panorama > Cloud Services > Configuration > Service Setup** and viewing the **Prisma Access Version**.



Prisma Access Version	
Prisma Access Version	12.1.1
PAN-OS Version	12.1.1
Applications & Threat Content	9001-9548

These features are activated with the **infrastructure upgrade** only for Prisma Access 6.0.1:

- Mexico Central Compute Region Support

These features require an **infrastructure and plugin upgrade** but don't require a dataplane upgrade; however, a minimum dataplane version of 10.2.10 is required for these features:

- None

These features require an **infrastructure, plugin, and dataplane** upgrade to PAN-OS 11.2.6, making them Prisma Access 6.0.1 Innovation features:

- None

Infrastructure, Plugin, and Dataplane Dependencies for Prisma Access 6.0 Preferred and Innovation Features

Prisma Access 6.0 features require one or more of the following components to function:

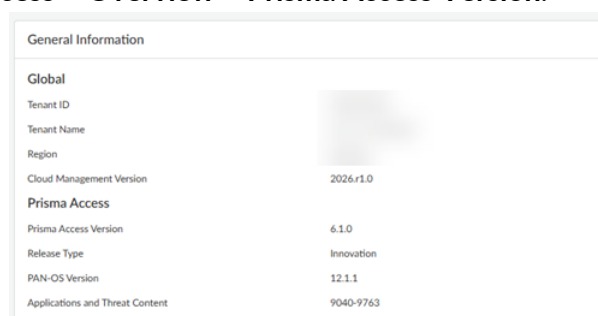
- **Infrastructure Upgrade**—The infrastructure includes the underlying service backend, orchestration, and monitoring infrastructure. Prisma Access upgrades the infrastructure before the general availability (GA) date of a Prisma Access release.

Features that require only an infrastructure upgrade to be unlocked take effect for all Prisma Access deployments, regardless of version, at the time of the infrastructure upgrade.

- **Plugin Upgrade (Prisma Access Panorama Managed Deployments Only)**—Installing the plugin activates the features that are available with that release. You download and install the plugin on the Panorama that manages Prisma Access.

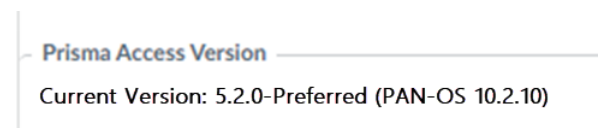
Prisma Access (Managed by Panorama) release 6.0 uses the **Cloud Services Plugin 6.0**.

- **Dataplane Upgrade**—The dataplane enables traffic inspection and security policy enforcement on your network and user traffic.
 - For Prisma Access (Managed by Strata Cloud Manager), go to **Manage > Configuration > NGFW and Prisma Access > Overview > Prisma Access Version.**



General Information	
Global	
Tenant ID	
Tenant Name	
Region	
Cloud Management Version	2026.r1.0
Prisma Access	
Prisma Access Version	6.1.0
Release Type	Innovation
PAN-OS Version	12.1.1
Applications and Threat Content	9040-9763

- For Prisma Access (Managed by Panorama) deployments, you can view your dataplane version by going to **Panorama > Cloud Services > Configuration > Service Setup** and viewing the **Prisma Access Version**. Prisma Access Preferred and Innovation run PAN-OS 11.2.6.



Prisma Access Version
Current Version: 5.2.0-Preferred (PAN-OS 10.2.10)



A dataplane upgrade to 6.0 Innovation is optional, and is only required if you want to take advantage of the features that require a dataplane upgrade.

These features are activated with the **infrastructure upgrade** only for Prisma Access 6.0:

- Advanced ZTNA Connector
- Extend Prisma Access User Group Policy Support with Short Form Format
- Mexico Central Compute Region Support
- Remote Network Site-Based Licensing and Simplified Onboarding
- Simplified Onboarding Workflow

These features require an **infrastructure and plugin upgrade** but don't require a dataplane upgrade; however, a minimum dataplane version of 10.2.4 is required for these features:

- BGP Filtering and Route Metric Support for Prisma Access

These features require an **infrastructure, plugin, and dataplane** upgrade to PAN-OS 11.2.6, making them Prisma Access 6.0 Preferred and Innovation features:

- Colo-Connect Inter-Region
- RFC6598, iOS, and Android Support for Static IP Address Allocation
- WildFire Hold Mode Support (11.2.4 or later dataplane required)

Prisma Access 6.0.1 Features

Here are the features in Prisma Access 6.0.1.

ZTNA Connector: Scalability Improvements

With your license or Private App add-on license, ZTNA Connector offers an enhancement that improves scalability, allowing users to onboard **20,000 applications per tenant** across all Connector Groups.

New Region Support for ZTNA Connector

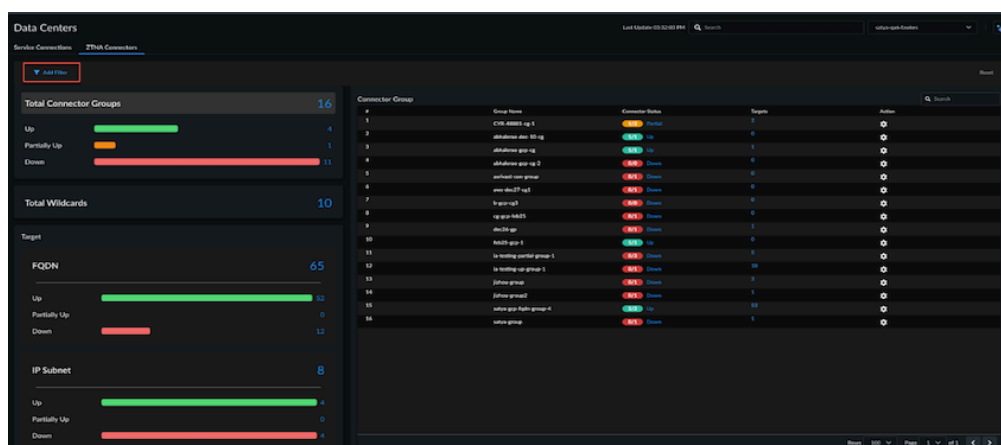
ZTNA Connector now provides secure and compliant multi-national enterprise level communication within and across **mainland China**. You will need a China L2 add-on license to enable the required functionalities. With China L2 add-on license, you get 10 Connectors, 20,000 FQDNs, and 1024 IP Subnets. If you need more than 10 Connectors, you need to get in addition a Private App add-on license.

South Africa is also added as a supported location for **ZTNA Connector**.

Visibility for ZTNA Connector

Depending on your license for ZTNA Connector, you can see the following updates in Strata Cloud Manager for visibility:

Select the number next to **Total Connector Groups**, **Total Wildcards**, **FQDN**, or **IP Subnet** to get the details for each ZTNA object. You can see the status related to each ZTNA object (UP, Partially Up, Down). Additionally, you can now monitor a **Wildcard's bandwidth** by selecting **Action**.



Traffic Replication for Explicit Proxy: Enhanced Visibility for SASE

Traffic Replication for explicit proxy addresses the challenge enterprises face when transitioning from on-premises network security infrastructure to SASE by preserving access to your packet captures (PCAPs) for threat investigation, forensic analysis, and compliance requirements. Traffic replication provides a complete copy of traffic traversing explicit proxy available for analysis.

When you enable Traffic replication for explicit proxy, captures and replicates all traffic, including SSL-decrypted content when configured with the appropriate decryption rules. This capability enables you to meet regulatory requirements. The replicated traffic is secured while in motion and at rest, with no alterations to the original packet form, ensuring both directions of communication are preserved without packet loss.

Traffic replication for explicit proxy extends the existing capabilities already available for mobile users and remote networks, providing consistent traffic visibility across all connection methods. You can use this feature with various third-party network detection and response (NDR) tools for enhanced security analytics. The replicated traffic is stored as PCAP files in Cloud Object Storage, where they remain available for 72 hours, enabling your security teams adequate time to download and analyze the data with your preferred forensic tools.

You can enable Traffic replication selectively for specific explicit proxy locations to control data volume, and the system automatically accommodates auto scaling events and infrastructure changes to ensure continuous replication. The functionality operates without affecting existing performance or capabilities, providing you with valuable security insights without compromising the user experience.

Prisma Access 6.0 Features

Here are the features in Prisma Access 6.0.0.

Advanced ZTNA Connector

Supported in: Prisma Access 6.0

Complex deployments, rigid licensing structures, and limited regional logging capabilities previously increased the administrative friction of adopting ZTNA Connector. These significant

updates to the ZTNA Connector address these challenges by improving operational efficiency, expanding global visibility, and simplifying configuration.

Regional Support for Strata Logging Service

ZTNA Connector now supports sending logs to [Strata Logging Service](#) instances in new regions, addressing global data residency needs. The supported regions are:

- Indonesia
- Qatar
- Saudi Arabia
- Taiwan

Simplified Onboarding Workflow

Prisma[®] Access now offers a simplified Day 0 [onboarding workflow](#) to set up ZTNA Connector. This guided, step-by-step process helps you:

- Configure to secure private apps
- Apply best-practice defaults
- Automate backend tasks
- Integrate Cloud Identity Engine (CIE), Strata Cloud Manager, and

This intuitive, action-oriented setup significantly reduces complexities during onboarding.

Streamlined Licensing

6.0 introduces a streamlined [licensing model](#) for ZTNA Connector:

- You can now enable ZTNA Connector without a ZTNA Connector add-on license.
- Based on your existing licenses, you receive 10 ZTNA Connector licenses with the base license.
- If you purchase the Private Apps add-on, you unlock a number of Service Connections and ZTNA Connectors up to the limit supported by the product in each tenant.

6.0 introduces new licensing for ZTNA Connector which streamlines the licensing structure, simplifying the process, and offers a more efficient approach.

This licensing model provides an option to **Enable ZTNA Connector** without a ZTNA add-on license. Based on your licenses, you receive free but limited licenses. If you purchase an unlimited private apps add-on license, you will get an unlimited Service Connections and ZTNA Connectors.

Support for DNS SRV records and SCCM

ZTNA Connector now supports:

- [DNS SRV](#) queries, allowing clients to intelligently locate AD domain controllers using structured, priority-based FQDNs.
- SCCM integration, enabling the ZTNA Connector to direct software updates through the correct AD site's distribution point.

This enhancement improves resource access, strengthens endpoint management, and maintains ZTNA-level security.

BGP Filtering and Route Metric Support for Prisma Access

Supported in: Prisma Access 6.0 (minimum 10.2.4 dataplane required)

For customers who need precise control over routing, [Prisma Access offers new BGP capabilities](#) to enhance network traffic and improve efficiency. The platform provides a UI-based configuration option on Panorama® and Cloud Management, enabling you to filter BGP prefixes advertised to remote networks (RNs) and service connections (SCs). This includes individual filtering options for all outbound mobile user, RN, and SC prefixes, as well as the ability to filter specific prefixes per RN and SC onboarding. BGP filtering can be configured per RN and SC BGP peer and also supports a global tenant-level configuration. Filtering options include both prefix and BGP community-based criteria.

This update allows you to create and apply custom routing policies to your service connections, including both regular and Colo-Connect connections. This functionality enables you to optimize traffic flow, improve network efficiency, and strengthen your security posture.

The BGP filtering and route metric support is integrated with the existing Prisma Access security platform. This means you can now leverage advanced routing capabilities alongside Palo Alto Networks' comprehensive suite of threat prevention features.

Colo-Connect Inter-Region

Supported in: Prisma Access 6.0

Today, large enterprises are building Colo-based performance hubs to reach private applications in hybrid, multicloud architectures because of the high-bandwidth and low-latency requirements. Typically, these hubs include interconnects to one or more cloud providers and connections to the on-premises data centers over a private or leased WAN. Performance hubs can route traffic between the public cloud and on-premises infrastructure at high speed, and are resilient because of the underlying interconnect infrastructure.

Prisma® Access [Colo-Connect](#) builds on the Colo-based performance hub concept, offering high-bandwidth private connections along with seamless Layer 2/3 connectivity to Prisma Access from existing performance hubs.

[Colo-Connect](#) handles inter-region traffic with a focus on high performance and scalable network solutions, ensuring seamless operation even if a compute location becomes unavailable. To address this need, Prisma Access has implemented an inter-region connectivity feature. This feature enables Colo-Connect instances across different regions to be interconnected and provides robust disaster recovery capabilities between regions.

This inter-region support provides higher bandwidth, enables seamless scalability across regions, and strengthens multicloud support.

DNS Resolution for Mobile Users—Explicit Proxy Deployments

Supported in: Prisma Access 6.0

Organizations using Explicit Proxy often face challenges integrating their cloud security with specialized internal network infrastructure, particularly regarding custom Domain Name Service (DNS) resolution. This limitation can interrupt seamless access to both public internet applications and critical internal private resources. Explicit Proxy now expands its capabilities to include comprehensive [DNS Proxy customization](#), solving this hybrid networking challenge. This feature allows you to seamlessly integrate regional DNS, custom third-party resolvers, or existing on-premises DNS infrastructure. By supporting FQDN-based resolution, the solution guarantees that all applications—whether public or privately hosted—are resolved correctly and securely. This optimization is supported on Panorama Managed Prisma[®] Access, delivering a more robust and flexible security posture for hybrid environments and optimizing the user experience.

Extend Prisma Access User Group Policy Support with Short Form Format

Supported in: Prisma Access 6.0

We introduced the ability to [extend Prisma Access user group policy](#) with the short form format. Migrating security policies from NGFW to Prisma Access requires policy elements standardization. Prisma Access only supports long-form DN entries for group-based policies, while the NGFW allows using other formats such as SAML account name/Common Name and email address. This feature enables customers to define the group format choice for security policy creation, allowing standardized policy creation across Prisma Access and NGFW.

Mexico Central Compute Region Support

Supported in: Prisma Access 6.0

Prisma Access supports the [Mexico Central compute region](#).

Region Support for Explicit Proxy

Supported in: Prisma Access 6.0

Explicit proxy extends its support to the following [regions](#):

- Bahrain
- Canada West
- France North
- Ireland
- Sweden
- South Africa West
- United Arab Emirates

Remote Network Site-Based Licensing and Simplified Onboarding

Supported in: Prisma Access 6.0 (*New Prisma Access Deployments Only*)

Managing remote network capacity using aggregate bandwidth licensing is complex, often requiring difficult resource estimation and manual redundancy configuration across compute regions. Prisma® Access 6.0 introduces [site-based licensing](#) for Remote Networks, enhancing flexibility and simplifying deployment for branch sites. This licensing model allows you to allocate your sites with predefined bandwidth capacities, ranging from 25 Mbps to 2.5 Gbps. By moving away from aggregate bandwidth-based licensing, you can more easily estimate and allocate resources for your remote sites.

With site-based licensing, you no longer need to pre-allocate bandwidth to specific Prisma Access compute regions or configure redundancy manually. This approach reduces complexity in network planning and provides a more straightforward way to manage and scale your branch sites.

Using this model, you can focus on the number and types of sites needed rather than estimating total bandwidth consumption across your network.

Site-based licensing in Prisma Access aligns better with your organizational structure and growth plans, providing a more intuitive and scalable approach to securing and connecting your branch sites. This licensing model aims to enhance your experience in deploying and managing Prisma Access, offering greater control and efficiency in resource allocation across your distributed network infrastructure.

Additionally, a simplified [onboarding workflow](#) for Prisma Access further reduces complexity by accelerating remote network setup.

RFC6598, iOS, and Android Support for Static IP Address Allocation

Supported in: Prisma Access 6.0

Some legacy networks use IP address-based authorization to restrict users' access to internal or external resources. A Prisma® Access Mobile Users—GlobalProtect® deployment assigns users an IP address from the mobile users IP address pool you assign during onboarding, and this user-to-IP address mapping can change in subsequent logins. To retain user-to-IP address mapping, Prisma Access lets you [assign static IP addresses](#) to users. With this feature, Prisma® Access allows you to allocate IP addresses to users based on the User or User-group, along with Theatre and Location groups.

Prisma Access adds the following enhanced functionality for static IP address allocation: support for iOS and Android mobile devices and support for RFC6598 addresses.

Simplified Onboarding Workflow

Supported in: Prisma Access 6.0

Organizations often face complex, manual setup processes when deploying SASE solutions, leading to delayed security protection. The Prisma® Access onboarding workflow addresses this challenge by providing a simplified initial setup process for new deployments. This guided workflow rapidly deploys and configures the necessary components for securing mobile users (via [GlobalProtect®](#) and [Explicit Proxy](#)) and for securing private applications (via [Service Connection](#)). By incorporating best-practice defaults, automating backend tasks, and seamlessly integrating the [Cloud Identity Engine](#) and [Strata Cloud Manager](#) with Prisma Access, this intuitive, action-oriented approach accelerates time-to-value and significantly reduces onboarding complexity.

WildFire Hold Mode Support

Supported in: Prisma Access 6.0

Preventing known malware from transferring while real-time signature lookups are underway often introduces a window of risk. If you have an active WildFire® or Advanced WildFire license, Prisma® Access now supports WildFire Hold Mode to immediately address this risk. Hold Mode enables you to configure Prisma® Access to [hold the transfer of a sample file](#) while the real-time signature cloud performs a signature lookup. When the lookup completes, Prisma Access releases the file to the requesting client (or blocks it, based on your organization's security policy for specific WildFire verdicts, preventing the initial transfer of known malware. You can configure Hold Mode on a per antivirus profile basis and apply a global setting for the signature lookup timeout and the associated action.

Changes to Default Behavior for Prisma Access 6.0 and 6.0.1

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> Prisma Access (Managed by Strata Cloud Manager) Prisma Access (Managed by Panorama) 	<ul style="list-style-type: none"> Prisma Access license Minimum Prisma Access 6.0 version required.

The following table details the changes in default behavior for Prisma Access version 6.0.1.

Component	Change
Remapped Mexico West Location	<p>To better optimize the performance of Prisma Access, the The Mexico West location is remapped to the Mexico West compute location.</p> <p>New deployments have the new remapping applied automatically. If you have an existing Prisma Access deployment that uses one of these locations and you want to take advantage of the remapped compute location, follow the procedure to add a new compute location to a deployed Prisma Access location.</p>

The following table details the changes in default behavior for Prisma Access version 6.0.

Component	Change
Remapped Mexico Central Location	<p>To better optimize the performance of Prisma Access, the Mexico Central location is remapped to the Mexico City, Mexico compute location.</p> <p>New deployments have the new remapping applied automatically. If you have an existing Prisma Access deployment that uses one of these locations and you want to take advantage of the remapped compute location, follow the procedure to add a new compute location to a deployed Prisma Access location.</p> <p>Please note these restrictions for the Mexico Central location and site-based remote networks:</p> <ul style="list-style-type: none"> X-Large sites are not supported. The maximum bandwidth per service IP will be limited to 2 Gbps instead of 3 Gbps, regardless of whether the selected license type is 2.5 Gbps or if the total of selected licenses falls between 2 Gbps and 3 Gbps. Colo-Connect is not supported.

Component	Change
IP Optimization Migrations Do not Support Automatic Restoration of VPN Connection Timeout Values Longer than 30 Minutes	<p>If you have an existing deployment and upgrade to IP Optimization, and if you have configured an Automatic Restoration of VPN Connection Timeout value in the GlobalProtect portal for greater than 30 minutes, a commit validation is seen after the upgrade to Prisma Access 6.0.</p> <p>To work around this issue, revert your commit, change the Automatic Restoration of VPN Connection Timeout to a value lower than 30 minutes, and redo the Commit and Push operation.</p>

Prisma Access Known Issues

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> Prisma Access (Managed by Panorama) 	<ul style="list-style-type: none"> Prisma Access license Minimum Required Prisma Access Version 6.0 Preferred or Innovation

Prisma Access has the following known issues.

Issue ID	Description
AIOPS-11286	When you have Colo-Connect enabled, cross-connects and connections-related information may not be up to date on subtenants in a multitenant environment.
CYR-59509	<p>After upgrading the Cloud Services plugin from 5.1 to 5.2 or later, the previously-configured Roles were not applied to the configuration, even though the configuration appears in the Panorama UI. This condition causes the administrator to not be able to view the Cloud Services tab in Panorama.</p> <p>Workaround: Go to Panorama > Admin Roles > <role-profile>, Disable and Enable the Plugins choice in the Plugins tab, and Push your changes to Panorama.</p>
CYR-59494	<p>The list of Remote Networks on the Remote Networks status page always displays a count of 0 items.</p> <p>Workaround: Ignore the total number of items that display. The Remote Network details display correctly on the Status page, only the number of items is incorrect.</p>
CYR-56688	If you delete Internal Host Detection in the Default agent settings (Network > GlobalProtect > Portals > <portal-config> > Agent > DEFAULT > Internal), the Internal Host Detection settings are not removed from the configuration in the Cloud Services plugin (Panorama > Cloud Services > Configuration > Mobile Users—GlobalProtect > Onboarding > > General > Internal Host Detection), causing the Internal Host Detection settings to reappear in the Default agent settings.

Issue ID	Description
	Workaround: Either remove the Internal host detection from the Cloud Services plugin configuration, or rename the Default agent settings.
CYR-55477	If you have a site-based license for remote networks, the Status page in Panorama (Panorama > Cloud Services > Status) incorrectly shows the allocated and available Remote Network bandwidth as 0.
CYR-54556	When using explicit proxy nodes, you must configure at least one domain under Workflows > Prisma Access Setup > Explicit Proxy > Advanced Security Settings > Authentication settings > Domains Used in Authentication Flow in Strata Cloud Manager. Failing to do so results in a commit failure.
CYR-54543 This issue is now resolved in Prisma Access 6.0.0-h17. See Prisma Access 6.0.0-h22 Addressed Issues .	Panorama Plugin-based GlobalProtect logout fails when there is a special character in username or computer name.
CYR-55402	The Global Portal Config for Internal Host Detection will overwrite the Internal Host Detection in the Portal Agent Config. But, if there are multiple agent configs, it will overwrite the very first config in the list, not DEFAULT. It depends on which config is at the top of the list.
CYR-54002	Geo-location is not functional for IPv6 only deployments. Workaround: Implement a dual stack deployment. IPv6 native deployments determine their location by latency probes, which may result in incorrect portal selection and incorrect language selection.
CYR-53726	For tenants using site-based licensing for branch sites, the site license type may display as Unknown for certain branch sites within SCM > Monitor > Branch Sites .
CYR-54342	In Insights > Data Centers > ZTNA Connectors > FQDNs > Bandwidth , the time stamp for Bandwidth is incorrect.
CYR-52409	When you have an existing deployment and upgrade to IP Optimization, and if you have configured an Automatic Restoration of VPN Connection Timeout

Issue ID	Description
	<p>value in the GlobalProtect portal for greater than 30 minutes, a commit validation is seen after the upgrade to Prisma Access 6.0.</p> <p>Workaround: Revert your commit, change Automatic Restoration of VPN Connection Timeout to a value lower than 30 minutes, and redo the Commit and Push operation.</p>
CYR-52287	<p>Panorama incorrectly allows users to configure QoS profiles with Egress Guaranteed values exceeding Egress Max values. This is an invalid configuration.</p> <p>Workaround: Configure an Egress Guaranteed value that is not greater than the Egress Max value.</p>
CYR-52286	<p>When onboarding a remote network using a site-based license, Panorama incorrectly allows you to create Remote Networks without attaching a QoS Profile. However, when you perform a commit operation, the commit fails with the error Failed to process Remote Network configuration (NETP_ERROR-200, details:). Please try again.</p> <p>Workaround: When configuring a site-based remote network, attach a QoS profile to the remote network.</p>
CYR-52233	<p>When you set up secure inbound access for remote networks, a Bandwidth field displays with fields for site-based licenses, even though your deployment uses aggregate bandwidth.</p> <p>Workaround: Select the bandwidth for the compute location to which the location corresponds.</p>
CYR-51257	<p>Strata Logging Service logs related to ZTNA Connector might not be seen in the Strata Cloud Manager log viewer for FedRAMP deployments.</p>
CYR-51157	<p>Secure Inbound Access is not supported with Remote Networks—High Performance deployments.</p>
CYR-51156	<p>BGP MRAI values are not applied to Remote Networks—High Performance deployments.</p>
CYR-51029	<p>IPv6 information is absent in the Panorama (Panorama > Cloud Services > Status > Monitor page) and Strata</p>

Issue ID	Description
	Cloud Manager pages if the config service is enabled on the tenant.
CYR-50900	<p>If you select a Mobile Users configuration item and you don't have a Mobile Users license, you might receive an error upon commit.</p> <p>Workaround: Do not select a Mobile Users configuration item if you don't have a Mobile Users license.</p>
CYR-50870	<p>When attempting to onboard a large number of ZTNA connector applications (more than 500), the application might not be onboarded and a 502 Server Error: Bad Gateway for url error might be encountered.</p> <p>Workaround: Attempt to re-onboard the application that failed.</p>
CYR-49865	In Mobile Users—GlobalProtect setup with IPv6 enabled, when a GlobalProtect client with only an IPv4 address connects to an IPv6-enabled gateway, edge localization is not working when users try to connect to an edge location. This behavior affects both existing deployments that have IP Optimization enabled and deployments that don't have IP Optimization enabled.
CYR-49816	The username in XAU within the Connect request won't be normalized to reflect the primary attribute in the directory setting. Instead, it will be the base64 encoded username carried in the authentication JWT token within the request.
CYR-49758	If the request includes a valid JWT token, the parsed username in the JWT will be used instead of the special authentication bypass username inserted by explicit proxy.
CYR-49265	When using Traffic replication, statistics do not display for deployments in the France North region. Workaround: To enable traffic replication for the France North region deployment, select the check box "Europe Northwest (Paris)" under the traffic replication tab and not France North.
CYR-48823	Double decryption isn't supported. Therefore, when sending a CONNECT request over an SSL tunnel,

Issue ID	Description
	inserting headers in the underlying actual request isn't supported.
CJR-48331	<p>Mobile Users—GlobalProtect users cannot perform an Auto or Transparent upgrade because a security policy is blocking the upgrade.</p> <p>Workaround: Create a Custom URL category for the URL pan-gp-client.s3.dualstack.us-west-2.amazonaws.com and allow traffic from the URL in the rule. You can also allow only the download for *.pkg and *.msi files for greater granularity in the rule.</p>
CJR-47807	<p>After creating filter rules, if you try to assign them to a filter group without selecting OK on the main BGP Filtering widget, the filter rules will not appear in the dropdown selection.</p> <p>Workaround:</p> <ol style="list-style-type: none"> 1. Create one or more BGP Filters. 2. Click OK on the BGP Filtering widget. 3. Reopen the BGP Filtering widget using the gear icon. <p>Then the BGP Filters display during BGP Filter Group creation.</p>
CJR-47616	<p>Increasing the subnet mask on an existing mobile user IP address pool (for example, if you change 10.6.0.0/18 to 10.6.0.0/17), or changing the region of an existing IP address pool, can cause issues for existing connected users.</p> <p>Workaround: Perform one or more of the following actions:</p> <ul style="list-style-type: none"> • Have the GlobalProtect mobile user refresh their connection. <p>Any changes to the GlobalProtect IP address pool scope (increasing the existing pool or using a completely different pool) would cause issues to the existing connected users, which can only be resolved after a successful GlobalProtect refresh where the app acquires the IP address from the newly allocated pool.</p>

Issue ID	Description
	<ul style="list-style-type: none"> • Add another address block to the mobile users IP address pool instead of changing the subnet in the existing pool. <p>For example, instead of changing a subnet in the pool from /18 to /17, consider adding another /18 address to the existing pool and leave the existing pool intact.</p>
CYR-47139	<p>ZTNA Connectors are disabled in a ZTNA Connector - Explicit Proxy integration if ZTNA Connector application blocks or connector blocks are configured with RFC6598 addresses that conflict with Explicit Proxy addresses.</p> <p>Workaround: If you have integrated ZTNA Connector with Explicit Proxy, do not use the "100.64.0.0/15", "100.72.0.0/15", or "100.88.0.0/15" subnets for:</p> <ul style="list-style-type: none"> • ZTNA Connector Application Blocks • ZTNA Connector Connector Blocks • IP subnets configured in ZTNA Connector that you have associated with applications
CYR-47038	<p>HTTP header insertion on Remote Networks is not supported when using Proxy Mode on Remote Networks and Source IP based visibility and enforcement is enabled.</p> <p>Workaround: Use HTTP header insertion on explicit proxy nodes.</p>
CYR-46759	<p>UDP Settings for DNS Queries are not honored in Explicit Proxy.</p>
CYR-46627	<p>Explicit Proxy is not supported if Accept Default Route over Service Connection is enabled.</p>
CYR-46445	<p>A transient error related to port 6081 that was processed on an NAT device caused the ZTNA Connector to go down.</p> <p>Workaround: When ZTNA Connector traffic is passing through a NAT device, make sure the NAT session is not mapped to port 6081.</p>
CYR-46349	<p>When using Remote Networks with Explicit Proxy with Traffic Steering in China, do not configure traffic steering rules with URL Category.</p>

Issue ID	Description
CYR-46191	<p>If the Explicit Proxy is configured with Private Application Access enabled and ZTNA Connector is added to the configuration, another commit from Panorama or Strata Cloud Manager might be required.</p> <p>Workaround: Make a small modification to the Explicit Proxy configuration on the Panorama or Strata Cloud Manager that manages Prisma Access and Push your changes.</p>
CYR-46145	When the Prisma Access autonomous system number or Prisma Access infra subnet is updated for an existing Prisma Access tenant, where ZTNA Connector and corresponding applications are onboarded, there will be outage for around 5 minutes after the update.
CYR-46093	If your deployment has implemented the functionality to support up to 25,000 remote networks and 50,000 IKE gateways, aggregate bandwidth usage statistics displays No data for the specified time period instead of the usage statistics.
CYR-45855	You cannot change the Infrastructure Subnet or the BGP AS number for Remote Networks—High Performance deployments.
CYR-45415	Administrators with read-only or disabled access to the Cloud Services plugin can modify the configuration outside of the cloud services plugin that affects cloud-services behavior, such as templates, device-groups, removing Cloud Services configuration, uninstalling the cloud-services plugin, and loading configuration files.
CYR-44202	Administrative users with read-only access to the Cloud Services plugin are able to modify the RBI tab.
CYR-43425	You cannot specify Outbound Routes for the Service for service connections if those service connections use RFC 6598 addresses.
CYR-43147	For autoscaled ZTNA connectors, during scale in, existing long lived sessions may be dropped prematurely that are handled by the ZTNA connector that is marked for scale in. There should be no impact for new traffic sessions post scale in.

Issue ID	Description
CYR-43132	During sub-tenant creation on Panorama, you cannot configure units for Remote Networks if the Mobile Users configuration is left blank, and vice versa.
CYR-42312	User-ID Across NAT is not supported with Colo-Connect.
CYR-42259	Explicit Proxy Private App Access does not work when RFC6598 is enabled.
CYR-42244	<p>If you are requesting a Prisma Access gateway name change as part of the Business Continuity for Mergers and Acquisitions feature, the updated FQDN does not display in Strata Cloud Manager or Panorama.</p> <p>Workaround: Reach out to your Palo Alto Networks account team, who will open an SRE case to update the FQDN for the gateway.</p>
CYR-42188	When using Explicit Proxy Private App Access, DNS over TCP does not function; however DNS over UDP functions correctly.
CYR-42130	Colo-Connect routing information does not display in the Serviceability Commands area.
CYR-42018	<p>If you have IP Optimization enabled, TLS 1.3 support for GlobalProtect is not supported.</p> <p>Workaround: Use a maximum TLS version of 1.2.</p>
CYR-41990	IPv6-to-IPv6 or IPv6-to-IPv4 source or destination traffic does not support the URL filtering actions Continue and Override .
CYR-41228	If you have IP Optimization enabled, you cannot use the SP interconnect feature.
CYR-41067	An incorrect Prisma Access version displays in the Prisma Access Version area of the UI. In Strata Cloud Manager, the version displays in Manage > Configuration > NGFW and Prisma Access > Overview > Prisma Access Version ; in Panorama Managed Prisma Access, the version displays in Panorama > Cloud Services > Configuration > Service Setup > Prisma Access Version .
CYR-40404	An FQDN target matching a wildcard might not be discovered for a connector group if the application is

Issue ID	Description
	<p>not accessible from some of the ZTNA connectors in the connector group.</p> <p>All connectors in a given group should be able to use DNS to resolve the application and access the application for the application to be auto-discovered in the group.</p> <p>Workaround: Associate the application object to the required connector group from Strata Cloud Manager.</p>
CYR-39795	<p>After installation of the Cloud Services plugin, an Explicit Proxy Kerberos server profile (default_server_profile) is installed by the __cloud_services user, even though Explicit Proxy is not enabled.</p> <p>Workaround: Ignore the changes.</p>
CYR-39551	<p>If you set up Prisma Access Dynamic DNS with an authentication type of TSIG, you should upload a .key file for the TSIG key file. The key file is considered not valid if it has non-ASCII characters in the content. If you provide a .key file for TSIG authentication with non-ASCII characters and you click OK, an error Please upload a file with the .key extension displays.</p> <p>Workaround: Provide a valid tsig key file.</p>
CYR-39153	<p>When performing an upgrade to a ZTNA Connector Group, there can be failures intermittently during the upgrade operation. For example, the upgrade status displays as partial_success or failed, even though some of the affected connectors are later upgraded successfully.</p> <p>Workaround: Retry the Connector Group upgrade at a later time. ZTNA Connector rechecks and provides you with the appropriate status of the Connector Groups.</p>
CYR-39148 This issue is now resolved in Prisma Access 6.0.0. See Prisma Access 6.0.0 Addressed Issues .	<p>When configuring Colo-Connect, Commit and Push operations to Colo Connect Device Groups may intermittently fail.</p> <p>Workaround: Retry the Commit and Push operation to the Colo-Connect Device Group.</p>
CYR-39028	<p>If you are upgrading your ZTNA Connector from 4.1 to a later Prisma Access version and the ZTNA connector application pools are configured within the RFC6598</p>

Issue ID	Description
	<p>address space (100.64.0.0/16 and 100.65.0.0/16), ZTNA connector traffic may be blocked on the MU-SPN.</p> <p>Workaround: Contact your Prisma Access team to update the SaaS Agent version of all your Prisma Access tenants.</p>
CYR-38619	Tenants that are onboarded in Switzerland and France cannot use ZTNA Connector.
CYR-38120	<p>All available locations do not show up in the list view in the Mobile Users—Explicit Proxy setup page.</p> <p>Workaround: Use the map view to select the missing locations.</p>
CYR-37983	<p>If you have IPv6 enabled for a Mobile Users—GlobalProtect user, retrieving the HIP report causes a crash.</p> <p>Workaround: If the GlobalProtect client is ipv6 enabled, run the HIP report using the client's IPv6 address. If the GlobalProtect client is IPv4 only, run the HIP report using the client's ipv4 address.</p>
CYR-37923	After creating a new URL category or security rule or an EDL, a local Panorama commit is required before using that object in RBI security rule associations.
CYR-37906	<p>If, when updating the ports for an existing wildcard object, you put spaces between the ports, a 500 internal server error is displayed.</p> <p>Workaround: Do not put spaces between the ports. For example, instead of 1-2, 80, 100-300, put 1-2,80,100-300.</p>
CYR-37887	<p>If you are using ZTNA Connector as part of the 30-day trial and have not purchased a license, onboarding might fail with a message that Something went wrong when you click the Enable ZTNA Connector button.</p> <p>Workaround: Refresh the UI to complete the onboarding of the ZTNA Connector feature.</p>
CYR-37826	If two or more ZTNA connector applications have the same FQDN, an Application Custom rule

Issue ID	Description
	<p>conflict message could display in the SD-WAN portal.</p> <p>Workaround: This message is spurious and can be ignored.</p>
CYP-37797	<p>The status page asks you for a one-time password (OTP) after a plugin upgrade.</p> <p>Workaround: Delete the expired license keys, delete the Panorama certificate, and retrieve the licenses and verify if the license keys are valid after you retrieve them; then, generate the OTP to verify.</p>
CYP-37755	<p>If you configure a Wildcard Target in ZTNA Connector, and if you try to change the port of an application that was discovered as a result of that target and was added to the FQDN Target, you receive an error that the name is too long.</p> <p>Workaround: While application names can be a maximum of 32 characters long, changing the port number makes the name too long in the ZTNA Connector infrastructure. If you encounter this error, try to give the application a shorter name.</p>
CYP-37706	<p>When using Explicit Proxy, an excessive amount of threat logs display.</p> <p>Workaround: Ignore the threat logs. These logs have no impact on Explicit Proxy functionality.</p>
CYP-37673	<p>Clicking the Panorama > Cloud Services > Status > Status > Remote Browser Isolation > Active Isolated Session link does not open the Monitor > Subscription Usage page in Prisma Access Cloud Management or Strata Cloud Manager.</p>
CYP-37466	<p>If you enable Colo-Connect, do not enable Bidirectional Forwarding Detection (BFD) on your VLAN.</p>
CYP-37356	<p>If you renew the App Acceleration license after it has expired (including the grace period for the license), the renewal does not take effect immediately.</p> <p>Workaround: Wait approximately one hour after license renewal before using App Acceleration.</p>
CYP-37290	<p>When onboarding a ZTNA Connector, you receive a <code>declaim requested by root</code> error.</p>

Issue ID	Description
	Workaround: Delete the connector that had the error and create a new one.
CYP-37227	<p>The creation of the IP subnet-based Connector Group sometimes fails with a group already exists message, even though the group does not exist.</p> <p>Workaround: Use another name for the IP subnet-based Connector Group.</p>
CYP-37208	When using Prisma Access Clean Pipe, the Network Details page (Panorama > Cloud Services > Status > Status > Network Details) does not show Clean Pipe entries.
CYP-36749	ZTNA connector flow logs related to netflow may not be visible in the Strata Cloud Manager Log Viewer.
CYP-34999	For Panorama Prisma Access tenants, if ZTNA Connectors are onboarded, the Provision Progress for service connections (Panorama > Cloud Services > Status > Status > Service Connections > Provision Progress) is showing provisioning progress for both ZTNA Connectors and Service Connections.
CYP-34720	GlobalProtect DDNS functionality does not work when using a Panorama running 10.1.x to manage Prisma Access with the Cloud Services plugin.
CYP-33877	If, during Explicit Proxy setup, you select Skip authentication to skip authentication for an address object, and then later want to enable authentication by deselecting Skip authentication for that address object, it can take up to 24 hours for the change to take effect after you make the change and Commit and Push your changes.
CYP-33471	<p>If you enable multi-tenancy, create a new sub tenant, configure Mobile Users—GlobalProtect, Remote Networks, and Colo-Connect device groups, then configure Colo-Connect subnets and VLANs, and a partial commit fails with an Unable to retrieve last in-sync configuration for the device error.</p> <p>Workaround: Perform a Commit and Push operation when configuring Colo-Connect for the first time instead of a partial commit.</p>

Issue ID	Description
CYR-33454	<p>If you configure Prisma Access in a multi-tenant deployment, perform a Commit and Push, then configure Colo-Connect, the choice to Commit and Push your changes is grayed out.</p> <p>Workaround: Click Commit > Commit to Panorama, then Commit > Push to Devices, click Edit Selections and make sure that Colo-Connect is selected in the Push Scope; then, retry the commit and push operation.</p>
CYR-33199	<p>Current user counts and 90 day user counts are not correct for Kerberos authenticated users.</p>
CYR-33145	<p>When a Prisma Access license for any service type expires, any Commit All operation fails a generic Commit Failed error message.</p> <p>Workaround: Make sure that your all your Prisma Access licenses have not expired before performing commits.</p>
CYR-32687	<p>EDLs, Address objects of type IP Wildcard Mask and FQDN, and Dynamic Address Groups do not work on decryption policies when Agent or Kerberos authentication is used with Explicit Proxy.</p> <p>Workaround: Use Address objects of IP Netmask, IP Range, or Address groups in the decryption policies.</p>
CYR-32666	<p>When importing a previously saved Panorama configuration that included a Colo-Connect configuration, or reverting from a previously-saved configuration, you receive errors if the following conditions are present:</p> <ul style="list-style-type: none"> • You are loading a Configuration that has Colo-Connect service connections configured. • You are loading an empty Prisma Access configuration. • You revert from a previously-saved configuration, and the following conditions are present: <ul style="list-style-type: none"> • A Colo-Connect configuration (with service connections) exists on the current configuration and a Colo-Connect configuration does not exist on the configuration to which you want to revert. • A Colo-Connect configuration does not exist on the current configuration and a Colo-Connect

Issue ID	Description
	<p>configuration (with service connections) exists on the configuration to which you want to revert.</p> <ul style="list-style-type: none"> • A Colo-Connect configuration (with service connections) exists on the current configuration and also exists on the configuration to which you want to revert. <p>Workaround: Colo-Connect service connections cannot be onboarded unless their corresponding VLANs are in an Active state. Delete any Colo-Connect service connections before exporting or reverting a Panorama image; then, re-create the Colo-Connect service connections after importing the new image.</p>
CYR-32661	<p>When GlobalProtect is connected in Proxy mode or Tunnel and Proxy mode, user logins will not count toward the number of current users or the number of users logged in over the past 90 days under Mobile Users—Explicit Proxy.</p>
CYR-32564	<p>ZTNA Connector app traffic is detected as a threat and dropped for Prisma Access Cloud Management if the default URL category is used.</p> <p>Workaround: Perform one or more of the following steps as required:</p> <ol style="list-style-type: none"> 1. Create a custom URL category and add application FQDNs for the onboarded applications for ZTNA connector. 2. If you are using a default profile group, clone a new group and attach the custom URL category you created in Step 1. If you are using a custom profile group, attach the custom URL category you created in step 1. 3. Make sure that you attach either the cloned profile group or the custom profile group (from step 2) to the security policy you created to allow traffic destined to ZTNA connector applications.
CYR-32511	<p>You can configure IPv6 DNS addresses even if IPv6 is disabled.</p>
CYR-32431	<p>When configuring Explicit Proxy, when you add Trusted Source Address values under Authentication Settings, configure other settings, and then return to the Authentication Settings tab, the trusted source addresses might not display correctly.</p>

Issue ID	Description
	<p>Workaround: Refresh the Panorama that manages Prisma Access, then return to the Authentication Settings tab to see the addresses.</p>
CYR-31603	<p>ZTNA Connectors with two interfaces are not supported in a Connector Group enabled for AWS Auto Scale. This is due to an AWS Auto Scale group limitation that ties both interfaces to the same subnet. See this article for details.</p> <p>Workaround: ZTNA Connectors with two interfaces are supported in Connector Groups that are not enabled for AWS Auto Scale. Ensure that all ZTNA Connectors with two interfaces are contained in a Connector Group that is not enabled for AWS Auto Scale.</p>
CYR-31187	<p>In order to use the Prisma Access Explicit Proxy Connectivity in GlobalProtect for Always-On Internet Security functionality, the default PAC file URL does not populate properly unless you do a commit and push to both Mobile Users—GlobalProtect and Mobile Users—Explicit Proxy.</p> <p>Workaround: When you Commit and Push, make sure that you choose both Mobile Users—GlobalProtect and Mobile Users—Explicit Proxy in the Push Scope when configuring Prisma Access Explicit Proxy connectivity in GlobalProtect.</p>
CYR-30966	<p>When all users are removed from a group, CIE does not sync the empty group to the firewalls. This is expected behavior.</p> <p>Workaround: Delete empty groups from Firewall configurations.</p>
CYR-30414	<p>If you have enabled multiple portals in a multitenant deployment that has only one tenant, and you then disable the multiple portal functionality on that single tenant, you are able to see both portals on the UI.</p> <p>Workaround: Open a CLI session on the Panorama that manages Prisma Access and enter the following commands, then perform a local commit on the Panorama:</p> <pre>set plugins cloud_services multi-tenant tenants <tenant_name> mobile-users multi-portal-multi-auth no</pre>

Issue ID	Description
	request plugins cloud_services gpcs multi-tenant tenant-name <tenant_name> multi_portal_on_off
CYR-30044 This issue is now resolved in Prisma Access 6.0.0. See Prisma Access 6.0.0 Addressed Issues.	<p>Predefined EDLs aren't being populated in the Block Settings list in a new Explicit Proxy deployment.</p> <p>Workaround: Onboard your Explicit Proxy deployment, perform a Commit and Push operation, and then go back and update the EDL in your block Settings.</p>
CYR-29964	<p>Attempts to reuse a certificate signing request (CSR) to generate a certificate results in a "Requested entity already exists" error.</p> <p>Workaround: Do not reuse CSRs.</p>
CYR-29933	<p>Attempts to use the verdicts:all -X "DELETE" API call more than one time per hour result in the {"code" :8, "message" : "Too many requests" error.</p> <p>Workaround: Do not use this API call more than one time per hour.</p>
CYR-29700	<p>If you configure multiple GlobalProtect portals in a multitenant Prisma Access Panorama Managed multitenant deployment, committing changes on a per-username basis fails with a "global-protect-portal-8443 should have the value "GlobalProtect_Portal_8443" but it is [None]" error.</p> <p>Workaround: If you have enabled multiple GlobalProtect portals and have a Prisma Access multi-tenant deployment, perform Commit All commit operations instead of committing on a per-user basis.</p>
CYR-26112	<p>If you do not have a Net Interconnect license, all Remote Networks in a theater are fully meshed, but if you haven't onboarded a Service Connection in a theater, the Remote Networks cannot be reached from Remote Networks in other theaters.</p> <p>Workaround: Either purchase a Net Interconnect license or onboard a service connection in a theater to have the Remote Networks communicate with other theaters.</p>

Issue ID	Description
ZY-6093	<p>For specific applications involving developer code (such as code AI or similar), the Private App Security OWASP best practices policy might get hits that are triggered by the nature of the app (for example, code snippets detected in the app requests could be interpreted as injection attempts). For such scenarios, we recommend creating an OWASP Best Practices policy clone, set it in Preview mode, analyze the alerts, and define proper exceptions to eliminate such false positives.</p>
ZY-5969	<p>Private App Security rules inspect HTTP request data to identify threats. When a rule flags a hit that is proved to be a false positive (for example, securing a coding app), it's crucial to apply the correct exclusion to prevent false positives. WAF rules primarily inspect two main variables that include cookie data:</p> <ul style="list-style-type: none"> • REQUEST_HEADERS—This variable inspects all request headers as a whole, which inherently includes any cookie header. • REQUEST_COOKIES—Some rules specifically inspect the Cookie header content by itself. In this case, the WAF log explicitly states that a REQUEST_COOKIE (or a similar cookie variable) matched. <p>To help create a proper exception for a false positive, Private App Security provides a field called "exclusionConfiguration" and applies the exclusion to the precise variable that triggered the match.</p>
ZY-5589	<p>Due to the nature of distributed systems, this change introduces a small, expected delay of up to a few seconds in how rate limits are applied across all locations.</p> <p>The configured time window for global rate limits (for example, 60 requests per 60 seconds) may now have a slight differential, typically up to a few seconds. For example, a 60-second limit might take up to 63 seconds to reset fully. This is a result of the necessary propagation delay, as data is aggregated from various data centers to our central service for processing. This approach is essential for maintaining the robustness and scalability of our platform.</p> <p>This change is part of an ongoing effort to enhance the stability and performance of our services. The slight</p>

Issue ID	Description
	timing differential is an expected trade-off for a more reliable and scalable rate-limiting system.
ZY-2603	Private App Security only inspects traffic destined to the private application accessed through GlobalProtect or Prisma Access Agent and remote networks connected over IPsec tunnels.
ZY-2151	<p>Threats—Non-SNI and mTLS traffic can be used to bypass the app security traffic inspection flow. An attacker could leverage this to bypass security controls by crafting requests using these protocols. This creates a significant security gap, as malicious traffic using these protocols would not be inspected or blocked by the WAF or other Private App Security components.</p> <p>Countermeasures—To mitigate the security risk of bypassing Private App Security for non-SNI and mTLS traffic:</p> <ul style="list-style-type: none"> • Enforce SNI and Inspect mTLS Traffic—Configure a reverse proxy or load balancer to enforce SNI for all incoming HTTPS connections. For mTLS traffic, terminate the mTLS connection at the proxy/load balancer and then re-encrypt the traffic with a separate certificate for inspection by the Private App Security infrastructure. • Deploy a reverse proxy or load balancer capable of SNI enforcement and mTLS termination. • Configure the proxy/load balancer to reject connections without SNI. • For mTLS, configure the proxy/load balancer to act as the server for the initial mTLS handshake. Validate the client certificate and then establish a new TLS connection to the back-end server using a certificate trusted by the Private App Security infrastructure. • Integrate the proxy/load balancer with the Private App Security components (such as WAF) to ensure all decrypted traffic is inspected.
ZY-1166	When you update the expired CA certificate in Strata Cloud Manager, it can take up to 90 minutes for the change to fully reach the dataplane. Make sure to plan ahead and replace certificates well before they expire, keeping this propagation time in mind.

Known Issues for Dynamic Privilege Access

Issue ID	Description
PANG-4870	<p>On macOS devices that have the Prisma Access Agent installed, if you remove the full disk access for the security extension for the Prisma Access Agent (after granting full disk access previously), the Prisma Access Agent will get stuck in the disabled mode.</p> <p>Workaround: Grant access to the security extension by selecting System Settings > Privacy & Security > Full Disk Access and enabling the securityExtension from the list of apps.</p>
PANG-4825	<p>When configuring forwarding profiles, an issue exists where configuring large numbers of forwarding rules for source applications, destination domains, and IP addresses (routes) can cause high CPU utilization.</p> <p>Workaround: Do not configure more than 100 forwarding rules for source applications, destination domains, and IP addresses.</p>
NETVIS-1363	<p>In Insights on Strata Cloud Manager, the Project Connectivity History view in the user details page shows only the project name and no other detail when the Prisma Access Agent user is connected. The Project Connectivity History is blank when the user is not connected.</p>
NETVIS-1263	<p>In Insights, the number of connected users listed in the Projects tab might not be accurate. In some cases, the number of connected users in the Project tab does not match the number of users in the Users tab. For example, when the same user is connected to two projects on different devices, the number of connected users in the Projects tab does not match the number of users in the Users tab.</p>
NETVIS-1207	<p>In Insights, the Projects tab does not show all the IP pools that are configured for a project. Only the IP pools that are in use are shown.</p>
EPM-2954	<p>User groups that have more than 50000 users are not supported in the project configuration of Dynamic Privilege Access. Make sure that the user group associated with a project has less than 50000 users.</p>

Issue ID	Description
EPM-1589	When configuring forwarding profiles, even though Strata Cloud Manager allows you to configure IP addresses with wildcards, using wildcard characters in destination IP addresses, such as 10.*.*.* , is not supported as it will cause inconsistent behavior in forwarding profiles.
EPM-1399	<p>Changing a project name in the Projects tab of the Dynamic Privilege Access page in Strata Cloud Manager is not supported at this time.</p> <p>Workaround: To rename a project, delete the existing project and perform an Access Agent push configuration, then create the project with the new name and perform an Access Agent push configuration.</p>
EPM-646	<p>On a Prisma Access tenant where Dynamic Privilege Access is enabled, a configuration push will fail if you try to push the Prisma Access Agent infrastructure configuration without first configuring any projects.</p> <p>Workaround: Configure at least one project before you do a push config.</p>
DRS-4907	<p>Updates made in the Identity Provider (IdP) are not immediately reflected in the Cloud Identity Engine and Prisma Access Agent management plane. This delay occurs because the Cloud Identity Engine needs to sync with the IdP to capture the changes. The Cloud Identity Engine runs sync jobs every 5 minutes, but only when no other sync is in progress. The duration of the sync process is affected by the magnitude of changes in the Cloud Identity Engine directory, meaning larger or more numerous changes will result in a longer sync time. After the sync is complete, it can take up to 15 minutes for the changes to appear in the Prisma Access Agent management plane.</p>
DRS-4691	<p>When searching for a user group in Cloud Identity Engine or Strata Cloud Manager using the Text Search option, surround the user group name with double quotes. For example, when searching for a user group named EXAMPLE.User_Group, enter "EXAMPLE.User_Group".</p>
DRS-4406	<p>When configuring a project in Strata Cloud Manager, you cannot search for a User group by providing a partial user group name.</p>

Issue ID	Description
	<p>Workaround: To search for a user group, enter the complete User group name.</p>
DOCS-7025	<p>An issue exists in Dynamic Privilege Access where existing IP pools configured in a project cannot be modified.</p> <p>Workaround: To modify an existing IP pool, delete the existing IP pool in a project and save the project. Then, edit the project again to add the new IP pool. For example, to change the IP pool address from 10.10.10.0/25 to 10.10.10.0/24, delete the existing pool in the project, save the project, and edit the project again to add the new IP pool.</p>
DOCS-5681	<p>Enabling ZTNA Connector on a Dynamic Privilege Access enabled tenant is not supported in Prisma Access 6.0.</p> <p>Enabling ZTNA Connector on a Dynamic Privilege Access enabled tenant can cause issues in routing. Service might also be impacted because Strata Cloud Manager does not support the deletion of ZTNA Connector once it has been created.</p>
DOCS-5611	<p>When authorizing user group mapping in Cloud Identity Engine for Dynamic Privilege Access, when selecting the SAML attributes you want Prisma Access to use for authentication, ensure that you select a Username Attribute that contains /identity/claims/name.</p> <p>If you select the wrong username attribute, your users will not be able to authenticate to their projects.</p>
DOCS-5463	<p>An issue exists where random tunnel disconnects can occur if the Collect HIP Data option is not enabled in the Agent Settings page. Therefore, do not disable Collect HIP Data in the Host Information Profile (HIP) section of the Access Agent Settings page.</p>
DOCS-3650	<p>For Cloud Identity Engine authentication to work on a Dynamic Privilege Access enabled Prisma Access tenant, ensure that a user group is not mapped to multiple SAML applications in the identity provider (IdP).</p> <p>If multiple apps are mapped to a user group, Cloud Identity Engine cannot determine which SAML app to</p>

Issue ID	Description
	connect to during authentication because there is no unique mapping.
ADI-33262	<p>On a Prisma Access tenant where Dynamic Privilege Access is enabled, a Mobile User Container > Access Agent configuration push will fail without first configuring a project in Strata Cloud Manager.</p> <p>Workaround: Configure at least one project before you do a push config.</p>
ADI-31601	<p>On a Dynamic Privilege Access enabled tenant, Strata Cloud Manager allows you to configure more than 100 IP pools per project, even though it will cause the push config to fail with a generic error.</p> <p>Workaround: Do not configure more than 100 IP pools per project.</p>
ADI-31538	<p>An issue exists where, when setting up a forwarding profile, the forwarding profile Type is displayed as "ZTNA Agent" instead of "Prisma Access Agent". Also, if you select Add Forwarding Profile, the drop-down shows "ZTNA Agent" instead of "Prisma Access Agent".</p> <p>Workaround: None. The forwarding profile type will be changed to "Prisma Access Agent" in the future.</p>
ADI-31523	<p>Do not create snippets with descriptions that contain special characters. Snippet descriptions that contain special characters such as ! ~ @ # \$ % ^ & * () _ + are not supported.</p>
ADI-30902	<p>Strata Cloud Manager uses the user and user group information from a Cloud Identity Engine directory in multiple configurations, such as Dynamic Privilege Access project configurations, Prisma Access Agent settings, security policies, and staged rollout configurations. After making these configurations, if you delete the directory from Cloud Identity Engine but don't delete the Strata Cloud Manager configurations that reference those users and user groups, you might encounter unexpected errors, such as "500 Internal Server Error."</p> <p>Workaround: When you remove a directory from Cloud Identity Engine, you must also delete the Strata Cloud Manager configurations that reference the users and user groups in that directory.</p>

Issue ID	Description
ADI-29665	Do not use special characters in project names, otherwise Strata Cloud Manager will issue a "Malformed Request" error message when you try to save the project configuration.
ADI-29434	In the Agent Settings page in Strata Cloud Manager, the recommended value for the Session timeout is 7 days.
ADI-29272	When creating a snippet, if you disable the Add prefix to object names option, ensure that you don't use duplicate agent settings names in two different snippets, since it can result in unexpected behavior.
ADI-26493	<p>In Access Agent > Infrastructure Settings in Strata Cloud Manager, the OnPrem DHCP Server option in the Client IP Pool Allocation section is not selectable. This is working as intended since OnPrem DHCP Server is not supported for Dynamic Privilege Access.</p> <p>This option will be renamed to OnPrem DHCP Server (Preview Only) so that existing Dynamic Privilege Access enabled Prisma Access tenants can function correctly.</p>

Prisma Access Addressed Issues

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none">Prisma Access (Managed by Panorama)	<ul style="list-style-type: none">Prisma Access licenseMinimum Required Prisma Access Version 6.0 Preferred or Innovation

The following topics describe issues that have been addressed in Prisma Access 6.0 and Prisma Access 6.0.1.

Prisma Access 6.0.1 Addressed Issues

Issue ID	Description
CYR-41740	Fixed an issue where, if there were more than 100 connectors onboarded in the same region in a short duration of time, private app access through some of the ZTNA connectors might not work.

Prisma Access 6.0.0-h40 Addressed Issues

Issue ID	Description
CYR-58965	Fixed an issue where Panorama did not send the onboarding commit job to the backend when onboarding Service Connections, requiring a secondary push to properly trigger the commit job for Service Connections.
CYR-58852	Fixed an issue where Panorama commit validation workflows would fail if a tenant's licenses had the "no_limit" string under the service_connection local service chain information in the license_capabilities. This occurred because the system was attempting to convert the string to an integer.
CYR-58332	Fixed an issue where commits to GlobalProtect gateways failed with a validation error related to the `max-version` setting in the SSL-TLS service profile.

Issue ID	Description
CYR-58134	Fixed an issue where the Private App Access option is automatically disabled by the Cloud Services plugin when the plugin was upgraded from 5.1.0-39 to 6.0.0-11 in Panorama. When this configuration was pushed to Prisma Access, customers faced outages to critical internal applications.
CYR-57700	Fixed an issue where any changes to the Cloud Services Plugin onboarding configuration on Panorama resulted in an error when the 'DEFAULT' config was missing in the GlobalProtect portal.
CYR-57636	Fixed an issue where users were unable to view remote network bandwidth usage statistics on Panorama.
CYR-57060	Fixed an issue where, on existing aggregate bandwidth deployments that have remote network SPNs configured and use site-based licensing, previously configured remote networks SPNs were not displayed in the Panorama UI.
CYR-55228	Fixed an issue where the bulk creation of remote networks for Prisma Access multitenant failed.
CYR-54503	Fixed an issue where domain configurations were not applied to mobile users during a partial commit on Panorama, while the same configurations were successfully applied to remote networks.
CYR-53575	Fixed an issue where commits for passive Panorama failed, preventing the ability to perform a required local commit from passive Panorama.

Prisma Access 6.0.0-h25 Addressed Issues

Issue ID	Description
CYR-56987	Fixed an issue where the Panorama > Cloud Services > Services > Monitor > <location> > Status Page filter is not working correctly.

Issue ID	Description
	Instead of showing a status, a continuously loading icon is displayed on the upper right.
CYR-54896	Fixed an issue where, when using VM Panorama 11.1.6-h4, users are unable to create access route from Panorama.

Prisma Access 6.0.0-h22 Addressed Issues

Issue ID	Description
CYR-55537	Fixed an issue related to search fields in remote network, service connection, and mobile user templates for the Zones tab.
CYR-55228	Fixed an issue where, after a bulk import of remote networks using a .csv file, a commit failure was encountered.
CYR-55216	Fixed an issue where the a commit-all operation failed for a Hybrid-SWG device or platform that doesn't support the Cloud Services plugin.
CYR-55138	Fixed an issue where the Aggregate Bandwidth widget was not being displayed for remote networks in the Cloud Services plugin.
CYR-54543	Fixed an issue where Panorama-based forced GlobalProtect logout was failing when a logged in user had a special character in the user name or computer name. You can now have a successfully log out users or computers that have a special character in the username or computer name using the logout button on the panorama plugin for Prisma Access.
CYR-54428	Fixed an issue related to the Service Connection Device Group Template Stack.
CYR-53485	Fixed an issue where a GlobalProtect app log certificate, which is required for ADEM, could not be generated for Prisma Access China.

Prisma Access 6.0.0-h11 Addressed Issues

Issue ID	Description
CYR-55020	Fixed an issue where the Cloud Services plugin did not display the Remote Networks and Mobile Users configuration.
CYR-49944	Fixed an issue where a secondary DNS server was configured, which should not be allowed.
CYR-29269	Fixed an issue to increase log the size and the number of log files for the Cloud Services plugin.

Prisma Access 6.0.0-h9 Addressed Issues

Issue ID	Description
CYR-54776	Fixed an issue where BGP filtering was enabled for all tenants in a multitenant deployment that was converted from a single tenant deployment. If you have an existing Prisma Access non-multitenant deployment and convert it to a multitenant deployment, only the first tenant (the tenant you migrated) supports BGP filtering.
CYR-53941	Fixed an issue where, when onboarding remote networks using configuration import in a multi-tenant deployment, an import error was seen.
CYR-53752	Fixed an issue where the Cloud Services plugin's trusted endpoint value was empty when the environment variable was set to None.
CYR-53092	Fixed an issue where the Panorama commit was failing when the UI attempted to generate the IoT configuration automatically in a tenant with that had Base SITE and IOT SITE SKUs.

Prisma Access 6.0.0-h3 Addressed Issues

Issue ID	Description
CYR-53485	Fixed an issue where a GlobalProtect app log certificate, which is required for ADEM, could not be generated for Prisma Access China.


Prisma Access 6.0.0 Addressed Issues

Issue ID	Description
CYR-53726	Fixed an issue where, for tenants using site-based licensing for branch sites, the site license type may display as Unknown for certain branch sites within SCM > Monitor > Branch Sites .
CYR-53725	Fixed an issue where, for tenants using site-based licensing for branch sites, the dashboard under SCM > Monitor > Branch Sites might be intermittently unavailable in Prisma Access locations, including Qatar, Taiwan, Indonesia, Israel, and Saudi Arabia.
CYR-52199	Fixed an issue where the drop down menu for bandwidth for Clean Pipe displayed incorrect bandwidths.
CYR-51478	Fixed an issue where, if you used Dynamic Privilege Access, using ZTNA Connectors without at least one service connection was not supported.
CYR-50707	Fixed an issue where, if you were using IP Optimization with ZTNA Connector, Source IP Address stickiness (the ability for users to maintain the same egress IP for the same source IP address in a session) was not supported.
CYR-47741	Fixed an issue where the Singapore Colo-Connect service connection went down after a dataplane upgrade to 10.2.10-h8.
CYR-46170	Fixed an issue where, if you enabled DDNS and you later pushed a service subnet change to your mobile users, you must also restart the

Issue ID	Description
	DDNS plugin on your Mobile User gateway for DDNS to pick up the change.
CYR-45847	Fixed an issue where, when a service subnet was changed, it as updated on the Prisma Access GlobalProtect gateways, but the GlobalProtect tunnel went down because NAT was not correctly implemented.
CYR-45517	Fixed an issue where, in the Colo-Connect tab, a read-only user was able to delete onboarding entries.
CYR-45341	Fixed an issue where Commit and Push jobs to Colo-Connect Device Groups were timing out, causing VLANs to not be deleted.
CYR-45440	Fixed an issue where, when configuring Admin Roles, the access information was not always saved correctly.
CYR-44391	Fixed an issue where Explicit Proxy deployments in China did not support using the Cloud Identity Engine or SAML for authentication.
CYR-44433	Fixed an issue where the status for Remote Network jobs that were successful can change from Success to Pending state.
CYR-44079	Fixed an issue where the GlobalProtect DDNS logs were not rotating and the file size kept increasing.
CYR-43690	Fixed an issue where, when attempting to modify or delete Connector IP Blocks in ZTNA Connector, the changes were not applied after a Commit and Push.
CYR-43062	Fixed an issue where we did not support the 5.1 DDNS feature along with the IPv6 sinkhole service.
CYR-42919	Fixed an issue where, when attempting to modify or delete Connector IP Blocks in ZTNA Connector, the changes are not applied after a Commit and Push.

Issue ID	Description
CYR-42480	Fixed an issue where private app access could be used in deployments only when Proxy Mode or Prisma Access Browser were enabled.
CYR-41838	Fixed an issue where the egress IP address for Remote Networks - High Performance deployments displayed twice when you retrieved it using the Prisma Access API.
CYR-39148	Fixed an issue where, when configuring Colo-Connect, Commit and Push operations to Colo Connect Device Groups might intermittently fail.
CYR-30044	Fixed an issue where predefined EDLs weren't being populated in the Block Settings list in a new Explicit Proxy deployment.

Panorama Support for Prisma Access 6.0

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> Prisma Access (Managed by Panorama) 	<ul style="list-style-type: none">  Prisma Access license  Minimum Required Prisma Access Version 6.0 Preferred or Innovation

Prisma Access (Managed by Panorama) releases 6.0 use the **Cloud Services Plugin 6.0** Cloud Services plugin. Prisma Access (Managed by Panorama) release 6.0.1 requires a minimum Cloud Services plugin version of 6.0.0-h9. If you're using Panorama to manage Prisma Access and need to upgrade to the 6.0 plugin, you need to:

1. [Review the required software versions for Panorama to support Prisma Access 6.0 Preferred and Innovation](#)
2. [Determine the upgrade path you'll need to follow for the Cloud Services Plugin](#)
3. [Upgrade the Cloud Services Plugin](#)

Required and Recommended Software Versions for Panorama Managed Prisma Access 6.0 and 6.0.1

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> Prisma Access (Managed by Panorama) 	<ul style="list-style-type: none"> Prisma Access license Minimum Required Prisma Access Version 6.0 Preferred or Innovation

Recommended Software Versions for Prisma Access 6.0.1 Preferred and Innovation

Prisma Access 6.0.1 Preferred and Innovation run a PAN-OS 11.2.6 dataplane. Prisma Access (Managed by Panorama) release 6.0.1 requires a minimum Cloud Services plugin version of 6.0.0-h9.

For Prisma Access 6.0.1 features, Palo Alto Networks **recommends that you upgrade your Prisma Access to the following versions** before installing the plugin.

Prisma Access Version	Cloud Services Plugin Version	Required Dataplane Version for 6.0.1	Recommended GlobalProtect Version	Recommended Panorama Version
6.0.1	Minimum version of 6.0.0-h9	6.0.1 Preferred and Innovation: PAN-OS 11.2.6	6.0.1.7+ 6.1.3+ 6.2.1+ Minimum required versions for IPv6 Support for Public Apps for IP Optimization: <ul style="list-style-type: none"> 6.2.6 client version for Windows and macOS 6.2.7 for Linux 6.1.7 for Android and IOS 	10.2.10+ 11.0.1+ 11.1.0 11.2.6 12.1.2 Before you upgrade your Panorama to 12.1.2, upgrade your Cloud Services plugin to 6.0.0-h22; then, upgrade your Panorama. Be sure to follow the upgrade path when upgrading your plugin.

Recommended Software Versions for Prisma Access 6.0 Preferred and Innovation

Prisma Access 6.0 Preferred and Innovation run on a PAN-OS 11.2.6 dataplane.

For Prisma Access 6.0 features, Palo Alto Networks **recommends that you upgrade your Prisma Access to the following versions** before installing the plugin.

Prisma Access Version	Cloud Services Plugin Version	Required Dataplane Version for 6.0	Recommended GlobalProtect Version	Recommended Panorama Version
6.0	6.0	PAN-OS 11.2.6 for 6.0 Preferred and Innovation	6.0.7+ 6.1.3+ 6.2.1+ Minimum required versions for IPv6 Support for Public Apps for IP Optimization: <ul style="list-style-type: none"> 6.2.6 client version for Windows and macOS 6.2.7 for Linux 6.1.7 for Android and IOS 	10.2.10+ 11.0.1+ 11.1.0 11.2.6 12.1.2 Before you upgrade your Panorama to 12.1.2, upgrade your Cloud Services plugin to 6.0.0-h22; then, upgrade your Panorama. Be sure to follow the upgrade path when upgrading your plugin.

Upgrade Considerations for Prisma Access 6.0

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> Prisma Access (Managed by Panorama) 	<ul style="list-style-type: none"> Prisma Access license Minimum Required Prisma Access Version 6.0 Preferred or Innovation

To upgrade your Cloud Services plugin to Prisma Access 6.0, use one of the following upgrade paths. To find your current plugin version in Panorama, select **Panorama > Cloud Services > Configuration > Service Setup** and check the plugin version in the **Plugin Alert** area.

Be sure to follow the [minimum Panorama versions](#) for each plugin version during the upgrade.

Installed Cloud Services Plugin Version	Targeted Version	Plugin Upgrade Path
5.1	6.0	Upgrade your plugin from Prisma Access 5.1 to Prisma Access 6.0 and commit and push your changes.
5.0	6.0	<ol style="list-style-type: none"> Upgrade your plugin from Prisma Access 5.0 to Prisma Access 5.1 and commit and push your changes. Upgrade your plugin from Prisma Access 5.1 to Prisma Access 6.0 and commit and push your changes.
4.1 and 4.2	6.0	<ol style="list-style-type: none"> Upgrade your plugin from Prisma Access 4.1 to Prisma Access 5.0 and commit and push your changes. Upgrade your plugin from Prisma Access 5.0 to Prisma Access 5.1 and commit and push your changes. Upgrade your plugin from Prisma Access 5.1 to Prisma Access 6.0 and commit and push your changes.
4.0	6.0	<ol style="list-style-type: none"> Upgrade your plugin to Prisma Access 4.1 and commit and push your changes. Upgrade your plugin to Prisma Access 5.0 and commit and push your changes. Upgrade your plugin from Prisma Access 5.0 to Prisma Access 5.1 and commit and push your changes.

Installed Cloud Services Plugin Version	Targeted Version	Plugin Upgrade Path
		<ol style="list-style-type: none"> 4. Upgrade your plugin from Prisma Access 5.1 to Prisma Access 6.0 and commit and push your changes.
3.0, 3.1, and 3.2 Preferred	6.0	<ol style="list-style-type: none"> 1. (3.0 plugins only) Upgrade your plugin to Prisma Access 3.1 and commit and push your changes. 2. (3.1 plugins only) Upgrade your plugin to either Prisma Access 3.2 or 3.2.1 and commit and push your changes. 3. Upgrade your plugin to either Prisma Access 3.2 or 3.2.1 and commit and push your changes. 4. Upgrade your plugin to Prisma Access 4.0 and commit and push your changes. 5. Upgrade your plugin to Prisma Access 4.1 and commit and push your changes. 6. Upgrade your plugin to Prisma Access 5.0 and commit and push your changes. 7. Upgrade your plugin from Prisma Access 5.0 to Prisma Access 5.1 and commit and push your changes. 8. Upgrade your plugin from Prisma Access 5.1 to Prisma Access 6.0 and commit and push your changes.
2.2 Preferred	6.0	<ol style="list-style-type: none"> 1. Upgrade your plugin to Prisma Access 3.0 and commit and push your changes. 2. Upgrade your plugin to Prisma Access 3.1 and commit and push your changes. 3. Upgrade your plugin to either Prisma Access 3.2 or 3.2.1 and commit and push your changes. 4. Upgrade your plugin to Prisma Access 4.0 and commit and push your changes. 5. Upgrade your plugin to Prisma Access 4.1 and commit and push your changes. 6. Upgrade your plugin to Prisma Access 5.0 and commit and push your changes. 7. Upgrade your plugin from Prisma Access 5.0 to Prisma Access 5.1 and commit and push your changes.

Installed Cloud Services Plugin Version	Targeted Version	Plugin Upgrade Path
		<ol style="list-style-type: none"> Upgrade your plugin from Prisma Access 5.1 to Prisma Access 6.0 and commit and push your changes.
Releases earlier than 2.2 Preferred	6.0	<ol style="list-style-type: none"> Upgrade your plugin to Prisma Access 2.2 and commit and push your changes. If your deployment is on a version of Prisma Access that is earlier than 2.2 Preferred, you must first upgrade to 2.2 before you can upgrade to 3.2. Upgrades from 2.0 or 2.1 versions of Prisma Access are not supported. Upgrade your plugin to Prisma Access 3.0 and commit and push your changes. Upgrade your plugin to Prisma Access 3.1 and commit and push your changes. Upgrade your plugin to either Prisma Access 3.2 or 3.2.1 and commit and push your changes. Upgrade your plugin to Prisma Access 4.0 and commit and push your changes. Upgrade your plugin to Prisma Access 4.1 and commit and push your changes. Upgrade your plugin to Prisma Access 5.0 and commit and push your changes. Upgrade your plugin from Prisma Access 5.0 to Prisma Access 5.1 and commit and push your changes. Upgrade your plugin from Prisma Access 5.1 to Prisma Access 6.0 and commit and push your changes.

Upgrade the Cloud Services Plugin

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none">Prisma Access (Managed by Panorama)	<ul style="list-style-type: none">Prisma Access licenseMinimum Required Prisma Access Version 6.0 Preferred or Innovation

Use the following procedure to upgrade the Cloud Services plugin.

Prisma Access uses the Cloud Services plugin in Panorama to activate its functionality.

For a list of the Panorama software versions that are supported with Prisma Access, see [Minimum Required Panorama Software Versions](#) in the [Palo Alto Networks Compatibility Matrix](#).

Before you upgrade the plugin, remove any non-Prisma Access templates from Prisma Access template stacks to avoid commit validation errors after upgrade and make sure that the Panorama that manages Prisma Access is running a supported PAN-OS version.

Use one of the following tasks to download and install the Cloud Services plugin.



HA Deployments Only—If you have two Panorama appliances configured in [High Availability \(HA\) mode](#), install the plugin on the Primary HA pair first, then the Secondary.

STEP 1 | Determine the [upgrade path](#) for the plugin to which you want to upgrade.

For some upgrade paths, you need to upgrade your plugin sequentially. For example, to upgrade from a 3.0 Preferred plugin to a 6.0 plugin, you must first perform interim upgrades to 3.1, 4.0, 4.1, 5.0, and 5.1 before upgrading to 6.0.

STEP 2 | Download and install the Cloud Services plugin versions you require.

- To download and install the Cloud Services plugin by downloading it from the Customer Support Portal, complete the following steps.
 1. Log in to the [Customer Support Portal](#) and select **Updates > Software Updates > Panorama Integration Plugin**.
 2. Find the Cloud Services plugin in the Panorama Integration Plug In section and **Download** it.



Do not rename the plugin file or you will not be able to install it on Panorama.

3. Log in to the Panorama Web Interface of the Panorama you licensed for use with the Prisma Access, select **Panorama > Plugins > Upload** and **Browse** for the plugin **File** that you downloaded from the CSP.
 4. **Install** the plugin.
- To download and install the new version of the Cloud Services plugin directly from Panorama, complete the following steps:
 1. Select **Panorama > Plugins** and click **Check Now** to display the latest Cloud Services plugin updates.

FILE NAME	VERSION
Name: cloud_services	
cloud_services-	

2. **Download** the plugin version you want to install.
3. After downloading the plugin, **Install** it.

STEP 3 | (Upgrades from Prisma Access 5.1 or earlier If you are upgrading from a Cloud Services plugin of 5.1 or earlier to 5.2 or later, go to **Panoraam > Admin Roles > <role-profile>**, **Disable** and then **Enable** the **Plugin** choice in the **Plugins** tab, and commit your changes to Panorama (**Commit > Commit to Panorama**).

After upgrading the Cloud Services plugin from 5.1 to 5.2 or later, the previously-configured Roles are not applied to the configuration, even though the configuration appears in the

Panorama UI. Without performing the Disable and Enable operation, you cannot view the Cloud Services tab in Panorama.

Admin Role Profile?

Name

AllAdmin

Description

Role

☒ Panorama

☐ Device Group and Template

Web UI

XMLAPI

Command Line

REST API

Plugins

✖ Plugins

Legend: ☒ Enable ☐ Read Only ☒ Disable

Context Switch

Device Admin Role

OK

Cancel

STEP 4 | Commit and Push your changes.

Getting Help

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none">• Prisma Access (Managed by Strata Cloud Manager)• Prisma Access (Managed by Panorama)	<ul style="list-style-type: none">❑ Prisma Access license❑ Minimum Required Prisma Access Version 6.0 Preferred and Innovation

The following topics provide information on where to find more about this release and how to request support:

- [Related Documentation](#)
- [Requesting Support](#)

Related Documentation

Use the following documents to set up and implement your Prisma Access deployment:

- Use the [Prisma Access Administrator's Guide](#) to plan, install, set up, and configure Prisma Access to secure your network.
- Use the vendor-specific tasks in the [Prisma Access Integration Guide](#) to use Prisma Access to configure mobile user authentication and secure your public cloud and third-party SD-WAN deployments.
- Use the [Strata Logging Service Getting Started Guide](#) to learn how to deploy Strata Logging Service (formerly Cortex Data Lake) and begin forwarding logs from your on-premise firewalls to Cortex Data Lake.

Visit <https://docs.paloaltonetworks.com> for more information on our products.

Requesting Support

For contacting support, for information on support programs, to manage your account or devices, or to open a support case, go to <https://support.paloaltonetworks.com>.

To provide feedback on the documentation, please write to us at: documentation@paloaltonetworks.com.

Contact Information

Corporate Headquarters:

Palo Alto Networks

3000 Tannery Way

Santa Clara, CA 95054

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

Palo Alto Networks, Inc.

www.paloaltonetworks.com

© 2024 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies.

