Prisma Access Release Notes (Panorama Managed)

Version 1.6.1

docs.paloaltonetworks.com

techDOCS paloalto NETWORKS

Contact Information

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

About the Documentation

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

Copyright

Last Revised

August 25, 2020

Table of Contents

Prisma Access (Panorama Managed) Release Information

Prisma Access simplifies the process of extending best-in-breed security to your remote network locations and your mobile workforce without having to build out your own global security infrastructure. You enable Prisma Access (Panorama Managed) using the Cloud Services plugin on Panorama.

In addition to this version of Prisma Access that you manage using Panorama, Palo Alto Networks offers another Prisma Access product, Prisma Access (Cloud Managed), that you manage using the Prisma Access app on the hub. This product has its own release notes.

Prisma Access—A cloud-based security infrastructure service that is designed to minimize the operational challenges associated with protecting your remote network locations and mobile users. With this service, Palo Alto Networks deploys and operates the security infrastructure you need globally, so that you can push consistent next-generation security out to your remote locations and users. Prisma Access supports the following capabilities:

- **Prisma Access for Networks**—You can deploy the service to secure your remote network locations.
- **Prisma Access for Users**—You can deploy Prisma Access to protect your mobile users with consistent next-generation security policies.
- **Service Connections**—You can connect the Prisma Access to up to 100 of your HQ or data center locations to enable users to access resources at your corporate sites and/or to enable access to your on-premise authentication service.
- **Prisma Access for Clean Pipe**—The Prisma Access for Clean Pipe service allows organizations that manage the IT infrastructure of other organizations, such as service providers, managed security service providers (MSSPs), or Telcos, to quickly and easily protect outbound internet traffic for their tenants.

Before you begin, make sure you review the following information:

Features Introduced in Prisma Access

The following table describes the new features introduced in Prisma Access version 1.6.1.

You do not need to upgrade your Panorama or the Cloud Services plugin from 1.6.0 to take advantage of the 1.6.1 release; Prisma Access upgrades its infrastructure to add the activation improvements automatically. See Features Introduced in Prisma Access 1.6.0 for information about the 1.6.0 Cloud Services plugin.

Feature	Description
Prisma Access Insights	Continuously monitor the health and performance of your Prisma Access environment with the new Insights app. Visually scan and interact with a variety of Insights dashboards to get status on your mobile users, remote network sites, service connections to your HQ and data centers, and the Prisma Access cloud infrastructure. When Insights detects an issue in your environment, the app generates an alert that gives you context and lets you know where to take action. Insights alerts also give you visibility into fixes that the Prisma Access team is addressing. Insights is available to you as part of a **public beta** for all Prisma Access users. To get started: **1.** Learn about Insights, including the role you might need to access the app. **2.** Launch the Insights app from the hub. **3.** Turn on email notifications for Insights alerts.
Simplified License Activation	If you are new to Prisma Access and activating your product for the first time, or adding a different license type to an existing license, the improved process steers you through the activation flow so you can quickly get started with using Prisma Access to secure your network and users. It doesn't matter if you plan to use Panorama or Cloud Management, the activation process is just as speedy. The license activation email enables you to view and activate all your Prisma Access purchases and tie them to a Customer Support account in one streamlined flow on the Hub.

Features Introduced in Previous Prisma Access (Panorama Managed) Releases

Review the list of features released in cloud services plugin 1.1.0 and later for Prisma Access (Panorama Managed); check here to read about the features introduced in the latest release.

- Features Introduced in Prisma Access 1.6.0
- Features Introduced in Prisma Access 1.5.1
- Features Introduced in Prisma Access 1.5.0
- Features Introduced in Prisma Access 1.4.0
- Features Introduced in Prisma Access 1.3.1
- Features Introduced in Prisma Access 1.3.0

Features Introduced in Prisma Access 1.6.0

Prisma Access does not support versions of the Cloud Services plugin earlier than 1.6, and you must upgrade to this version.

The following table describes the new features introduced in Prisma Access version 1.6.0.

Feature	Description
DNS Enhancements for Mobile Users	If you specify the same DNS server to resolve both internal and external domains, Prisma Access does not proxy the DNS request, and you can view the actual source IP address of the client that sent the DNS request. This enhancement allows you to enforce source IP address-based DNS policies or identify endpoints that communicate with malicious domains using the source IP of the DNS requests.
DNS Additions for Remote Networks	You can use Prisma Access to specify DNS servers to resolve both internal and public domains. If you specify an internal DNS server to resolve internal DNS domains and then specify either a public server or Prisma Access' Cloud Default server to resolve external domains, Prisma Access proxies the requests from the remote network site. You can also specify an external DNS server that is closer to the egress points of your remote network sites than your internal DNS server, which can provide optimal connectivity for SaaS applications such as Microsoft Office 365.
Clean Pipe Intra-zone Connection Redundancy	Prisma Access allows you to configure two VLAN attachments for a single Clean Pipe location in an active/backup configuration for intra-zone redundancy—an enhancement to the current implementation, where you can specify two different VLAN attachments in different availability zones (inter-zone redundancy).
QoS for Clean Pipe	For Clean Pipe deployments, you can create QoS policies to define the traffic that receives QoS treatment and QoS profiles to define the classes of service, including priority, that the traffic can receive. You can define QoS based on DSCP values or zones (Trust or Untrust).
Secure Inbound Access Support for Remote Networks	If you are hosting an internet-facing application or service in your remote network location, you can use Prisma Access to front-end that application or service and provide secure access from both internal and external users over the internet.
200 Tenant Support for Multitenancy	The Cloud Services Plugin increases multitenant support from 100 to 200 Prisma Access tenants. This gives Service Providers and large enterprises the capability to expand how they deploy and support disparate, segregated environments. For concurrent Panorama administrator login maximums, see the Prisma Access Administrator's Guide (Panorama Managed).
Support for Individual BGP Peers on Primary and	To facilitate dynamic IPSec tunnel failover for BGP deployments if the on-premises devices do not use the same IP addresses for BGP peering, you can specify different BGP peer and local IP addresses for the primary and

Feature	Description
Secondary IPSec Tunnels	secondary (active and backup) IPSec tunnels for service connections and remote network connections.
DLP on Prisma Access	This release adds support for Data Loss Prevention (DLP) on Prisma Access. DLP on Prisma Access uses predefined patterns, built-in settings, and options that make it easy for you to protect files that contain certain file properties (such as a document title or author), credit card numbers, regulated information from different countries (like social security numbers), and third-party DLP labels. *DLP is an add-on license on Prisma Access. You can either start with a 60-day trial or purchase a license to use Enterprise DLP on Prisma Access.* DLP on Prisma Access includes the following elements: • You can Block files that match data patterns as well as create Alert notifications. • DLP on Prisma Access supports the use of *snippets* and *data masking*. If a pattern in a security policy matches an alert or block notification, Prisma Access extracts a snippet of the sensitive data that matched. Prisma Access uses data masking to partially mask the snippets to prevent the sensitive data from being exposed. You can configure DLP on Prisma Access to completely mask the sensitive information, unmask the snippets, or disable snippet extraction and viewing.
Directory Sync Integration with Prisma Access	Prisma Access for Users and Prisma Access for Networks can leverage Palo Alto Networks' Directory Sync service to retrieve user and group information for policy enforcement.
ECMP load balancing for Lower-Bandwidth Remote Network Connections	You can configure ECMP Load Balancing for remote networks with a bandwidth of 50, 100, or 150 Mbps, as well as 300 Mbps, allowing lower-bandwidth connections to increase their fault tolerance by adding up to four IPSec tunnels for a single remote network.
Sinkhole Mobile User IPv6 Traffic	Prisma Access extends the protection of mobile user traffic from IPv4/IPv6 dual-stacked endpoints with a new CLI command that enables you to sinkhole IPv6 mobile user traffic. Because endpoints can automatically fall back to an IPv4 address, you can enable a secure and uninterrupted user experience for mobile user traffic to the internet.

Features Introduced in Prisma Access 1.5.1

The following table describes the new features introduced in Prisma Access version 1.5.1.

Feature	Description
New Prisma Access location and compute location	As part of continuous improvement to the Prisma Access service, a new location and new compute region, Bahrain, has been added. This new location displays automatically as a choice in the Prisma Access GUI.

Feature	Description
New compute locations for Belgium and Switzerland	Prisma Access has added new compute locations for the following locations: • **Belgium**—Moved from Netherlands to Belgium compute location • **Switzerland**—Moved from Germany to Switzerland compute location There is no change to existing deployments. If you have already onboarded Belgium and Switzerland, they use the existing compute locations. To use the new compute locations with an existing deployment, delete the existing location, perform a commit operation, then re-add the location.

Features Introduced in Prisma Access 1.5.0

The following table describes the new features introduced in Prisma Access version 1.5.0.

Feature	Description
PAN-OS 9.0 feature support	This release offers support for PAN-OS 9.0, which includes the following new features and enhancements: • DNS security • Inspection of HTTP/2 traffic • Improved URL filtering • Built-in External Dynamic List (EDL) for bulletproof ISPs • Portal Configuration Assignment and HIP-Based Access Control Using New Endpoint Attributes • Wildcard address support in security policy rules • Mixed Authentication Method Support for Certificates or User Credentials Note that the following 9.0 features are not supported: • Policy Optimizer • FQDN Support for Static Route Next Hop, PBF Next Hop, and BGP Peer
Route preferences and preferred backup for service connections	In addition to Prisma Access' default routing for service connections, Prisma Access allows a new choice, *Hot potato routing*, which changes the way routes are imported and advertised to and from Prisma Access so that traffic destined to service connections (for example, HQ or data center traffic) exits the Prisma Access network as quickly as possible. In addition, to help ensure routing symmetry in the event of a link failure, you can choose a preferred service connection to use as a backup if a link to a service connection fails (Backup SC).
ECMP load balancing for remote network connections	To provide additional network resiliency using redundant instances of your customer premises equipment (CPE), Prisma Access allows you to add up to four IPSec tunnels for a single remote network.
BGP default route support for remote network connections	Prisma Access can advertise a default route for remote network connections using BGP; you can then use this route in your organization's network to direct traffic to Prisma Access.

Feature	Description
API command enhancements	Prisma Access adds improvements to the commands you use to retrieve the public IP addresses (the source IP addresses that Prisma Access uses for requests to an internet-based source). The API command has the following enhancements for mobile user deployments: • The API command lists the locations associated with the reserved IP addresses. • You can easily retrieve both the active IP addresses for each location and the reserved IP addresses for those locations that are used for scaling events. You can request the active addresses, the reserved addresses, or all sets of addresses.
Custom URL Category enhancements	You can specify up to 2,000 wild card (*.example.com) URLs (including those specified in custom URL categories), an increase from 500, when you use traffic forwarding rules with service connections.
Redistribute HIP information	To ensure consistent Host Information Profile (HIP) policy enforcement and to simplify policy management, you can redistribute HIP information received from mobile users and users at remote networks that use the GlobalProtect app from Prisma Access to other gateways, firewalls, and Panorama appliances in your enterprise, including the Panorama that manages Prisma Access.
View HIP report from Panorama	After you configure Prisma Access to redistribute HIP information to Panorama, you can then view the HIP report from Panorama.

Features Introduced in Prisma Access 1.4.0

The following table describes the new features introduced in Prisma Access with Cloud Services plugin version 1.4.0.

Feature	Description
Increased Location Support for Mobile Users, Remote Networks, and Service Connections	To better accommodate worldwide deployments and provide best-of-breed local coverage, you can now choose from more than 100 locations in 76 countries when you onboard your mobile users, remote network connections, and service connections. Be aware of the following changes and requirements as a result of the added locations: • When you first install the plugin, log out and then log back in to Panorama to see the new locations. • For existing customers, Prisma Access retains all existing locations in addition to adding support for the new locations; however, existing location names have changed. In addition, if you allow your mobile users to manually select gateways

Feature	Description
	from the GlobalProtect app, the gateway names that mobile users see from the app have changed. See Changes to Default Behavior for details. • For mobile user deployments, if you currently add Prisma Access public IP addresses to an allow list, you must allow the addresses that Prisma Access assigns for any new locations that you add. To ensure that mobile users do not lose access to SaaS or public applications after you add more locations, Prisma Access pre-reserves unique addresses for each location, and you can run an API script and add the pre-reserved addresses to an allow list before you add new mobile user locations. See Changes to Default Behavior for more information. • For mobile user deployments, there is a minimum number of IP addresses that are required for each region where you deploy the locations. When you configure mobile user deployments in Panorama, the UI validates the minimum IP address pool and prompts you if changes are required. This validation is not available if you configure locations using CLI. If you deploy all locations using CLI, we recommend that you add a /18 address in the Worldwide pool for mobile users.
Custom Local IP Address for BGP	For service connections or remote network connections that use BGP, you can specify a custom local IP address that Prisma Access uses as its local IP address for BGP. This custom address is useful when the device on the other side of the connection (such as an Amazon Web Service (AWS) Virtual Private Gateway) requires a specific local IP address for BGP peering.
Automatic Creation of Template Stack, Templates, and Device Groups for Multi-Tenant Deployments	To speed up the process of configuring additional tenants in a multi-tenant deployment, Prisma Access automatically creates templates, template stacks, and device groups for each tenant you create after the first one, instead of requiring you to manually create these components for each tenant. When you enable multi-tenancy, existing templates, template stacks, and device groups still migrate over to the first tenant. For each subsequent tenant you add, Prisma Access creates the templates, template stacks, and device groups and adds them to the access domain you create.

Feature	Description
Administratively Logout Mobile Users from Panorama	To immediately remove mobile users from access to your organizations' resources, you can log out active mobile users from the Cloud Services plugin in Panorama.
HTTP/HTTPS Traffic Forwarding to Service Connections	Prisma Access can redirect HTTP or HTTPS internet traffic from mobile users and remote networks, and forward and route that traffic over a service connection. With this capability, you can for example, steer traffic through a third-party security stack (service chain) before egressing to the internet. Another use case is to redirect certain websites' traffic to be routed through the organization's on-premise network.
Clean Pipe Service for Multi-Tenant Deployments	To allow organizations that manage the IT infrastructure of other organizations, such as service providers or telecommunications providers (Telcos), to quickly and easily protect outbound internet traffic for their tenants, Palo Alto Networks introduces the Clean Pipe service with this release. A service provider or Telco will be able to route their customers (configured as tenants) to the Clean Pipe service using a Partner Interconnect. After the traffic crosses the Partner Interconnect, it will be sent to a tenant-dedicated instance of Clean Pipe for security, and then routed to the internet. An API that allows you to quickly and easily onboard tenants is also available. To use the Clean Pipe service, you must purchase a Clean Pipe license and deploy Prisma Access in multi-tenant mode. After you purchase and activate this license, a new Clean Pipe tab is activated in the Cloud Services plugin. See Changes to Default Behavior for details.

Features Introduced in Prisma Access 1.3.1

The following table describes the new features introduced in the Cloud Services plugin version 1.3.1.

This release has changes to default behavior for mobile users regional IP pools when you upgrade that might affect your deployment. See Changes to Default Behavior for a list of the changes.

Feature	Description
Region Selection	When you onboard mobile users, this release includes the ability to specify one or more locations in a region in order to exclude deployment in all regions. This

Feature	Description
	feature provide more granular control over deployed regions and allows you to exclude regions as required by your policy or industry regulations. You select the locations in the region from locations on a map during the onboarding process. *This release changes the method of onboarding mobile users, because you now must select one or more locations. See Changes to Default Behavior for details.*
Reduced IP Address Pool Requirement for Mobile Users	You can now specify a minimum IP address pool of a /23 subnet (512 addresses) for a single region when you onboard mobile users. The lowered IP pool requirement is useful in proof of concept or evaluation situations when you don't have a large available block of private IP addresses. After you onboard a single region, you can then onboard additional regions in stages and add more IP address pools for those regions.
Pre-defined IPSec Tunnel Configurations	Prisma Access includes pre-defined IPSec tunnel profiles for some common third-party IPSec and SD-WAN devices. These profiles expedite and simplify the onboarding of service connections and remote network connections that use one of these devices to terminate the connection.
Clientless VPN Portal	This Prisma Access release supports Clientless VPN.
Clientless VPN Reverse Proxy for SaaS Security	Prisma Access allows you to control unsanctioned and employee-owned device access to your network and redirect device traffic to Prisma Access for inspection without putting your network or data at risk. Unsanctioned device access control utilizes SAML redirection by proxy instead of directly exposing the SaaS app on your network, removing all possible vulnerabilities to data exfiltration and malware propagation.
New location *Paris* Available for Mobile Users, Remote Networks, and Service Connections	An additional location, Europe (Paris), is added to the list of available locations. *Existing deployments with all gateways specified do not have this region added automatically; to add it, select Panorama > Cloud Services > Configuration > Mobile Users > Configure > Locations and select the Paris location in the map that displays.*

Feature	Description
Additional Bandwidth Choices for Remote Networks	To better accommodate larger networks, additional remote network bandwidth choices of 500 Mbps or 1000 Mbps (1000 Mbps) is added. All existing remote network bandwidth choices are retained. *This feature is being deployed in Preview Mode for 1.3.1. We will deliver up to 500 Mbps or 1000 Mbps of throughput on a best-effort basis during the preview. The actual performance will vary depending upon the traffic mix.*
Support for Overlapping Subnet - Internet Outbound	You can deploy remote network locations with overlapping subnets in the same region (for example, for a guest network at a retail store) for internet outbound only. Prior to this release, you had to specify separate regions for any remote networks that have overlapping subnets. *Configuring remote networks with overlapping subnets changes the behavior of the remote network; see Remote Network Locations with Overlapping Subnets in the Prisma Access Administrator's Guide for details. Other remote networks in your deployment without overlapping subnets are not affected.*

Features Introduced in Prisma Access 1.3.0

The following table describes the new features introduced in the Cloud Services plugin version 1.3.0. For additional information on how to use the new features in this release, refer to the Prisma Access Administrator's Guide (Panorama Managed).

Upgrading to 1.3 causes changes to device groups.

Feature	Description
Quality of Service (QoS) Support	You can now enable QoS in Prisma Access to mark and shape QoS traffic. Prisma Access delivers the same QoS marking and shaping features available today in Palo Alto Networks next-generation firewalls. • You can create PAN-OS security policies to mark traffic destined to Prisma Access for mobile users and for remote network connections. For service connections, Prisma Access honors

Feature	Description
	traffic marking from your on-premise devices. In addition, you can optionally use on-premise devices to mark traffic for remote networks. • You can create QoS profiles to shape QoS traffic for service connections and for remote network connections and apply those profiles to traffic that you marked with PAN-OS security policies, traffic that you marked with an on-premise device, or both PAN-OS-marked and on-premise-marked traffic.
Support for Additional Service Connections	You can now configure up to 100 service connections in Prisma Access. Previously, a maximum of three service connections were allowed and you had to use remote network connections for additional connections to an HQ or data center site, which limited throughput to the configured bandwidth of the remote connection. You can configure up to three service connections with no license cost; however, each additional connection uses 300 Mbps of the remote network bandwidth allocation from your Prisma Access license. *The license cost for additional service connections does not change their functionality. Prisma Access does not limit the bandwidth over service connections, and additional service connections work the same as other service connections.*
Additional Bandwidth Choices for Remote Networks	In addition to the existing remote network bandwidth choices of 2 Mbps, 5 Mbps, 10 Mbps, 25 Mbps, 50 Mbps, 100 Mbps, or 300 Mbps, you can now select 20 or 150 Mbps, to better match commonly-used ISP speeds.
Expanded Visibility for Mobile Users	You now have expanded visibility for mobile users, including their client OS, their last login time, and their public IP addresses. You can view a list of currently logged in users or view historical information of previously-logged in users for a 90-day time period. To view User ID information, select Panorama > Cloud Services > Status > Status; then click either Current Users or Users (Last 90 days) in the Mobile Users area.
Multiple Prisma Access Instances On a Single Panorama Appliance (Multi-Tenancy)	You can now host and manage multiple instances of Prisma Access (known as *tenants*) on a single

Feature	Description
	Panorama appliance. With multi-tenancy, each single Panorama appliance supports up to 100 tenants, each with their own templates and template stacks, device groups, and access domains. This enables you to create tenant-level administrative users who can view and edit the configuration for a single tenant. You allocate remote network and mobile user license resources for each tenant based on the license that is associated with the Cloud Services plugin in Panorama. The minimum license allocation for each tenant is 500 Mbps for remote networks and 500 mobile users. You can also configure a tenant with only remote networks (minimum 500 Mbps) or mobile users (minimum 500 mobile users).  *Since this feature is supported starting with PAN-OS version 8.1.6, you must use the Cloud Services plugin with a Panorama appliance running a minimum version of 8.1.6.*
GlobalProtect App Generate Ticket Option	Panorama now allows GlobalProtect administrators and Help Desk support personnel to generate a ticket that end users must supply to disable the GlobalProtect app for Windows or for Mac.  *Since this enhancement is supported starting with PAN-OS version 8.1.6, you must use the Cloud Services plugin with a Panorama appliance running a minimum version of 8.1.6.*
Persistent Public IP Addresses for Mobile User Gateways	This feature is applicable if you are adding Prisma Access public IP addresses to an allow list in your network to control access for SaaS or public applications. With this release, Prisma Access now assigns two new sets of public IP addresses for mobile user gateways: • One set that is assigned to gateways that are currently active. • Another set to reserve in case of a scaling event, infrastructure upgrade, or other event that causes an IP address change for mobile users. These new IP addresses will persist across future upgrades. Prisma Access provides each customer with their own unique set of IP addresses. While the currently

Feature	Description

	assigned IP address will change after you upgrade, this change does not affect mobile users' ability to connect to Prisma Access.
	
	  *Public IP addresses for remote networks will not change after you upgrade, and you do not have to reconfigure your IPSec tunnels.*
	
	You can retrieve these new addresses by retrieving your API key and entering a curl command in the following format:
	
	`curl -k -H header-api-key:Current-API-Key "https://api.gpcloudservice.com/getAddrList/latest?get_egress_ip_all=yes"`
	
	Where *Current-API-Key* is the Prisma Access API key.
	
	For example, given an API key of **123abc**, use the following curl command to retrieve the public IP address:
	
	`curl -k -H header-api-key:123abc "https://api.gpcloudservice.com/getAddrList/latest?get_egress_ip_all=yes"`
	
	If you have a large number of mobile users from a single region, the reserved IP addresses might be insufficient to scale; in this case, Prisma Access adds more public IP addresses to the allocated IP sets and you will have to retrieve those new IP addresses to add to your allow lists. These extra sets of IP addresses also persist after an upgrade. Continue to use the curl command to get notified when additional sets of IPs are added to the reserved pool.

PAN-OS 8.1 Support	The Prisma Access infrastructure is upgraded to PAN-OS version 8.1. You can now implement PAN-OS 8.1 features in Prisma Access, including but not limited to the following features:
	
	• **Security Features:**
	  • SaaS Application Hosting Characteristics
	  • Simplified App-ID
	  • HTTP Header Insertion and Modification
	  • Service-Based Session Timeouts
	  • Automatic SAN Support for SSL Decryption
	  • WildFire Script Sample Analysis

Feature	Description

	• **Management Features:**
	  • Rule Usage Tracking (also known as Policy Rule Usage Tracking)
	  • Configuration Table Export
	  • Reporting Engine Enhancements
	  • Enhanced Application Logging
	• **Mobile Features:**
	  • Optimized Split Tunneling for GlobalProtect
	  • Extensible Authentication Protocol (EAP) Support for RADIUS
	  • Support for Multiple Username Formats
	  *Upgrading the infrastructure to 8.1 causes changes to default behavior; for more information, see the following documentation:*
	  • Changes to Default Behavior *for PAN-OS and GlobalProtect 8.1*
	  • Changes to Default Behavior *for the User-ID Agent*
	  In particular, please note that previously, the firewall normalized usernames received from User-ID sources (such as an LDAP directory) to the domain \username format. In PAN-OS 8.1, when the Primary Username is in UPN format, it will not be normalized as in previous PAN-OS versions. As a result, usernames are displayed in their original format (for example, username@domain).

Features Introduced in Prisma Access 1.2.0

The following table describes the new features introduced in the Cloud Services plugin version 1.2.0. For additional information on how to use the new features in this release, refer to the Prisma Access Administrator's Guide.

Feature	Description
Gateway Selection Improvements	To allow mobile users to use the best gateway for your organization, the following gateway improvements have been implemented:

Feature	Description
	• Mobile users now automatically connect more reliably to a Prisma Access gateway that is inside the country from which they are connecting. • Mobile users can manually select a gateway (either a gateway in Prisma Access or an on-premise gateway) using the GlobalProtect app on their endpoint. See Manage Priorities for Prisma Access and On-Premise Gateways for more information.
Status Monitor Improvements	The following improvements have been made in the Panorama > Cloud Services > Status area: • To better show network status, the fields in the Panorama > Cloud Services > Status > Monitor window are changed. Click the Service Connection, Remote Networks, or Mobile Users radio button and hover over any of the circled locations on the map to get a detailed view of the number of service connections, remote network tunnels, or remote users that are configured and their status. In addition, the Logging Service radio button shows the current data retention settings and log quotas for Infrastructure and Audit Logs, Detailed Logs, and Summary Logs. • The Panorama > Cloud Services > Status > Network Details area has been divided into four areas with radio buttons that allow you to see the network details divided by Service Infrastructure, Service Connection, Remote Networks, and Mobile Users.
Internal DNS domains for mobile users increased to 1,024	Prisma Access can now support up to 1,024 internal domains.
FQDNs of all Prisma Access gateways now available	You can now view the full FQDNs of all gateways that are available in Prisma Access. To view the FQDNs, select Panorama > Cloud Services > Status > Network Details and click the Mobile Users radio button. The FQDNs display in the Gateways area. *These gateways replace the primary and secondary gateways.*
paloalto-shared-services App-ID released	To make sure that Panorama can communicate with Prisma Access and Cortex Data Lake, configure internet gateway firewall security policies to allow the App-ID paloalto-shared-services, in addition to the App-ID paloalto-logging-service. The App-ID paloalto-shared-services is released as part of content version 8067, and you can review the Customer Resources article Palo Alto Shared Services App-ID

Feature	Description
	for more information. Before the release of this App-ID, administrators needed to add a security policy that contained the paloalto-logging-service App-ID, SSL, and web-browsing on the internet gateway firewall to allow communication between the services, which was less secure than using the new App-ID.

Features Introduced in Prisma Access 1.1.0

The following table describes the new features introduced in the Cloud Services plugin version 1.1.0.

Feature	Description
Dynamic Routing Support	For a multi-site environment, support for the dynamic routing protocol—BGP— makes it easier for you to onboard your remote network locations and service connections without manually configuring static routes. When you configure your on-premises BGP routers to broadcast information on subnets in remote networks or at headquarters, Prisma Access learns these routes and enables communication between the headquarters and the remote network locations or between remote network locations.
Redundancy Across Service Connection and Remote Networks	For a better user experience, the Prisma Access now supports redundant routes directing traffic from your mobile users and remote network locations to your headquarters or data center over a service connection. This enhancement is available for BGP and static route configurations. If, for example, you have set up three service connections and a service connection tunnel is down, mobile user and remote network traffic is automatically routed over the other two operational service connections or remote network tunnels.
Smaller Bandwidth Allocation	Support for 2 Mbps and 5 Mbps of bandwidth is now available for your remote network locations with lower bandwidth requirements. From the total bandwidth pool you purchase, you can divide the available bandwidth across each remote network location that you onboard in increments of 2 Mbps, 5Mbps, 10 Mbps, 25 Mbps, 50 Mbps, 100 Mbps, or 300 Mbps.
Egress IP Address List for Prisma Access Infrastructure	If you have configured IP address allow lists to manage access to SaaS applications such as O365 or to applications that you host on the public cloud, changes to the IP addresses in your Prisma Access infrastructure can pose a challenge. As Prisma Access dynamically deploys firewalls to meet the requirements of your network and mobile users, you can now subscribe to a notification URL to learn about IP

Feature	Description
	address changes in your Prisma Access infrastructure. You then can use a script or manually retrieve the list of IP addresses for all firewalls in your Prisma Access infrastructure, or just GlobalProtect gateways, GlobalProtect portals, or remote network firewalls and adjust your policies with IP-based restrictions to safely enable access for all SaaS or cloud applications.

Changes to Default Behavior

The following chapter details the changes in default behavior after you upgrade from the Cloud Services plugin version 1.5.*x* to version 1.6. For the system requirements you need before you upgrade, see Upgrade the Cloud Services Plugin.

Because you do not need to upgrade your Panorama or the Cloud Services plugin from 1.6.0 to take advantage of the 1.6.1 release (Prisma Access upgrades its infrastructure automatically), these changes also apply to Prisma Access 1.6.1.

Component	Change
ECMP load balancing for remote networks	If you enable ECMP load balancing to use up to four IPSec tunnels with a single remote network, Prisma Access uses the same link for return traffic as it uses to send the traffic (Enabled with Symmetric Return). After you upgrade the plugin to 1.6, if your deployment has the setting of Enabled, you will be prompted to change it to Enabled with Symmetric Return. If you do not change this setting, you will receive an error when you perform a local commit until you change it. If you already have Enabled with Symmetric Return specified for ECMP, or if you have not enabled ECMP, no action is required.
Hot potato routing AS-PATH prepending changes	When you enable Hot Potato Routing for service connections, the following AS-PATH prepending changes are made. The changes for secondary BGP peers are new for 1.6, and some additional changes are made for primary connections: • The service connection does not prepend its AS-PATH to prefixes on a gateway that is directly connected to the service connection. If you specify a secondary BGP peer, the service connection prepends the AS-PATH for the secondary connection once. • The service connection prepends the AS-PATH three times to prefixes on gateways connected directly to its backup service connection (a change from twice). If you specify a secondary BGP peer, the service connection prepends the AS-PATH for the secondary connection four times. • The service connection prepends the AS-PATH six times to prefixes on gateways that are connected to other service connections (a change from four times). If you specify a secondary BGP peer, the service connection prepends the AS-PATH for the secondary connection seven times.
Addition of __cloud_services Panorama Administrative User	After you install the Cloud Services plugin 1.6, the plugin creates a Panorama administrative user with a username of **__cloud_services**. This user account is required to enable communication between Enterprise DLP on Prisma Access and the Prisma Access management infrastructure. Palo Alto Networks recommends that you change the password for this administrative user in accordance with your organization's password policy. If you have deleted the **__cloud_services** user, you must re-add the user manually. The account is used to register and activate Enterprise DLP on Prisma Access, and for continued DLP scanning using the data patterns and data filtering profiles referenced in security policy rules.

Upgrade the Cloud Services Plugin

After reviewing the Prisma Access Known Issues, use the following procedure to upgrade the Cloud Services plugin. Prisma Access does not support versions of the Cloud Services plugin earlier than 1.6, and you must upgrade to this version. After upgrading to cloud services plugin version 1.6, you cannot downgrade to an earlier version.

Prisma Access does not support FIPS-CC mode.

If this is the first time you are installing the plugin, refer to License and Install the Prisma Access Components for instructions.

You can manage Prisma Access with a Panorama appliance running one of the following versions:

- PAN-OS 9.0.4 or a later PAN-OS 9.0 version
- PAN-OS 9.1.1 or a later PAN-OS 9.1 version
- PAN-OS 10.0.0 or a later PAN-OS 10.0 version

Note the upgrade path to use if you are upgrading from PAN-OS 9.0 to 10.0.

While using Panorama 9.1 is supported with Prisma Access, upgrading to Panorama 9.1 does not give you access to 9.1 features in Prisma Access. The Prisma Access infrastructure supports PAN-OS features up to release 9.0.

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

Before you upgrade the plugin, remove any non-Prisma Access templates from Prisma Access template stacks to avoid commit validation errors after upgrade.

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

If you are currently running the Cloud Services plugin 1.4, you can upgrade directly to the 1.6 plugin without an interim upgrade to the Cloud Services plugin 1.5.

- **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 Software Updates,
  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	Release Date	Size
Name: cloud_services			
[redacted]	[redacted]	[redacted]	966K
cloud_services-1.6.0	1.6.0	2020/04/20	4M

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

Prisma Access Known Issues

Prisma Access has the following known issues.

Issue ID	Description
CYR-11752 This issue is now resolved in plugin version 1.6.0-h1. See Prisma Access 1.6.0-h1 Addressed Issues.	When using a Panorama running PAN-OS 9.1 in multi-tenant mode and log in as a tenant-level user, you cannot add remote networks or configure mobile users. **Workaround:** Log in as the admin user and perform the remote network or mobile user configuration.
CYR-11532	If you use traffic forwarding rules with service connections and you have a traffic rule configured with the Source as a specific region and the URL includes a wild card, and the source address of the traffic does not match the rule, the URL specified in the rule cannot be reached. **Workaround:** Configure the source address in the traffic rule as Any.
CYR-11504	If you have configured a remote network for secure inbound access to a remote network site, do not configure a service connection to redirect mobile user and remote network internet traffic using policy-based forwarding (PBF) traffic forwarding rules; these two functionalities are not compatible.
CYR-11467	When you check the Cortex Data Lake Status at Panorama > Cloud Services > Status > Status > Cortex Data Lake, the statistics displayed there might not display accurate storage and retention information. **Workaround:** Go to the hub and select **Cortex Data Lake** to see the most up-to-date information.
CYR-11496	If you enable ECMP on a remote network, the values shown in the Statistics tab under Panorama > Cloud Services > Status > Monitor > Remote Networks for Ingress Peak Bandwidth (Mbps) are correct; however, if you click the hyperlink for this value, the pop-up window that displays might show an incorrect value.
CYR-11414	When creating a new mobile user deployment in multi-tenant mode, you receive an error that the Portal Hostname is not available when you assign it during mobile user onboarding. **Workaround:** Before you begin your mobile user configuration, add an Infrastructure Subnet, commit all your changes to Panorama, and push the configuration changes to Prisma Access.
CYR-11201	Some files are being skipped for DLP scanning when using OneDrive to upload multiple files.
CYR-11087	When using DLP on Prisma Access, you can upload up to 25 files at a time.

Issue ID	Description
CYR-11019	When attaching a parent Device Group to a new remote network tenant in multi-tenant mode, the administrator is unable to attach device groups and templates. **Workaround:** Log out, then log back in to Panorama.
CYR-10909	If you use Box to upload multiple files, and one or more of the files are larger than 5 MB, the upload of all files will not complete. To continue, find the files in Box that are larger than 5 MB and click X to stop the download of those files.
CYR-10789	Traffic statistics for remote networks might exceed the configured bandwidth; for example, a remote network configured for 300 Mbps might show an ingress or egress peak bandwidth that is higher than 300 Mbps. **Workaround:** No workaround is required. Because Prisma Access measures the peak bandwidth values using a short time interval, the peak bandwidth might occasionally exceed the configured remote network values.
CYR-10623	When you check the status in a multi-tenant deployment by selecting Panorama > Cloud Services > Status, the information in the All Tenants area displays twice.
CYR-10445	DLP on Prisma Access is not supported in a Prisma Access multi-tenant deployment.
CYR-10387	If you have DLP on Prisma Access enabled for more than one Prisma Access instance in a single Customer Support Portal (CSP) account, data filtering profiles are synchronized across all instances. This behavior can result in unexpected consequences; for example, the deletion of a custom data pattern or data filtering profile for one instance does not delete that pattern or profile for other instances in the CSP account. For this reason, Palo Alto Networks recommends that you move each Prisma Access instance to its own CSP account.
CYR-10053	If you change the master key in Panorama (in Device > Master Key and Diagnostics), the master key for Cloud Services is not synchronized with this master key. **Workaround:** Select Panorama > Cloud Services > Configuration > Service Setup > Service Operations > Edit Master Key and manually change the master key to be the same as the Panorama master key.
CYR-10044	When using Slack to upload multiple files, the Slack client treats the multiple file upload as a single request. If one of the files is not successfully uploaded, Slack retries the upload of all files a maximum of three times. If, after three retries, Slack cannot upload one or more of the files, the Slack client displays an error in the UI and doesn't upload any of the files.
CYR-10043	When you upload a file using Slack, and the file is blocked, Slack detects the block operation as an upload failure and retries the file upload, which results in the same file being uploaded and blocked twice.

Issue ID	Description
	Workaround: This is normal Slack file upload behavior. Be aware that a single file that is uploaded using Slack might appear twice in the data filtering logs as being blocked.
CYR-9613	When you delete a data filtering profile from a Prisma Access device group that is not shared, the profile name still appears when you add or configure a Security Profile Group, in the Data Filtering Profile area.
CYR-9502 This issue is now resolved in plugin version 1.5.1. See Prisma Access 1.5.1 Addressed Issues.	When the bandwidth for a remote network was changed, a new Service IP Address was created for the remote network, instead of retaining its existing Service IP Address. This behavior has been observed in the US West, South Korea, Ireland, and France North locations. **Workaround:** After you change the bandwidth of a remote network connection, run the API script to retrieve the new Service IP Address.
CYR-9455	In a GlobalProtect deployment where the portal has multiple agent configs, when a GlobalProtect client logs in using the app, the portal looks for a matching agent config for the client by checking its OS type along with the config selection criteria. The agent configs are checked from top to bottom. If the OS type matches, but the config selection criteria does not, GlobalProtect marks the agent config as non-matching and moves to the next agent config to check for a match; however it no longer checks the OS type in these agent configs, and only looks for a match of the config selection criteria. This condition can cause the client to receive an agent config that has matching config selection criteria, but a non-matching OS type.
CYR-9348	When configuring HIP redistribution, you cannot retrieve HIP information and set policies for the following use cases: • A user connected to a Prisma Access location (gateway) who attempts to access an internal resource. • A user protected by a remote network who attempts to access a resource from another remote network.
CYR-9213	When using DLP on Prisma Access, when you upload a .docx file using SharePoint that was exported from Google Docs, the upload fails.
CYR-9183	When setting up the GlobalProtect gateway connection settings (Network > GlobalProtect > Gateways > Agent > Connection Settings) and specifying a Netmask to Restrict Authentication Cookie Usage, the commit fails if only a Source IPv4 Netmask is specified. **Workaround:** Specify a Source IPv6 Netmask of 0, which disables the option for the specified IP address type.
CYR-9079 This issue is now resolved in plugin version 1.6.0. See Prisma Access 1.6.0 Addressed Issues.	Certificate profiles do not display in the HIP Objects' certificate profile (Objects > GlobalProtect > HIP Objects > <*hip-object-name*> > Certificate > Certificate Profile) if the HIP object is Shared (that is, not under a specific device group).

Issue ID	Description
CYR-9061	If using Slack, Box, or Gmail to upload a file using DLP on Prisma Access, the response page is not displayed to the client if the upload is blocked.
CYR-9007	When you upload multiple files, and one file exceeds the maximum latency or maximum file setting, any remaining files in the upload queue will not be scanned. **Workaround:** Re-attempt the multiple file upload operation without the file that exceeded the maximum file size or latency setting.
CYR-9003	Reverse DNS queries do not work in Prisma Access. **Workaround:** Because type A and AAAA queries for internal domains work, you can specify **`*.in-addr.arpa`** in a query so that Prisma Access sends all reverse DNS queries to internal DNS servers.
CYR-8787	When you Commit and Push changes to the Prisma Access security infrastructure, the Push Scope does not display the device group or template that was changed. **Workaround:** Select Commit > Commit and Push, and under Push Scope, select Edit Selections > Prisma Access and select the Mobile Users, Remote Networks, or Service Setup device group or template to which you want to commit changes.
CYR-8245	When you onboard a mobile user location, you cannot see or select all locations in a region if you are using Panorama with a Firefox browser version earlier than 65. **Workaround: Use a Firefox version with a version of 65 or later, or a different browser (for example, Chrome).**
CYR-8244	When performing a Commit and Push operation for the Clean Pipe service, you receive an error that the Clean Pipe service had insufficient license resources, even though you have sufficient licensed bandwidth. **Workaround:** Select Panorama > Licenses, then select Retrieve license keys from license server to retrieve the Clean Pipe licenses again.
CYR-8238 This issue is now resolved in plugin version 1.5. See Prisma Access 1.5.0 Addressed Issues.	The RIB In and RIB Out tabs under Panorama > Cloud Services > Status > Network Details > Service Connection > Show BGP Status and Panorama > Cloud Services > Status > Network Details > Remote Networks > Show BGP Status are displaying null pages.
CYR-8017	If you add an existing template under one of the template stacks of Prisma Access (for example, Service_Conn_Template_Stack, Mobile_User_Template_Stack, or Remote_Network_Template_Stack), you cannot use objects of the added template in other Prisma Access templates that are part of the same template stack. Previously, you could view and use objects from existing templates in Prisma Access templates if the templates were a part of a Prisma Access-specific template stack, which is not standard Panorama behavior.

Issue ID	Description
CYR-7907	In multi-tenant mode, Prisma Access automatically creates a set of templates, template stacks, and device groups for each tenant you create for remote networks, mobile users, and the Clean Pipe service. Prisma Access creates tenant-specific sets for all products, even if you are licensed for only one Prisma Access type. When you delete a tenant, Prisma Access deletes the template and device group set for which you are licensed, but does not delete the unlicensed set. For example, if you have a remote network deployment and delete a tenant, Prisma Access does not delete the set it created for the mobile users and Clean Pipe. **Workaround:** Manually delete the unused, unlicensed set of templates, template stacks, and device groups after you delete a tenant.
CYR-7900	The Traffic Forwarding feature (Panorama > Cloud Services > Configuration > Service Setup > Settings > Traffic Forwarding) is not supported with multi-tenant deployments.
CYR-7814 This issue is now resolved in plugin version 1.6.0. See Prisma Access 1.6.0 Addressed Issues.	Secondary tunnels are not supported with Prisma Access/AWS integrations that use dynamic (BGP) routing.
CYR-7795	When performing a commit operation, the commit fails with the Last Push State Details showing as The Prisma Access Infrastructure team is looking into the commit issue. Go to the Cloud Services > Status > Status tab for real-time Status Information. This message might be repeated multiple times in the window. **Workaround:** Wait 30 minutes, then retry the commit operation. This commit issue is temporary and is related to Prisma Access infrastructure.
CYR-7702	When you log out a Prisma Access mobile user from the Current Users window, the user still displays in the window after the logout operation. **Workaround:** Close and then reopen the Current Users window to show the correct user status.
CYR-7440	If you have two Panoramas set up in an active-primary and passive-secondary setup for Prisma Access, you cannot log out mobile users from the passive-secondary Panorama.
CYR-7332	When you try to configure an Infrastructure Subnet (Panorama > Cloud Services > Configuration > Service Setup > Settings) in multi-tenant mode, you can receive an Operation Failed message. **Workaround:** Refresh the Panorama UI to have Prisma Access correctly apply the infrastructure subnet to the tenant's configuration.
CYR-7128	When you perform a Commit All operation for mobile users, Prisma Access should display the commit status for portals and gateways separately;

Issue ID	Description
	however, Prisma Access is displaying failures for portals under gateway status, and is displaying commit failures for gateways under portal status. **Workaround:** Enter the `debug plugins cloud_services prisma-access get-job-result jobid` *commit-job-id-number* command, where *commit-job-id-number* is the ID of the commit operation that failed, to check and verify the commit operation for portals and gateways.
CYR-6475	When you select the Overlapped Subnets check box when configuring a remote network, the source zone in the traffic logs changes to the remote network name that is configured in Panorama > Cloud Services > Configuration > Remote Networks > Onboarding > *Name*.
CYR-6384	Pre-defined IKE Crypto, IPSec Crypto, and IKE Gateways templates do not display. **Workaround:** Select Panorama > Cloud Services > Configuration > Service Setup (for service connections) or Panorama > Cloud Services > Configuration > Remote Networks (for remote network connections), click the gear icon in the Settings area to open the Settings, then click OK.
CYR-6369	When in multi-tenant mode, if you create a custom admin user with an Admin Role Profile that has Read Only access to the Panorama tab and has Plugin access disabled, that user can view, configure, and commit changes for subtenants. **Workaround:** Disable access to the Panorama tab in the Admin Role Profile.
CYR-6317	Administrative users who configure Prisma Access using Panorama 9.0 can configure unsupported features. Prisma Access removes any unsupported features during the commit operation so that these features are not enabled in the cloud. **Workaround:** Make sure features in use are available in PAN-OS 8.1.
CYR-6241	For releases before 1.3.1, Prisma Access did not always enforce the minimum IP pool requirement for all regions in a mobile user deployment. In some cases, you could have specified an IP pool in the Americas region and that pool applied to all locations where you had deployed the Prisma Access gateways. When you perform your first commit after upgrading the Cloud Services plugin, Prisma Access checks that you have allocated an IP pool for all locations where you have deployed Prisma Access gateways, and you might receive a message that your IP pool is not sufficient for the deployed regions. **Workaround:** If you receive this message, either specify an IP pool for the regions that do not have them, specify a Worldwide IP pool, or remove the locations in regions that do not have IP pools.
CYR-6108	When you configure Clientless VPN with Prisma Access, the default security rule configuration uses the application-default service, which blocks clientless-vpn traffic.

Issue ID	Description
	Workaround: Change the default security rule to any service or service-http and service-https.
CYR-6107	When configuring multi-tenant, if you create any device groups that are children or grandchildren of other device groups you create under the Shared parent device group, select only the device group at the lowest hierarchical level (child or grandchild) when you associate the device group to an access domain; do not select the parent.
CYR-6080	You cannot reset the rule hit count for all Authentication and Application Override policies. **Workaround:** Reset rules using a list of rules or a rule name for Authentication and Application Override policies.
CYR-6013	When you migrate a single tenant to multi-tenant mode, you must do a local commit and then push the configuration before you add more tenants.
CYR-5888	When using the multi-tenant feature and creating template stacks and templates for a tenant, the Description of the template stacks and templates do not display in the Panorama > Templates page.
CYR-5867	After upgrading to a new version of the Cloud Services plugin, you are able to downgrade. The downgrade operation should be disallowed. **Workaround:** Do not downgrade the Cloud Services plugin after you have upgraded it.
CYR-5842	When using the multi-tenant feature and migrating the first tenant to multi-tenancy, you can select template stacks and templates that are not associated with the tenant that you want to migrate, including templates that are used with on-premise firewalls. **Workaround:** When you convert to multi-tenant mode, be sure to choose only those templates that you want to associate to the first tenant to migrate.
CYR-5700	When you create tenant names for the multi-tenancy feature, avoid using names like *Tenant-1*, *Tenant-2*, *Tenant-3*, and so on. The system logs reserve a small number of characters for the tenant name in the log output and, if tenants have similar names, it can be difficult to associate the tenant with the logs. We recommend using a unique and short name for tenants (for example, *Acme* or *Hooli*).
CYR-5690	When configuring multi-tenancy, if you are planning to later configure Prisma Access for mobile users, you must do a local Commit of the your changes for the plugin (Commit > Commit to Panorama) after you add templates, template stacks, and device groups for each tenant and before you onboard each tenant.
CYR-5563	When using the multi-tenancy feature, users who manage single tenants cannot see the system logs. The Monitor > Logs > System choice is not available. This limitation applies to all Administrators who have an

Issue ID	Description
	administrative role of Device Group and Template. Only superusers can view system logs in multi-tenancy mode.
CYR-5561	When using the multi-tenancy feature and logged in as a tenant-level administrative user, opening the Panorama Task Manager (clicking Tasks at the bottom of the Panorama web interface) shows all tasks for all tenants, including any tasks done at the superuser (Admin) level.
CYR-5476	When you enable multi-tenancy and migrate your configuration to the first sub-tenant, CLI commands are not supported for this operation. As a result, you must, use the Panorama user interface (UI).
CYR-5427	When configuring a tenant in multi-tenancy mode, create a unique name for each IPSec tunnel and IKE gateway for service connections and remote network connections, and try to use a name that will not be duplicated by another tenant. While there is no effect to functionality, you cannot delete an IPSec tunnel or IKE gateway if another tenant is using a tunnel or gateway with the same name.
CYR-5159	If you configure a mobile user IP address pool for a single region instead of Worldwide, mobile users can still view and attempt to connect to all available gateway regions from their GlobalProtect app. This attempt fails because there is no IP address pool to allocate for other regions. **Workaround:** To allow mobile users to manually select a gateway, either configure an IP address pool for the region in the location where you want the users to connect, or configure a Worldwide IP address pool for mobile users in Prisma Access to allow them to select all the locations you have deployed.
CYR-5139	In an environment with on-premise firewalls on each side of Prisma Access and the remote network connections to which the on-premise firewalls are connected are in different regions, users behind one on-premise firewall cannot contact users behind another on-premise firewall unless you have configured an explicit policy to allow traffic between zone Trust and zone Trust.
CYR-5098	If you change the master key in Panorama (in Device > Master Key and Diagnostics), the master key for Cloud Services is not synchronized with this master key. **Workaround:** Select Panorama > Cloud Services > Configuration > Service Setup > Service Operations > Edit Master Key and manually change the master key to be the same as the Panorama master key.
CYR-5062	When regular dynamic updates are downloaded to Panorama (by default, every Wednesday at 01:02), the MD5 checksum is changed. This condition can cause the Panorama configuration and the Prisma Access infrastructure to lose synchronization. While no tunnels are affected by this out of synchronization state, the status for Service Connections, Remote Networks, Mobile Users, and the Logging Service show a Config Status of Out of Sync.

Issue ID	Description
	Workaround: Perform a Commit and Push operation on the Panorama.
CYR-4954	After you upgrade the Cloud Services plugin from version 1.1.0 to 1.3.0, Configuration Assistant screens may display on the Panorama > Cloud Services > Configuration > Service Setup, Remote Networks, and Mobile Users tabs, even though you might have already used the Configuration Assistant before. **Workaround:** Click Don't Show Again when the screens display. These screens do not affect existing system configurations.
CYR-4010	The BGP router configuration on the Prisma Access firewalls can receive a maximum of 15000 prefixes from each peer. And the total number of routes (static and dynamic) learned through BGP cannot exceed 25000. Exporting more than 25000 routes may adversely affect traffic flow on your network.
CYR-3968 This issue is now resolved in plugin version 1.6.0. See Prisma Access 1.6.0 Addressed Issues.	Remote Network statistics (Panorama > Cloud Services > Status > Remote Networks > Status and Panorama > Cloud Services > Status > Remote Networks > Statistics) can take up to 1 minute to display after a traffic event occurs.
CYR-3952	After you generate a new API key by selecting Panorama > Cloud Services > Configuration > Service Setup > Generate new API Key, the previous API key is still valid for a period of time (up to five minutes). You use this API to retrieve the list of IP addresses for your Prisma Access firewalls.
CYR-3645	To use tunnel monitoring with BGP, the IP address that you are monitoring on the Prisma Access firewall must be part of a static subnet configured on a remote network location. The IP address cannot be a BGP exported subnet.
CYR-3638	For service and remote network connections that have BGP enabled, the Prisma Access ignores any route it receives from a neighbor with an AS number in its AS_PATH list that duplicates an AS number in the Prisma Access AS infrastructure (Infra-AS).
CYR-3544	The default priority of the cloud gateways in the Prisma Access are set to None instead of Highest.
CYR-3469	If you have configured a Notification URL, when you onboard a new remote network location, two notifications are sent to the URL instead of only one.
CYR-3385	When you configure the same AS number for the service connection and remote network location(s), the routes are not imported in to the firewall on the remote network location.
CYR-3330	Mobile users cannot connect to remote network locations without a service connection.

Issue ID	Description
CYR-3114	If your commit fails when you onboard Prisma Access components for the first time, the Task Manager does not always describe the cause of the failure. **Workaround:** To find the errors, select Panorama > Cloud Services > Status > Monitor and click the Status tab. Invalid configurations are indicated with a red bubble in the Config Status column and an error of `Validation Error`.
CYR-3034	When configuring SAML, you must perform all configuration with a role of Superuser, including any configuration you perform for SAML using CLI.
CYR-2648	The Panorama > Cloud Services > Configuration page is grayed out when Panorama is not in sync with NTP. **Workaround:** Make sure to synchronize time with NTP (Panorama > Setup > Services > NTP).
CYR-2633	You cannot change the region associated with multiple remote network locations in a single commit push to the Prisma Access. **Workaround:** If you need to change the region on more than one remote network location, change them one at a time and complete the commit push before changing the region on the next remote network.
CYR-2578	Master Keys do not work for two Panorama appliances set as HA primary and secondary appliances. **Workaround:** Deselect the Enable HA check box on the secondary Panorama appliance and commit the changes, set the same Master Key on both the primary and secondary Panorama appliance, then re-enable HA on the secondary Panorama appliance and commit the changes.
CYR-2028	The Device > Setup > Management page is not available on the Panorama appliance running the Prisma Access plugin. You cannot configure NT LAN Manager (NTLM).
CYR-1836	You cannot enforce MFA when users at one of your corporate HQ locations attempts to access a resource at a remote network location.
CYR-1646	Although Panorama allows you to delete the Mobile_User_Template that was created when the Prisma Access was provisioned, deleting this template also deletes your onboarding configuration and, upon commit, removes your Prisma Access for mobile users configuration.
CYR-1189	When you onboard a new service connection or a remote network, the count for service connection and total remote peers displayed on Panorama > Cloud Services > Status > Status is inaccurate until the provisioning is complete.
CYR-1120	On Panorama, you cannot validate commit on a device group or template configuration before pushing the configuration to the Prisma Access infrastructure for remote networks and mobile users.

Issue ID	Description
CYR-950 This issue is now resolved in plugin version 1.5.0. See Prisma Access 1.5.0 Addressed Issues.	You cannot view detailed HIP reports from the Monitor > Logs > HIP Match.
CYR-575	You cannot configure the Prisma Access gateway as an internal gateway.

Prisma Access Addressed Issues

The following topics describe issues that have been addressed in Prisma Access by the Prisma Access:

Prisma Access 1.6.1 Addressed Issues

Issue ID	Description
CYR-12146	Fixed an issue where Prisma Access was not advertising mobile user subnets through BGP.
CYR-11781	Fixed an issue where the API script was returning extra portal IP addresses when requesting gateway IP addresses.
CYR-11459	Fixed an issue where, when a client tries to log in to the auto-scaled gateway, the MFA response lands on the incorrect gateway.
CYR-11444	Fixed an issue where user-to-IP address mapping entries showed `Never` as the idle timeout and maximum timeout values instead of showing the actual values.

Prisma Access 1.6.0-h1 Addressed Issues

Issue ID	Description
CYR-11851	Fixed an issue where AS-PATHs were not prepended correctly for a backup service connection in a multi-tenant environment.
CYR-11840	Fixed an issue where user names with special characters were not reported correctly.

Issue ID	Description
CYR-11822	Fixed an issue where, in a multi-tenant deployment, hot potato routing-related configuration did not become enabled for a tenant.
CYR-11760	Fixed an intermittent issue where logs were delayed or missing when querying for logs by applying filters. To leverage this fix, you must upgrade your minimum Panorama version to 9.0.9 as well as upgrade the Cloud Services plugin to 1.6.0-h1.
CYR-11752	Fixed an issue where, when using a Panorama running PAN-OS 9.1 in multi-tenant mode and logging in as a tenant-level user, you could not add remote networks or configure mobile users.

Prisma Access 1.6.0 Addressed Issues

Issue ID	Description
CYR-11159	Fixed an issue where a SIP Message is not parsed correctly when a packet is received in separate segments, which caused the receiver to receive a corrupted message.
CYR-11037	Fixed an issue where multiple GlobalProtect portals in Prisma Access were not being selected in the correct order (GlobalProtect was caching the previous profile that was used).
CYR-10838	Fixed a firewall issue on firewalls where a process (`userid`) restarted while processing incorrect IP address-to-username mappings that contained blank usernames from User-ID agents.
CYR-10836	Fixed an issue where, after enabling a Cortex Data Lake license, the management plane memory utilization would increase unexpectedly when some connections between the firewall and Customer Support Portal server were blocked, leading to multiple process restarts due to an out-of-memory (OOM) condition.
CYR-10835	Fixed an issue where Security Assertion Markup Language (SAML) response validation failed with a certificate mismatch error, even if the firewall had the same certificate on IdP.
CYR-10734	Fixed an issue where a Commit and Push operation from Panorama failed in passive firewalls when pushing a large number of new Security policy rules to both firewalls in a high availability (HA) pair.
CYR-10728	Fixed an issue where connections proxied by the firewall (such as SSL Decryption, GlobalProtect portal and gateway connections, and SIP over TCP) failed due to a buffer allocation failure. Some connections failed with a `proxy decrypt failure` message.

Issue ID	Description
CYR-10655	Fixed an issue where a Commit operation failed because of memory and deadlock issues in the Prisma Access infrastructure.
CYR-10569	Fixed an issue where an administrator could not create a large number of additional remote network tunnels in a multi-tenant configuration.
CYR-10474	Fixed an issue where Prisma Access was using the management interface for certificate revocation list (CRL) checks (the management interface is not supported in Prisma Access).
CYR-10444	Fixed an issue where, when using DLP on Prisma Access, you can configure a security policy in a non-Prisma Access device group; however, if you are using the same parent device group for on-premise firewalls and Prisma Access firewalls, committing your changes will fail, because the on-premise firewalls do not have references to the data filtering profile in the Prisma Access device group.
CYR-10319	Fixed an issue where Prisma Access could not display the Verify Account window to enter the one-time password (OTP) for account verification.
CYR-10303	Fixed an issue on the firewalls where the dataplane restarted unexpectedly when processing HTTP/2 traffic if packet-diag debugs were enabled.  *This fix is available in PAN-OS releases 9.0.6 and later and 9.1.0 and later.*
CYR-10239	Fixed an issue where logs for the Clean Pipe service were not being forwarded to Cortex Data Lake.  *If you continue to encounter this issue, select Panorama > Cloud Services > Clean Pipe, click the gear icon in the Settings area to edit the settings, click OK, then perform a push operation to the Clean Pipe service.*
CYR-9751	Fixed an issue where, after installing the plugin but before the account has been verified with a one-time password (OTP), Panorama could not retrieve the logs from Cortex Data Lake.
CYR-9698	Fixed an issue where users were experiencing connection failures to the India West Prisma Access location.
CYR-9638	Fixed an issue where WildFire logs were not displaying in Cortex Data Lake because a new enum was added in the subtype of threat logs for next-generation firewalls, which changed the integer value of the subtype.

Issue ID	Description
CYR-9540	Fixed an issue where the Detailed Log View of DLP data filtering logs from one location could not be viewed if the Panorama running Prisma Access was in another location.
CYR-9079	Fixed an issue where certificate profiles do not display in the HIP Objects' certificate profile (Objects > GlobalProtect > HIP Objects > <*hip-object-name*> > Certificate > Certificate Profile) if the HIP object is Shared (that is, not under a specific device group).
CYR-7814	Fixed an issue where secondary tunnels are not supported with Prisma Access/AWS integrations that use dynamic (BGP) routing.
CYR-3968	Fixed an issue where remote network statistics (Panorama > Cloud Services > Status > Remote Networks > Status and Panorama > Cloud Services > Status > Remote Networks > Statistics) can take up to 1 minute to display after a traffic event occurs.

Prisma Access 1.5.1 Addressed Issues

Issue ID	Description
CYR-9826	Fixed an issue where some applications, URLs, and threats could not be properly identified.
CYR-9626	Fixed an issue where onboarding a Clean Pipe instance failed with the message `Fail to load completions for regions from cloud service`.
CYR-9502	Fixed an issue where, when the bandwidth for a remote network was changed, a new Service IP address was created for the remote network, instead of retaining its existing service IP address. This behavior has been observed in the US West, South Korea, Ireland, and France North locations.
CYR-9394	Fixed an issue where, when mobile users were using the Clientless VPN application, they were not being directed to the company-specific domain name and instead were being redirected to the Prisma Access-specific domain`companyname.gpcloudservice.com`. In addition, when using Microsoft SAML, users were being redirected to `https://companyname.gpcloudservice.com:443/SAML20/SP`.

Prisma Access 1.5.0 Addressed Issues

Issue ID	Description
CYR-9179	Fixed an issue where searches did not work in Route Information Base (RIB) queries.
CYR-8945	Fixed an issue where mobile users in the Costa Rica location were getting the Canada East location as an alternative gateway, although other gateways had a better latency.
CYR-8836	Fixed an issue where mobile users were experiencing intermittent timeouts when authenticating.
CYR-8712	Fixed an issue where SAML authentication failed with a `Failure while validating the signature of SAML` message, even though the certificates on IDP and firewall side are identical.
CYR-8467	Fixed an issue where a commit and push operation did not get distributed to the entire Prisma Access infrastructure.
CYR-8461	Fixed an issue where Prisma Access was sending logs that indicated that NTP was having synchronization issues.
CYR-8447	Fixed an issue where Public ASN numbers were not allowed when onboarding a Clean Pipe.
CYR-8408	Fixed an issue where the Clean Pipe Pairing Key was incorrectly spelled in the Cloud Services plugin user interface.
CYR-8382	Fixed an issue where, when the Manual option was checked in the Portal config, and Manual Gateway Locations were selected during mobile user onboarding, a push attempt failed with a `manual constraints failed` error message.
CYR-8381	Fixed an issue where users could not reach the internet after Overlapped Subnets was enabled for two remote network connections.
CYR-8238	Fixed an issue where the Local RIB and RIB Out tabs under Panorama > Cloud Services > Status > Network Details > Service Connection > Show BGP Status and Panorama > Cloud Services > Status > Network Details > Remote Networks > Show BGP Status are displaying null pages.
CYR-8224	Fixed an issue where a large number of login and timeout events were being experienced from the Prisma Access gateway.
CYR-6271	Fixed an issue where a connection from the GlobalProtect app to the Prisma Access portal was timing out with a `Portal Not Found` error.

Issue ID	Description
CYR-5388	Fixed an issue where a service connection was showing a status of Down even though the IPSec tunnel was up.
CYR-950	Fixed an issue where you could not view detailed information on HIP Match logs on Monitor > Logs > HIP Match.

Prisma Access 1.4.0-h2 Addressed Issues

Issue ID	Description
CYR-8447	Fixed an issue where Public ASN numbers were not allowed when onboarding a Clean Pipe.
CYR-8408	Fixed an issue where the Clean Pipe Pairing Key was incorrectly spelled in the Cloud Services plugin user interface.
CYR-8350	Fixed an issue where customers with only a Mobile Users license could not enable multi-tenancy.
CYR-8251	Fixed an issue where a mobile users commit operation failed with an error of `hostname should end with .gpcloudservice.com`.

Prisma Access 1.4 Addressed Issues

In addition to the following issues, GPC-8189 has been addressed, which affected GlobalProtect app users who select a manual gateway.

Issue ID	Description
CYR-7662	Fixed an issue where a Panorama appliance with the Cloud Services plugin installed (managing Prisma Access or Cortex Data Lake) failed to authorize one-time-password (OTP) submissions during the onboarding process.
CYR-6521	Fixed an issue where, when configuring multi-tenancy, the push scope is not automatically populated when changes are made to sub-tenant templates. **Workaround:** Select Commit > Commit and Push and Edit Selections in the Push Scope.Then select Prisma Access and select the tenant and service for which you want to make the changes, then select Commit and Push.
CYR-6416	Fixed an issue where, after upgrading from the Cloud Services plugin 1.3.0 to 1.3.1, previously-onboarded Mobile User locations can become deselected in the Onboarding area (Panorama > Cloud Services > Configuration > Mobile Users > Configure >

Issue ID	Description
	Locations). All locations are still active, functional, and visible in the Status area (Panorama > Cloud Services > Status > Monitor > Mobile Users). **Workaround:** This is a rare occurrence. If your deployment experiences this issue, select Panorama > Cloud Services > Configuration > Mobile Users > Configure, click the Locations tab, re-select the gateways you previously onboarded, then Save and Commit your changes.
CYR-6332	Fixed an issue where logged-in Clientless VPN users are not listed in the Mobile Users Status page (Panorama > Cloud Services > Status > Status > Mobile Users).
CYR-6051	Fixed an issue where, when configuring multi-tenancy, when you delete a tenant, the system also deleted the templates and template stacks associated with the tenant. This can cause issues with on-premise firewalls or other devices that also use these templates. **Workaround:** Create unique template stacks and templates for each tenant, and do not share them with any other devices.
CYR-5984	Fixed an issue where, when using the multi-tenant feature and logging in to a single tenant as a tenant-specific administrative user, the screen became blank and you cannot view the tenant information. **Workaround:** Select Panorama > Cloud Services > Status or Panorama > Cloud Services > Configuration and click the Refresh button (on the top right next to the Help button). It can take up to 10 seconds for the screen to display the tenant's configuration.

Prisma Access 1.3.1-h5 Addressed Issues

Issue ID	Description
CYR-6834	Fixed an issue where, when you upgraded the Cloud Services plugin and accessed the Panorama > Cloud Services > Configuration > Mobile Users page, you received an error that the portal hostname was invalid.

Prisma Access 1.3.1-h4 Addressed Issues

Issue ID	Description
CYR-6897	Fixed an issue where, when onboarding a remote network connection that was within the licensed bandwidth allocation, a

Issue ID	Description
	message displayed indicating that there wasn't enough licensed bandwidth.

Prisma Access 1.3.1-h3 Addressed Issues

Issue ID	Description
CYR-6608	Fixed an issue where account verification failed when proxy servers are used with the Panorama appliance and the DNS servers are internal only.
CYR-6606	Fixed an issue where you could not see the QoS Profile choice in Panorama, in Network > Network Profiles > QoS Profile. You should see this choice in the Service_Conn_Template and the Remote_Network_Template, but not in the Mobile_Users_Template.
CYR-6557	Fixed an issue where, after upgrading to 1.3.1, commits failed with an error indicating that mobile user regions were not set.

Prisma Access 1.3.1 Addressed Issues

Issue ID	Description
CYR-6131	Fixed an issue where the Online Help pages in the multi-tenancy area did not display the information for multi-tenancy in the topic that displays.
CYR-6105	Fixed an issue where a remote network could not be onboarded; clicking OK did not close the configuration window.
CYR-6006	Fixed an issue where an infrastructure subnet could not be specified on M-600 devices.
CYR-5793	Fixed an issue where, when you viewed mobile user information in the Panorama > Cloud Services > Status > Status area, users who are logged into multiple devices using the same gateway appeared in the list of logged-in users and previously logged-in users only once. The list correctly displayed the multiple device information if users were logged into multiple devices using different gateways.
CYR-5720	Fixed an issue where, when assigning IP address pools, if the total number of IP addresses for all regions equals 4,096, you receive a popup window that you need to configure a minimum of 4,096 addresses, even though you have configured the minimum.

Issue ID	Description
CYR-5304	Fixed an issue where the addition of a new device group (Service_Conn_Device_Group) could cause commit-related errors.
CYR-4891	Fixed an issue where notifications for loopback IP (loopback_ip) addresses were not being sent when the loopback IP address changes.

Prisma Access 1.3.0-h6 Addressed Issues

Issue ID	Description
CYR-6267	Fixed an issue where the Cloud Services plugin displayed a blank screen after the Panorama virtual appliance was upgraded to 8.1.6.

Prisma Access 1.3.0 Addressed Issues

Issue ID	Description
CYR-5382	Fixed an issue where, after you upgrade the Panorama on which your Prisma Access plugin resides, you needed to Commit and Push your Prisma Access configuration. To do so, click Commit > Commit to Panorama and click Commit > Commit and Push. Then, click Edit Selections > Prisma Access, and select Prisma Access for remote networks, Prisma Access for mobile users, and Prisma Access for service setup. Then click OK and Push.
CYR-5360	Fixed an issue where policy rule hit counts for security policies that were renamed or deleted were appearing when using CLI commands.
CYR-5243	Fixed an issue where mobile users could not manually connect to a Prisma Access gateway because of a DNS resolution error.
CYR-5186	Fixed an issue where mobile users could not connect to a Prisma Access gateway because a DNS lookup resolved to multiple IP addresses.
CYR-5153	Fixed an issue where, if you had enabled BGP on your service connections or remote networks, when you viewed the Show BGP status table (available from Panorama > Cloud Services > Status > Network Details > Service Connection and Panorama > Cloud Services > Status > Network Details > Remote Networks), only the first 256 entries were shown in the RIB-In tab.

Issue ID	Description
CYR-5089	Fixed an issue where downgrading the Panorama appliance from PAN-OS release 8.1 to 8.0 could cause the Prisma Access configuration to lose synchronization.
CYR-4980	Fixed an issue where, when using multi-tenancy, you could not create users with the ability to configure and manage a single tenant.
CYR-4876	Fixed an issue where threat packet captures could not be downloaded from the Cortex Data Lake. You must upgrade your Panorama to PAN-OS 8.1.6 to fix this issue.
CYR-4697	Fixed an issue where Network Address Translation-Traversal (NAT-T) was disabled by default. Enabling NAT-T allows customers to connect devices behind NAT to service connections and remote networks without having to enable NAT-T. If you use an Encapsulated Security Protocol (ESP) instead of UDP port 4500 and your peer is not behind NAT, you should disable NAT-T.
CYR-3344	Fixed an issue where, in Panorama, selecting Network > GlobalProtect > Portals > *GlobalProtect-portal-config* > Agent > *agent-config* > App and changing Allow User to Disable GlobalProtect App from Allow to Allow with Ticket did not display an 8-character hexadecimal ticket request number.
CYR-2437	Fixed an issue where, if configured Panorama to use a proxy server (Panorama > Setup > Services > Proxy server), all traffic to the Prisma Access and the Cortex Data Lake would bypass the proxy server.

Prisma Access 1.2.0-h2 Addressed Issues

Issue ID	Description
CYR-5074	Fixed an issue where, after upgrading to Prisma Access version 1.2 from a Panorama appliance running release 8.0, remote network and BGP information is missing from the Panorama > Cloud Services > Status > Network Details > Remote Networks area. In addition, BGP information is missing from the Panorama > Cloud Services > Status > Network Details > Service Connection area.

Prisma Access 1.2.0 Addressed Issues

Issue ID	Description
CYR-4695	Fixed an issue where insufficient internal DNS domains were available in the Prisma Access mobile users configuration. The maximum number of DNS domain entries is now 1,024.
CYR-4542	Fixed an issue where mobile users were being routed to a Prisma Access gateway in a region that were farther from their location than other gateways.
CYR-4495	Fixed an issue where the Cortex Data Lake license was displaying a different region than the region for which it had been registered.
CYR-4261	Fixed an issue where a valid commit operation failed with the reason `ssl-tls-service-profile 'SSL_FOR_GPaaS_Cert' is not a valid reference`.
CYR-4250	Fixed an issue where a DNS CNAME to another DNS name was not resolving to an IP address.
CYR-4246	Fixed a reporting issue where the peak bandwidth time was not displaying when you hover over the fields in Panorama > Cloud Services > Status > Remote Networks > Statistics > Ingress Peak Bandwidth (Mbps) and Egress Peak Bandwidth (Mbps) fields.
CYR-4188	Fixed an upgrade issue where a commit failed with the error `Validation Failure - plugins > cloud_services > logging-service not expected here`.
CYR-4122	Fixed an issue where the status and usage statistics displayed on Panorama > Cloud Services > Status > Monitor was reset for Peak Ingress Egress Throughput, Peak Egress Throughput, Peak Ingress Egress Throughput Timestamp, and Peak Egress Throughput Timestamp. This reset occurred after a maintenance window for the Prisma Access or on an HA failover of the remote network firewalls in the cloud infrastructure.
CYR-4082	Fixed an issue where the Show BGP Status link on Panorama > Cloud Services > Status > Network Details did not always display BGP status information. **Workaround**: Refresh the BGP status window to fetch the information.
CYR-4047	Fixed a commit synchronization issue where a commit operation was not synchronized correctly with other commit operations.
CYR-4013	Fixed a consistent naming issue so that parameters in the command to retrieve the Public IP (Egress IP) and Loopback IP addresses are more descriptive. In the $fwType area, gpcs_gw is changed to gpcs_gp_gw, gpcs_pt is changed to gpcs_gp_portal,

Issue ID	Description
	and remote_network is changed to gpcs_remote_network. In the $addrtype area, egressip is changed to public_ip and loopbackip is changed to loopback_ip.
CYR-3667	Fixed a statistics display issue where all records in the Panorama > Cloud Services > Status > Remote Networks > Statistics area were not being displayed.
CYR-3397	Fixed an update issue where Apple device and iOS updates could not be downloaded from the internet.
CYR-2876	Fixed an issue where only subnets greater than or equal to /19 could be specified for the IP address pool for mobile users. Now, you can specify a minimum of a /20 subnet (minimum of 4,096 available IP addresses) in different regions or globally.
CYR-2657	Fixed an issue where the plugin was unable to get the default GlobalProtect Portal domain. A fix has been added to renew the Cortex Data Lake certificate automatically. Previously, the error message `The plugin is unable to get the default GlobalProtect Portal domain` displayed. This issue could have occurred when you completed the one-time password (OTP) account verification process when only the Cortex Data Lake license was activated in Panorama, and then activated the Prisma Access licenses for remote networks or mobile users. **Workaround:** To fix this issue, redo the OTP verification by navigating to Panorama, selecting Panorama > Cloud Services > Configuration, and clicking Verify.

Prisma Access 1.1.0 Addressed Issues

Issue ID	Description
CYR-3508	Fixed a bulk import issue that occurred when you exported your existing remote network configuration with dynamic IP addresses for both the Primary Peer and the Secondary Peer, and then imported that configuration back in to Panorama.
CYR-3314	You can now authenticate mobile users to GlobalProtect gateways in the cloud using SAML authentication.
CYR-3036	Fixed a license validation error that prevented you from allocating more bandwidth to a remote network that you had already onboarded.
CYR-3013	Fixed a display issue with duplicate entries on Panorama > Cloud Services > Status > Monitor for cloud firewalls in each region where you had onboarded remote networks.

Issue ID	Description
CYR-2924	The logs on Panorama display the message: `Unableto connect to API gateway`. You can ignore this message because the firewalls can successfully communicate with Cortex Data Lake.
CYR-2888	Fixed an issue where, for IPSec tunnels configured with Proxy IDs, Panorama does not display the IPSec tunnel status accurately even though the tunnel is up. **Workaround:** Remove the Proxy ID configuration for the IPSec tunnel.
CYR-2662	Fixed a display issue that occurred when you reinstalled the cloud services plugin and loaded a previously saved Prisma Access configuration snapshot.
CYR-2199	The certificate warning no longer displays when an Android device connects to the GlobalProtect portal that uses the default domain.
CYR-445	The Prisma Access firewalls can now ingest User-ID mappings using the User-ID Syslog listener.

Getting Help

The following topics provide information on where to find more about this release and how to request 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 secure your SD-WAN and public cloud deployments.
- Use the Cortex Data Lake Getting Started Guide to learn how to deploy Cortex Data Lake and begin forwarding logs from your on-premise firewalls to Cortex Data Lake.

Refer to the following documentation on the Technical Documentation portal or search the documentation for more information on our products:

- **Panorama Administrator's Guide**—Provides the basic framework to quickly set up the Panorama™ virtual appliance or an M-Series appliance running version 9.0 or 9.1 for centralized administration of the Palo Alto Networks firewalls.
- **PAN-OS Administrator's Guide**—Provides the concepts and solutions to get the most out of your Palo Alto Networks next-generation firewalls. This includes taking you through the initial configuration and basic set up on your Palo Alto Networks firewalls for PAN-OS 9.0 or 9.1.
- **GlobalProtect Administrator's Guide**—Describes how to set up and manage GlobalProtect™ for GlobalProtect 9.0 and 9.1.

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