Cloud Identity Engine

Simplify Zero Trust with Easy-to-Deploy User Identity and Access Across All Locations

Identity is a critical component of a Zero Trust approach to network security. With enterprises increasingly migrating from on-premises to cloud identity providers, and users connecting from anywhere, it is difficult to keep security and identity information connected and in sync across the network.

Networks are designed for a single source of identity, and this can lead to inconsistent security between data centers, campus networks, public clouds, and hybrid environments. Until a few years ago, on-premises identity providers (e.g., Microsoft AD) observed comprehensive adoption across enterprise customers. However, as cloud usage has accelerated, 87% of organizations are moving or planning to move to cloud-based identity sources (IdPs) in the next two years.[1]

Identity and authentication services have transitioned from highly protected, trusted network enclaves to services that exist both inside and outside the enterprise—enterprises are either using a hybrid model (using both on-prem and cloud identity providers) or have completely transitioned from on-premises to the cloud, and in most cases using multiple cloud identity providers.

Put another way, enterprises in this day and age find it difficult to consistently verify users and enforce identity-based security at all times as enterprises are migrating from on-premises (e.g., LDAP) to cloud identity providers (e.g., Azure AD, Okta, Ping, Microsoft AD, Google Identity), which has led to a fragmentation of enterprise identity, privileges, and entitlements. This has led to network security operators struggling to secure their workforce and enable safe and secure access to applications and data they need to get their work done.

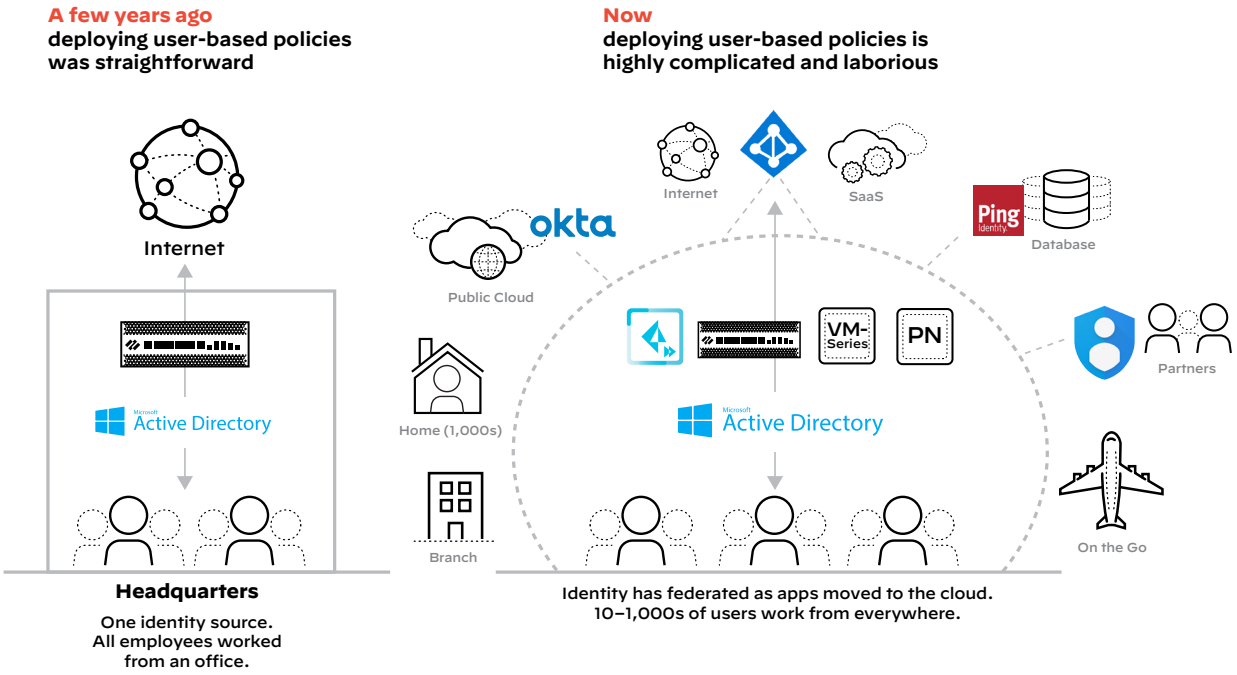

Figure 1: Managing identity has become challenging to the enterprise

Configuring, maintaining, and synchronizing the network security ecosystem with the multiple identity providers used by an enterprise is time-consuming and resource-intensive, resulting in significantly increased effort and delayed projects. Moreover, lack of visibility into user activity across security controls leads to gaps in security posture.

Fragmentation of identities in an enterprise and the resulting difficulty in ensuring consistent application of identity-based security controls have created a significant barrier to adopting Zero Trust measures to protect organizations against data breaches.

This transition demands a highly adaptable solution that enables identity-based controls in a cloud-first world.

1. Doug Cahill, *ESG Master Survey Results: Trends in IAM: Cloud-Driven Identities*, December 30, 2020, https://www.esg-global.com/research/esg-master-survey-results-trends-in-iam-cloud-driven-identities.

Existing Solutions Fail to Support Today's Hybrid Identity Infrastructure

Organizations today need to transition to cloud identity stores as their apps are moving to the cloud, but they give up midway as deploying identity controls is complex. Security teams using user-based policies with on-premises identity sources struggle to implement the same use case with cloud identity providers (IdP) efficiently. Existing solutions require manually configuring each identity provider, with every firewall and relying on APIs for each identity provider which can take months to years to complete.

Moving from on-premises to the cloud requires organizations to first move to a hybrid world and fully transition to the cloud over months or years. Moreover, no other provider can support identity and authentication with both on-prem and cloud identity providers, as well as enforce user-based controls across both on-premises infrastructure (e.g., enterprise data center and branch security) and cloud infrastructure.

Business Benefits

- **Achieve Zero Trust for a cloud-first world.** Easily and consistently verify user identity prior to granting access using point-and-click IdP integrations.
- **Unified identity across infrastructure.** Synchronize user, group, and authentication data across all FwaaP products.
- **Prevent credential-based attacks.** Deploy pervasive MFA for all apps and users irrespective of the app or the IdP.
- **Always-on identity for Zero Trust.** Global, resilient, cloud native engine.
- **Instant MFA for all data center apps.** Use the cloud identity provider's MFA for all data center apps instantly.
- **Investment protection.** Smoothly transition from on-prem to the cloud—IdPs, firewalls, or apps—with minimal effort.

The Industry's First Cloud Native Identity Synchronization and Authentication Service, Providing a Single Source of Identity for All Users Everywhere

Identity-based security controls are a foundational requirement to achieve Zero Trust. Palo Alto Networks Cloud Identity Engine is an entirely new cloud-based architecture for identity-based security that can consistently authenticate and authorize your users, regardless of location and where user identity stores live—on-premises, in the cloud, or hybrid. As a result, security teams can effortlessly allow all users access to applications and data everywhere and quickly move toward a Zero Trust security posture. Cloud identity Engine saves you time and hassle in deploying and managing identity-based controls on your network security infrastructure, using a point-and-click configuration with real-time identity synchronization.

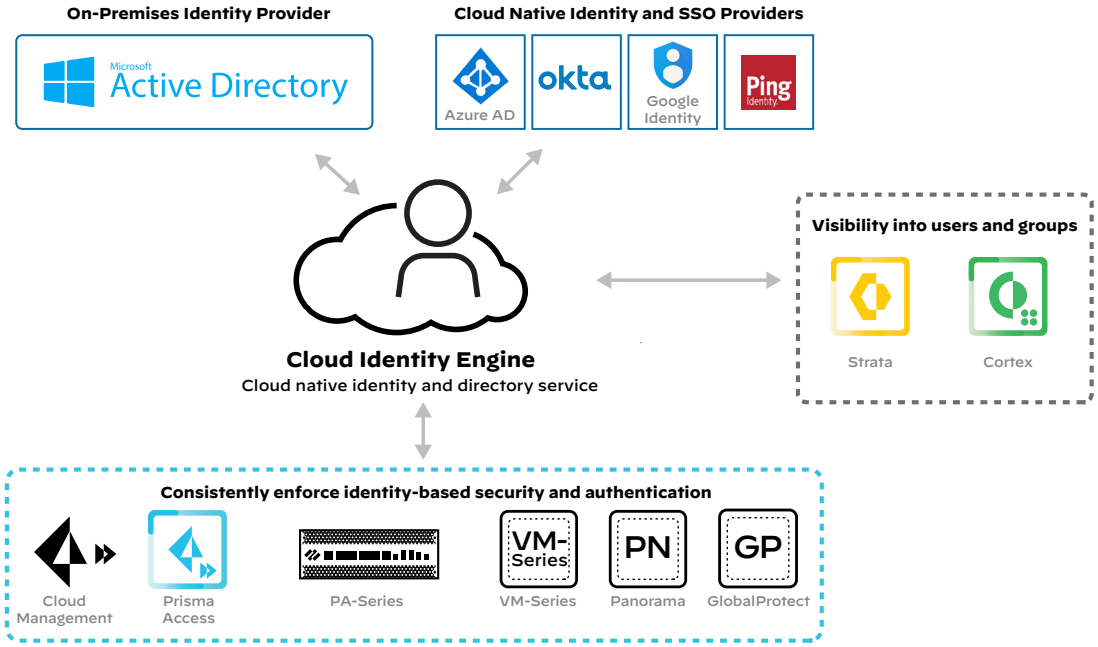

Figure 2: Cloud Identity Engine provides a single source of identity and authentication across Palo Alto Networks products

Key Capabilities

Simplifying Identity-Based Group Policies

Cloud Identity Engine unifies identity across the network security infrastructure by synchronizing users, groups, and authentication data across all Palo Alto Networks products. It supports both on-premises and cloud identity providers from a single point, allowing security and identity teams to have synchronized user, group, and authentication information across the entire network security infrastructure. Organizations can leverage their existing security policies, but now with cloud identities and smoothly transition from on-premises to the cloud with minimal effort.

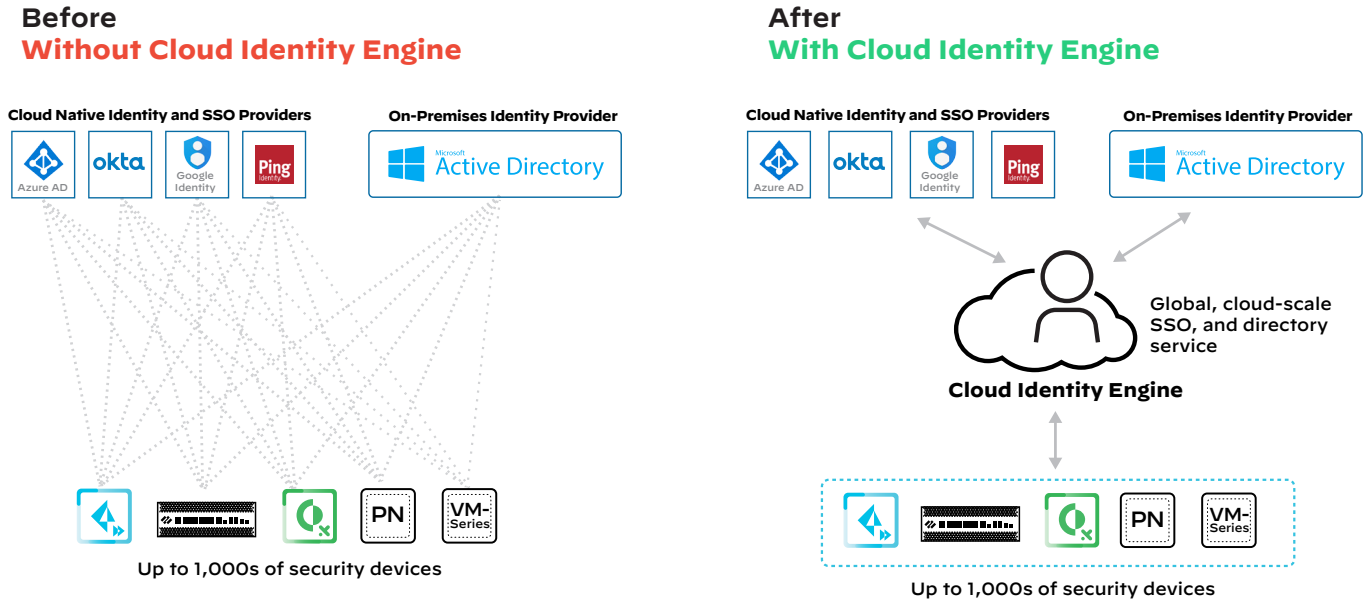

Figure 3: Unifying identity security through our enterprise network with assured synchronization of user information at all times

Achieving this was highly resource-intensive and operationally heavy in the past. Security teams had to rely on APIs to connect their firewalls to each identity provider, and adding a new identity provider required configuring all their security devices with the identity provider again. With Cloud Identity Engine, security teams can easily configure and connect with multiple identity providers—on-premises, multicloud, and hybrid identity providers—and enforce user group-based security policies. Adding a new identity provider can be achieved in around 10 minutes.

Additionally, Cloud Identity Engine offers real-time identity synchronization, which means any incremental changes to identity information—for example, every time a user joins, moves, or terminates—and any changes by identity providers are pulled and addressed automatically. Security teams no longer need to do anything after the initial setup as the user and group information is always in sync in Cloud Identity Engine.

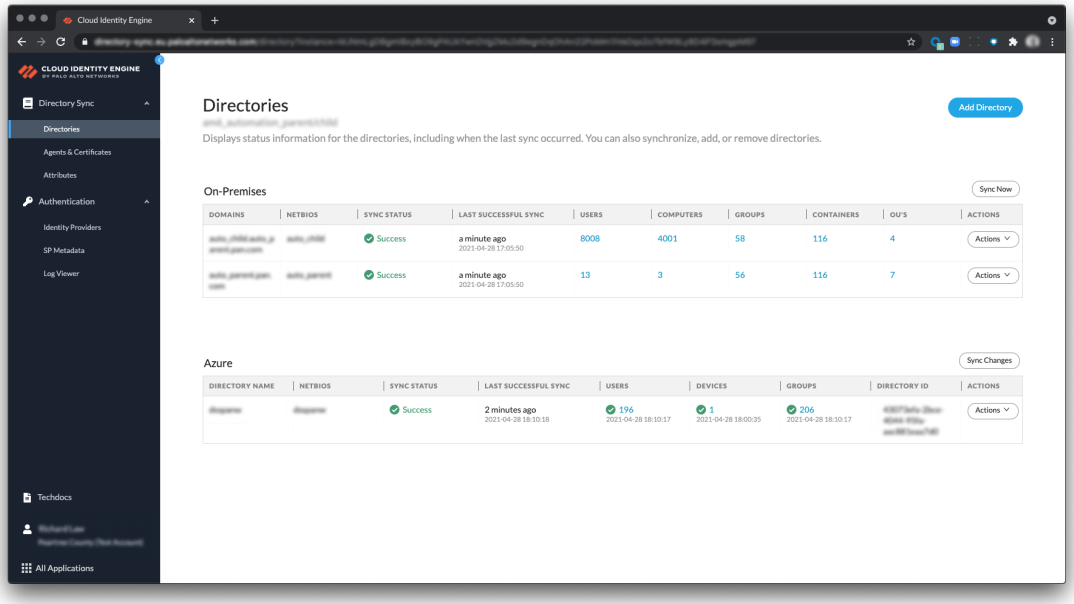

Figure 4: Configure multiple identity providers with ease on the Cloud Identity Engine app

Simplifying Cloud Authentication Setup and Management

IdPs can also serve to authenticate users who are leveraging single sign-on to access websites. Palo Alto Networks has supported on-premises authentication for many years. However, setting up authentication with cloud IdPs is complex as cloud IdPs rely on SAML protocol for authentication. In SAML authentication, every time an IdP is added or a new instance of the same IdP is created, network security teams need to configure that IdP with every firewall and management system. This leads to time-consuming and expensive network configuration.

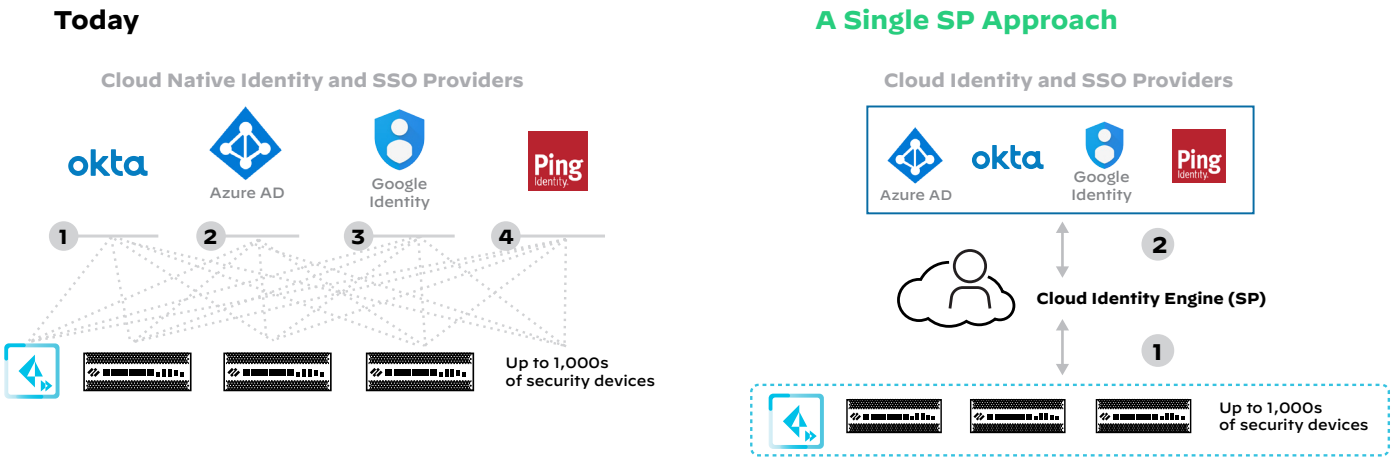

Figure 5: Setting up authentication with multiple identity providers

Cloud Identity Engine is a cloud service in which customers can integrate with one or more IdPs of their choice with just a few clicks, eliminating the frustration of configuring IdPs with each security device. Palo Alto Networks is the only vendor that can offer MFA across both cloud applications and an on-premises application, enabling secure authentication across all users and applications. It provides network security teams a single point to implement and manage MFA irrespective of on-premises or cloud IdP.

Multi-authentication in the Palo Alto Networks Cloud Identity Engine allows customers to configure a single authentication endpoint (GlobalProtect, Authentication Portal, Admin login) with multiple authentication types and/or multiple identity providers. For example, a single GlobalProtect™ authentication flow can be completed with Okta, Azure, or certificate-based authentication, depending on which user is trying to gain access. This is essential when multiple IdPs with multiple authentication types are present on a network. Note, Cloud Identity Engine does not enforce MFA policies. It simplifies the setup and management of MFA.

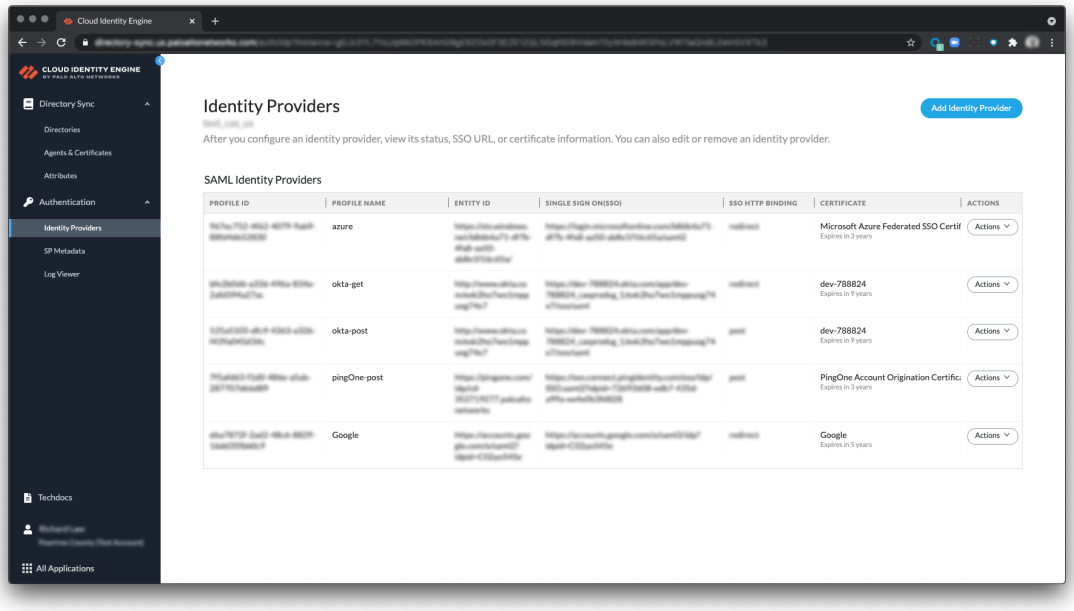

Figure 6: Configure multiple authentication providers with ease on the Cloud Identity Engine app

Operational Benefits

- **Accelerate transition from on-premises to cloud-based identity.** Manage on-premises, multicloud, and hybrid identity providers from a single point.
- **Easy setup.** Consistently verify user identity prior to granting access. Easily apply these controls everywhere in your enterprise: data center, campus, public cloud, branches, and remote users.
- **Consistently authenticate and authorize users at scale.** Accurately enforce security decisions for all your users at all times.
- **Maintenance-free.** Automatic synchronization of all identity-related data from all active directories in the cloud.
- **Optimize firewall performance for user-based policies.** Only push user groups to the firewalls that need them.
- **Save time and resources.** Quickly deploy and manage identity-based controls. Integrate with identity providers in about 10 minutes with point-and-click IdP integrations.
- **Customizable authentication experience per user or group.** Allow users and groups to authenticate with the appropriate authentication type for that user or group (e.g., in merger and acquisition situations).
- **Ensure privacy of personal data.** Selectively distribute employees' data based on company policy with System for Cross-domain Identity Management (SCIM) granular access control.

Table 1: Palo Alto Networks Cloud Identity Engine Privacy, Features, and Capabilities

Privacy with Cloud Identity Engine

Trust and Privacy	Palo Alto Networks has strict privacy and security controls in place to prevent unauthorized access to sensitive or personally identifiable information. We apply industry-standard best practices for security and confidentiality. You can find further information in our Cloud Identity Engine privacy datasheet.

Versions and Requirements

Availability	The full feature set of Cloud Identity Engine is available as a (free) core feature on Palo Alto Networks Next-Generation Firewalls: hardware (PA-Series), virtual (VM-Series), and management (Panorama) platforms running on PAN-OS 10.1 and above. Cloud Identity Engine for group-based policy is available as a (free) core feature on Palo Alto Networks Next-Generation Firewalls: cloud (Prisma Access) and management (Panorama, Cloud Management) platforms running any software version with the Panorama plugin.

The Directory Sources Supported for User- and Group-Based Policy Across Palo Alto Networks Products

	Prisma Access	Prisma Access Cloud Management	NGFW (PA/VM/CN-Series) OS Requirements	Panorama OS Requirements
Microsoft AD	Available via Panorama plugin	Available	PAN-OS 10.1 and above	PAN-OS 10.1 and above
Azure AD	Available via Panorama plugin	Available	PAN-OS 10.1 and above	PAN-OS 10.1 and above
Okta	Available via Panorama plugin	Available	PAN-OS 10.1 and above	PAN-OS 10.1 and above
Google	Not Available	Not Available	PAN-OS 10.1 and above	PAN-OS 10.1 and above

Note: Users have the option to connect to Azure AD using Graph APIs or the SCIM protocol.

Identity Providers (IdPs) Supported for Cloud Authentication (SAML) Across Palo Alto Networks Products

	NGFW (HW/VM/CN-Series) OS Requirements	Panorama OS Requirements
Azure	PAN-OS 10.1 and above	PAN-OS 10.1 and above
PingID	PAN-OS 10.1 and above	PAN-OS 10.1 and above
Okta	PAN-OS 10.1 and above	PAN-OS 10.1 and above
Google	PAN-OS 10.1 and above	PAN-OS 10.1 and above
Other SAML 2.0 IdPs	PAN-OS 10.1 and above	PAN-OS 10.1 and above

Note: Starting with PAN-OS 10.2, connect with two or more SSO/MFA providers via a single GlobalProtect/Authentication Portal/Admin login

Visibility into Users and Groups for Security	Determine user behavior to correlate threats to users on Cortex XDR, SaaS Inline, Device Insights, ADEM, CDL, Explore, Visualization and Reporting) to correlate threats and prevent data loss.
Time to Configure New Identity Provider	~10 minutes
Connection with Directories	Cloud Identity Engine connects with on-premises and cloud directories, offering the granularity needed to provide real-time, user-based security policy that continuously updates to match your identity stores. This optimizes our implementation to provide group-based policy in the most efficient manner by only updating the changes that have occurred rather than continuously synchronizing the entire AD structure. Users have the option to connect to Azure AD using Graph APIs or the SCIM protocol.
Recommended for	1. User and group-based policies 2. Authentication on Palo Alto Networks Next-Generation Firewalls
Global Deployment	Cloud Identity Engine is a global deployment available in 10 Global locations: Australia, Canada, Europe (Netherlands), Germany, India, Japan, Singapore, UK, United States, and United States FedRamp.
Availability and Licensing	Cloud Identity Engine is available through the Palo Alto Networks Apps Hub and does not require a license.

To learn more, check out the following resources:

- Cloud Identity Engine Demo
- Cloud Identity Engine Lightboard: Simplify Zero Trust for User-Based Security
- Cloud Identity Engine System Requirements
- Set Up the Cloud Identity Engine
- Cloud Identity Engine Privacy Datasheet
- Cloud Identity Engine LIVEcommunity to ask questions and see FAQs
- Best Practice Assessment: This complimentary assessment helps you maximize the capabilities of your NGFW, such as identity-based security controls to prevent successful cyberattacks.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com