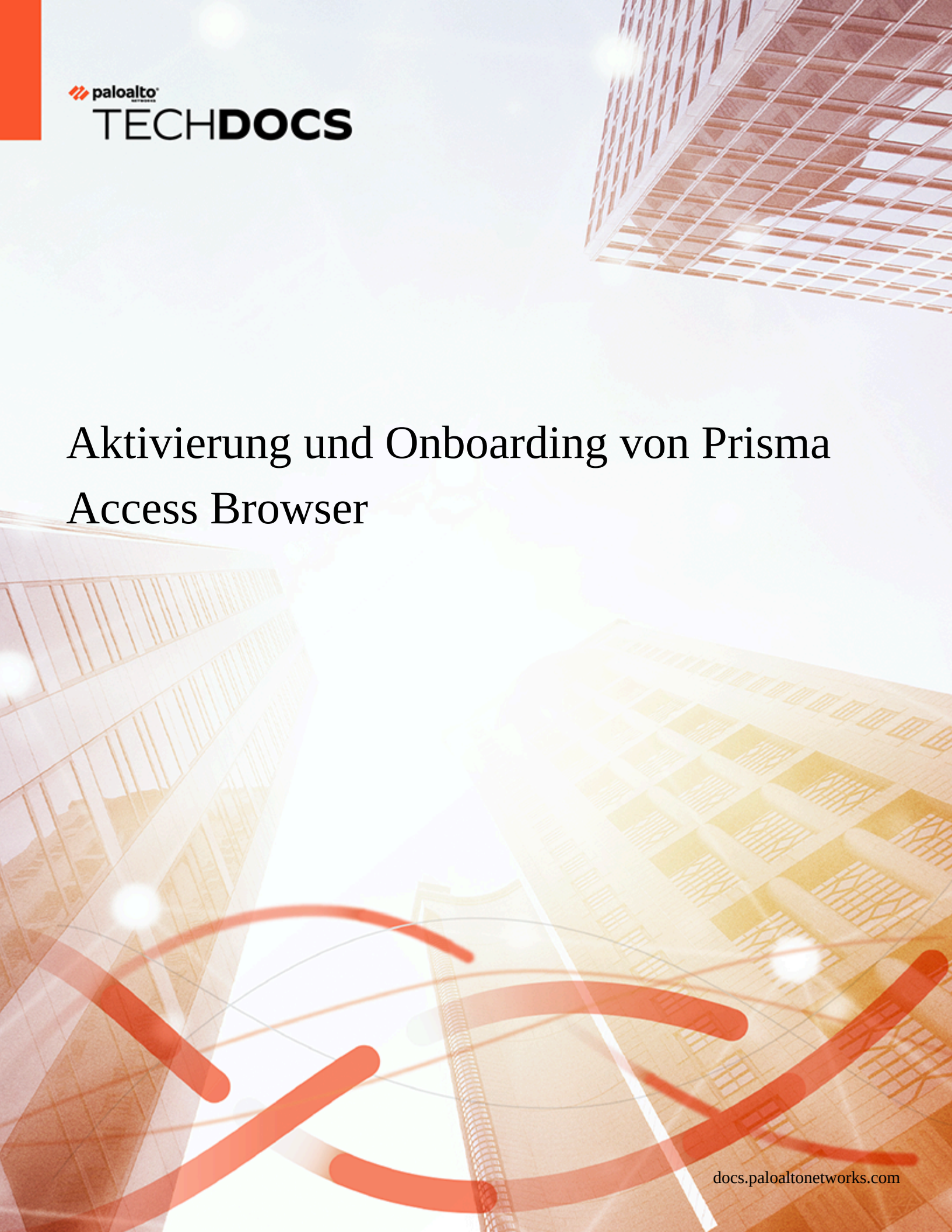
paloalto TECHDOCS

Aktivierung und Onboarding von Prisma Access Browser



Contact Information

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

About the Documentation

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

Copyright

Last Revised

July 15, 2024

Table of Contents

Neuen Prisma Access Browser mit der Bundle-Lizenz für Prisma Access Enterprise aktivieren

Wo kann ich das verwenden?	Was brauche ich?
• Strata Cloud Manager • Panorama	• Aktivierungslink für Ihr Produkt • Für die Aktivierung wird der Strata-Protokollierungsdienst (Strata Logging Service, SLS) benötigt • Cloud Identity Engine (CIE) ist enthalten und wird während der Aktivierung gestartet • Konto beim Customer Support Portal (CSP)

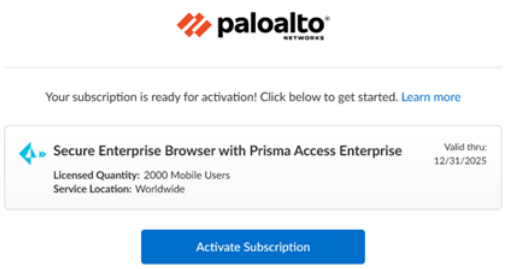
Informieren Sie sich vor dem Ausführen dieser Aufgabe über die Voraussetzungen.

- Cloud
- Panorama

Bundle-Lizenz für von der Cloud verwalteten Prisma Access Browser

Nachdem Sie von Palo Alto Networks eine E-Mail zur Identifizierung der zu aktivierenden Lizenz erhalten haben, starten Sie den Aktivierungsvorgang mithilfe des Aktivierungslinks.

STEP 1 | Wählen Sie in Ihrer E-Mail **Abonnement aktivieren** aus.



STEP 2 | Folgen Sie den Anweisungen zur Aktivierung einer Prisma Access-Lizenz, zur Zuweisung einer Prisma Access-Lizenz und zur Planung von Dienstverbindungen.

STEP 3 | Fahren Sie mit der Zuweisung der Lizenzen und Add-ons für Prisma Access Secure Enterprise Browser fort. **Produkte** oder **Add-ons** sind auf der Grundlage Ihres Vertrags standardmäßig aktiviert.

STEP 4 | Wählen Sie den **Secure Enterprise Browser mit Prisma Access Enterprise** aus.

Dies ist vergleichbar mit der Zuweisung von PA-Lizenzen für mobile Benutzer. Sie können Prisma Access Browser-Lizenzen mehreren Prisma Access-Mandanten teilweise zuweisen und aktivieren. Beispiel:

- Sie können 5.000 Einheiten von Prisma Access Browser Enterprise für mobile Benutzer erwerben.
- Diese können Sie wie folgt zuweisen:
  - 1.000 Einheiten für einen PoC-Mandanten (dies ist die erforderliche Mindestmenge)
  - 3.000 Einheiten für einen Produktionsmandanten
  - Lassen Sie 1.000 Einheiten für die spätere Verwendung inaktiviert

STEP 5 | Im Prisma Access Browser Administratorhandbuch finden Sie weitere Informationen zur Verwaltung von Prisma Access Browser.

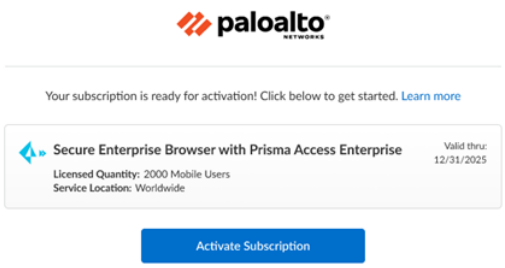
STEP 6 | (Optional) Weisen Sie Rollen zu, damit Ihre Administratoren Prisma Access Browser verwalten können.

Bundle-Lizenz für von Panorama verwalteten Prisma Access Browser

Nachdem Sie von Palo Alto Networks eine E-Mail zur Identifizierung der zu aktivierenden Lizenz erhalten haben, starten Sie den Aktivierungsvorgang mithilfe des Aktivierungslinks.

Nicht für Panorama mit mehreren Mandanten verfügbar.

STEP 1 | Wählen Sie in Ihrer E-Mail **Abonnement aktivieren** aus.



STEP 2 | Befolgen Sie die Anweisungen zum Aktivieren einer Lizenz für Prisma Access (verwaltet von Panorama).

STEP 3 | Fahren Sie mit der Aktivierung der verfügbaren Add-ons fort. **Produkte** oder **Add-ons** sind auf der Grundlage Ihres Vertrags standardmäßig aktiviert.

STEP 4 | Wählen Sie den **Secure Enterprise Browser mit Prisma Access Enterprise** aus.

STEP 5 | Wechseln Sie in Panorama auf die Registerkarte **Panorama** > **Prisma Access Browser-Registerkarte** > **Cloud Services-Plug-in**.

Dadurch wird eine neue Registerkarte mit einer eingeschränkten Version von Strata Cloud Manager geöffnet, die nur die Prisma Access Browser-spezifischen Ansichten enthält.

STEP 6 | Im Prisma Access Browser Administratorhandbuch finden Sie weitere Informationen zur Verwaltung von Prisma Access Browser.

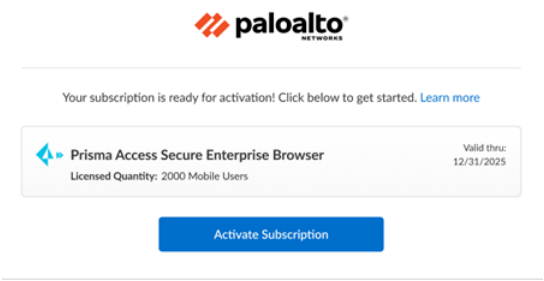
STEP 7 | (Optional) Weisen Sie Rollen zu, damit Ihre Administratoren Prisma Access Browser verwalten können.

Aktivieren der Lizenz für Standalone Prisma Access Browser

Wo kann ich das verwenden?	Was brauche ich?
• Strata Cloud Manager	• Aktivierungslink für Ihr Produkt • Cloud Identity Engine (CIE) ist enthalten und wird während der Aktivierung gestartet • Konto beim Customer Support Portal (CSP)

Informieren Sie sich vor dem Ausführen dieser Aufgabe über die Voraussetzungen.

Nachdem Sie von Palo Alto Networks eine E-Mail zur Identifizierung der zu aktivierenden Lizenz erhalten haben, starten Sie den Aktivierungsvorgang mithilfe des Aktivierungslinks.



STEP 1 | Melden Sie sich mit Ihrer E-Mail-Adresse an.

- Wenn Sie ein Konto beim Palo Alto Networks-Customer Support Portal haben, geben Sie die E-Mail-Adresse ein, die Sie bei der Registrierung für dieses Konto verwendet haben, und wählen Sie **Weiter** aus.
- Wenn Sie kein Konto beim Palo Alto Networks-Kundensupport haben, **erstellen Sie ein neues Konto** > **Passwort** > **Weiter** aus.

Der Dienst verwendet diese E-Mail-Adresse für das Benutzerkonto, das dem Mandanten zugewiesen ist, den Sie für diese Lizenz verwenden. Diesem Mandanten und allen anderen, die mit dieser E-Mail-Adresse erstellt wurden, wird die Rolle `Superuser` zugewiesen.

STEP 2 | Wenn mit Ihrem Benutzernamen nur ein Konto beim Customer Support Portal verknüpft ist, ist das **Konto beim Kundensupport** vorab ausgefüllt.

Wenn Sie mehr als ein Konto beim Customer Support Portal haben, müssen Sie mit einem anderen Verhalten rechnen.

STEP 3 | Ordnen Sie das Produkt dem **Empfänger** Ihrer Wahl zu.

Der angegebene Name ist der Einfachheit halber derselbe wie für Ihr Konto beim Customer Support Portal. Sie können den angegebenen Namen verwenden oder ihn ändern.

STEP 4 | Wählen Sie die Datenerfassungs-**Region** aus, in der Sie Ihr Produkt bereitstellen möchten.

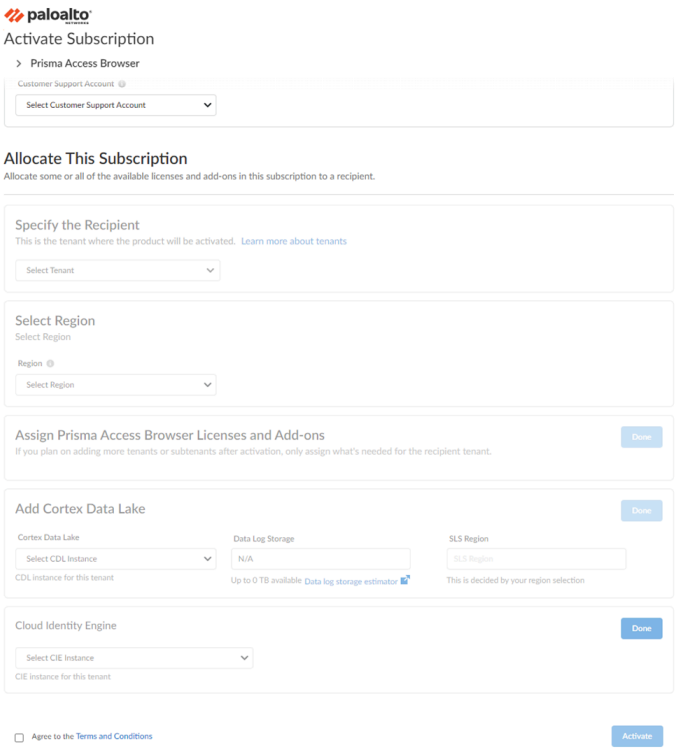
STEP 5 | Ordnen Sie die Prisma Access Secure Enterprise Browser-Lizenzen und -Add-ons zu

1. Wählen Sie **Prisma Access Secure Enterprise Browser** aus.
2. Dies ist vergleichbar mit der Zuweisung von PA-Lizenzen für mobile Benutzer. Sie können Prisma Access Browser-Lizenzen mehreren Prisma Access-Mandanten teilweise zuweisen und aktivieren. Beispiel:
   - Sie können 1.000 Einheiten von Standalone Prisma Access Browser erwerben
   - Diese können Sie wie folgt zuweisen:
     - 200 für einen PoC-Mandanten (dies ist die erforderliche Mindestmenge)
     - 600 für einen Produktionsmandanten
     - Lassen Sie 200 Einheiten für die spätere Verwendung inaktiviert

STEP 6 | Fügen Sie Strata Logging Service (früher Cortex Data Lake) zum Speichern von Mandantendaten (z. B. Konfiguration, Telemetrieprotokolle, Systemprotokolle und Statistiken) hinzu. Sie können eine vorhandene Instanz auswählen oder eine neue Instanz erstellen.

STEP 7 | Wählen Sie Cloud Identity Engine aus oder erstellen Sie eine neue CIE-Instanz, um alle Benutzer in Ihrer Infrastruktur zu identifizieren und zu verifizieren.

STEP 8 | **Stimmen Sie den allgemeinen Geschäftsbedingungen zu** und wählen Sie **Aktivieren** aus.



STEP 9 | Im Prisma Access Browser Administratorhandbuch finden Sie weitere Informationen zur Verwaltung von Prisma Access Browser.

STEP 10 | (Optional) Weisen Sie Rollen zu, damit Ihre Administratoren Prisma Access Browser verwalten können.

Onboarding von Prisma Access Browser in die Strata Cloud Manager

Wo kann ich das verwenden?	Was brauche ich?
• Strata Cloud Manager	❑ Prisma Access mit Bundle-Lizenz für Prisma Access Browser ❑ Superuser- oder Prisma Access Browser-Rolle

Informieren Sie sich vor dem Ausführen dieser Aufgabe über die Voraussetzungen.

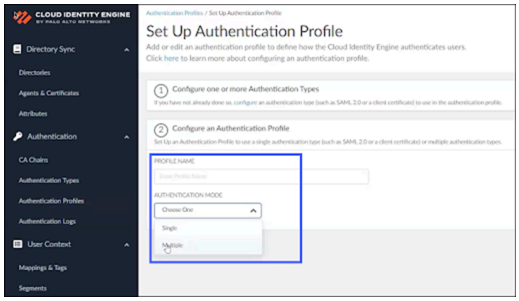
Abschließen der Aufgaben zur Vorbereitung des Onboardings

Vor dem Onboarding von Prisma Access Browser müssen Sie zunächst einige Aufgaben abschließen.

STEP 1 | Definieren Sie die Cloud Identity Engine-Entitäten. Diese können Sie mithilfe der Cloud Identity Engine konfigurieren, die Sie während der Aktivierung ausgewählt haben.

STEP 2 | Sie benötigen das Authentifizierungsprofil und die Benutzergruppen, die Teil Ihres Onboarding-Prozesses sind. Diese werden in der Cloud Identity Engine konfiguriert. Weitere Informationen finden Sie unter Authentifizierungsprofil und Benutzergruppen.

Sie können nur ein Authentifizierungsprofil haben. Wenn Sie mehr als einen Identitätsanbieter (IdP) verwenden, können Sie mehrere IdPs pro Profil konfigurieren. Verwenden Sie hierfür beim Konfigurieren des Authentifizierungsprofils für die Auswahl ***Authentifizierungsmodus*** *die Einstellung* ***Mehrere****.*

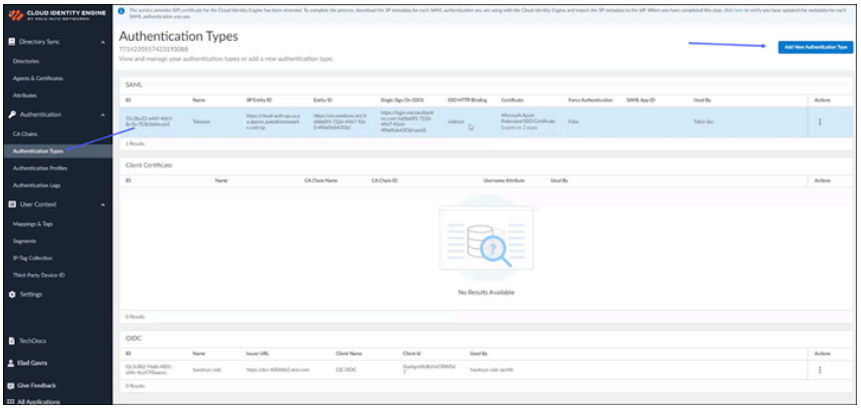


Hinzufügen der IdP-Konfiguration

Sie können Ihren derzeitigen SAML-IDP-Anbieter verwenden, um einen einzelnen Satz mit Anmeldeinformationen in Ihrem Netzwerk zu verwalten. Die IdP-Konfiguration ist eine Komponente der Cloud Identity Engine, die Sie innerhalb dieses Tools verwalten können.

STEP 1 | Wählen Sie in der Cloud Identity Engine die Option **Authentifizierungstyp** aus.

STEP 2 | Klicken Sie auf **Neuen Authentifizierungstyp hinzufügen**.



Wenn Sie zum Ausfüllen Ihrer Benutzergruppen die Informationen des IdP-Anbieters verwenden, müssen Sie sicherstellen, dass Sie eine gültige E-Mail-Adresse korrekt eingeben. Der UPN reicht nicht aus.

STEP 3 | Klicken Sie in „Authentifizierungstyp einrichten“ auf „SAML 2.0 **einrichten**“.

STEP 4 | Weitere Informationen zum Konfigurieren Ihres SAML-Authentifizierungsprogramms finden Sie unter Konfigurieren eines SAML 2.0-Authentifizierungstyps in der Cloud Identity Engine.

STEP 5 | (Optional) Verwenden Sie Google Workspace Integration.

Onboarding von Prisma Access Browser

Nachdem Sie die Schritte zur Vorbereitung des Onboardings durchgeführt haben, können Sie Prisma Access Browser in die Strata Cloud Manager einbinden.

Sie müssen Prisma Access Browser in der Strata Cloud Manager aktivieren und konfigurieren, bevor Sie Benutzer hinzufügen können. In der Regel ist dies ein einmaliger Vorgang, der nur einmal nach der Aktivierung erforderlich ist. Sie können jedoch jederzeit zurückkehren, um diese Aufgaben auszuführen, falls Änderungen erforderlich sind.

Für diesen Prozess steht Ihnen ein Assistent zur Verfügung. Außerdem können Sie die globale Konfiguration jederzeit ändern. Der Assistent bietet detaillierte Anweisungen zur Ausführung der einzelnen Integrationsschritte.

Welche Steuerelemente angezeigt werden, hängt von Ihrer Prisma Access Browser-Lizenz ab. Es sind nicht alle Onboarding-Funktionen der Strata Cloud Manager für alle Lizenzen verfügbar.

Wählen Sie in der Strata Cloud Manager die Optionen **Workflows** > **Einrichtung Prisma Access** > **Prisma Access Browser** aus.

Schritt 1 – Benutzer

Definieren Sie die Benutzerauthentifizierungsmethode und binden Sie Benutzergruppen ein.

STEP 1 | Wählen Sie in der Dropdown-Liste das **CIE-Profil aus, das für die Benutzerauthentifizierung verwendet werden soll**.

STEP 2 | Wählen Sie in der Dropdown-Liste „Benutzergruppen“ die **Benutzergruppen** aus, die Zugriff auf Prisma Access Browser erhalten sollen.

STEP 3 | **Nächster Schritt: Prisma Access-Integration**.

Schritt 2 – Prisma Access-Integration

STEP 1 | Aktivieren Sie externe Verbindungen zu Prisma Access.

1. Wählen Sie **Zu Einstellungen für expliziten Proxy gehen** aus.
2. Dadurch gelangen Sie zu **Workflows** > **Einrichtung Prisma Access** > **Expliziter Proxy** .
3. Aktivieren Sie Prisma Access Browser.
4. **Fertig**.

STEP 2 | Lassen Sie Prisma Access Browser in der Prisma Access-Sicherheitsrichtlinie zu.

1. Wählen Sie **Verwalten > Prisma Access > Sicherheitsrichtlinie** aus.
2. Dadurch gelangen Sie zu **Verwalten** > **Prisma Access** > **Sicherheitsrichtlinie**.
3. Fügen Sie eine Regel hinzu, die Webdatenverkehr in Ihrer Sicherheitsrichtlinie zulässt.
4. Übertragen Sie die Konfiguration per Push, um die Regel zu akzeptieren.
5. **Fertig**.

STEP 3 | Erstellen Sie eine Dienstverbindung.

1. Wählen Sie **Dienstverbindung erstellen** aus.
2. Dadurch gelangen Sie zu **Workflows** > **Einrichtung Prisma Access** > **Dienstverbindungen** und **Dienstverbindung hinzufügen**.
3. **Fertig**.
4. **Nächster Schritt: Routing.**

Schritt 3 – Routing

Mit dem Steuerelement „Routing“ können Sie verwalten, wie Netzwerkverkehr in Prisma Access Browser behandelt wird. Diese Funktion dient zum Einrichten der Standardkonfiguration für Prisma Access Browser. Wenn Sie die Details des Steuerelements für eine bestimmte Regel anpassen müssen, finden Sie unter Steuerelemente zur Browseranpassung weitere Informationen zu Datenverkehrsflüssen.

STEP 1 | Wählen Sie eine der folgenden Optionen aus:

- **Nur privaten Anwendungsverkehr über Prisma Access weiterleiten**.
- **Gesamten Verkehr über Prisma Access weiterleiten**.

STEP 2 | (Optional) Stellen Sie sicher, dass der Prisma Access Browser-Datenverkehr optimal fließt, wenn der Browser erkennt, dass er im internen Netzwerk ausgeführt wird. Diese Identifikation basiert auf dem Aufbau einer Verbindung mit einem Host, der nur innerhalb des internen Netzwerks verfügbar ist.

- Geben Sie den FQDN zur Auflösung ein.
- Geben Sie die erwartete IP-Adresse ein.

STEP 3 | **Nächster Schritt: Durchsetzung von SSO-Anwendungen**.

Schritt 4 – Durchsetzen von SSO-Anwendungen

Es ist wichtig, dass sich Ihre Benutzer ausschließlich mit Prisma Access Browser bei SSO-fähigen Anwendungen authentifizieren können. Dadurch wird sichergestellt, dass externe Akteure keinen Zugriff auf Ihre Unternehmensanwendungen haben. So wählen Sie Ihren Identitätsanbieter (IdP) aus:

STEP 1 | Wählen Sie in „Identitätsanbieter auswählen und konfigurieren“ den verfügbaren IdP aus. Die Optionen sind:

- Okta
- Microsoft Azure Active Directory
- PingID
- OneLogin
- VMware Workspace ONE Access

STEP 2 | Beachten Sie bei der Konfiguration Ihrer lokalen Einstellungen unbedingt die Ausgangs-IP-Adressen.

STEP 3 | **Nächster Schritt: Herunterladen und verteilen.**

Schritt 5 – Herunterladen und verteilen

Sie können die Prisma Access Browser-Installationsdateien herunterladen, um sie auf Ihrem eigenen Gerät zu testen, bevor Sie sie an Ihre Benutzer senden. Sobald Sie mit Ihren Tests zufrieden sind, können Sie das entsprechende Installationsprogramm herunterladen, das von Ihrer Mobile Device Management-(MDM-)Anwendung verteilt werden soll.

Sie können Ihren Benutzern auch den Download-Link senden, damit sie Prisma Access Browser selbst herunterladen können. Dies ist ein einzelner Link nur für macOS- und Windows-Benutzer.

STEP 1 | Treffen Sie Ihre Wahl aus den verfügbaren Optionen:

- Desktop:
  - macOS
  - Windows
- Mobiltelefon:
  - iOS
  - Android

Sie können Ihren Benutzern auch den Download-Link senden, damit sie Prisma Access Browser selbst herunterladen können. Dies ist ein einzelner Link nur für macOS- und Windows-Benutzer.

Wenn Sie Ihren Benutzern den Download-Link senden, erinnern Sie sie daran, dass sie sich nur mit der E-Mail anmelden können, die im IdP-Dienst konfiguriert ist.

STEP 2 | **Nächster Schritt: Browserrichtlinie**.

Schritt 6 – Browserrichtlinie

Sie können nun beginnen, sich mit der Richtlinien-Engine von Prisma Access Browser vertraut zu machen und diese zu konfigurieren, um eine sichere Benutzerumgebung zu schaffen.

STEP 1 | Wählen Sie **Browserrichtlinie** aus.

STEP 2 | Dadurch gelangen Sie zu **Verwalten** > **Konfiguration** > **Prisma Access Browser** > **Richtlinie** > **Regeln**.

STEP 3 | Verwalten Sie die Richtlinienregeln für Prisma Access Browser.

Onboarding neuer Benutzer

Der Onboarding-Workflow umfasst eine konfigurierbare Reihe von Fenstern, die angezeigt werden, wenn ein neuer Endbenutzer den Browser zum ersten Mal verwendet.

Je nach IT-Bedarf und Anforderungen können Sie bis zu acht einzelne Seiten auswählen, über die die Endbenutzer den Browser mit ihren Bildern und Lesezeichen anpassen und einige grundlegende Informationen über den Browser abrufen können – also eine Art „Schnellstart“-Anleitung.

Über das Anpassungs-Steuerelement des Onboarding-Assistenten können Sie den Onboarding-Workflow konfigurieren. Sie können auswählen, welche Fenster in Ihrem Netzwerk angezeigt werden.

Sie konfigurieren dies unter **Verwalten** > **Konfiguration** > **Prisma Access Browser** > **Richtlinie** > **Profile**, wenn Sie ein Profil zur **Browseranpassung** erstellen oder bearbeiten und **Onboarding-Assistent** auswählen. Weitere Konfigurationsdetails finden Sie in den Informationen zu den Steuerelementen zur Browseranpassung für den Onboarding-Assistenten.

Zuweisen von Prisma Access Browser-Rollen

Wo kann ich das verwenden?	Was brauche ich?
• Strata Cloud Manager	❑ Prisma Access mit Bundle-Lizenz für Prisma Access Browser oder Standalone-Lizenz für Prisma Access Browser ❑ Rolle: Superuser für mehrere Mandanten oder Superuser mit Zugriff auf das Customer Support Portal

Sie können eine rollenbasierte Zugriffssteuerung für verschiedene Arten von Prisma Access Browser-Administratoren erstellen und verwalten. Auf diese Weise kann der Hauptadministrator in einer großen Organisation zusätzliche Administratoren mit den entsprechenden Berechtigungen für ihre jeweiligen Rollen, einschließlich Sichtbarkeit und Zugriff, ernennen.

Nach der Aktivierung Ihrer Lizenz können Sie den Administratorbenutzerzugriff verwalten und eine der folgenden Prisma Access Browser-spezifischen Rollen zuweisen:

Rollen im Unternehmen	Berechtigungen	Unterstützte Anwendungen
Zugriffs- und Datenadministrator für PA Browser	Lese- und Schreibzugriff zum Festlegen und Verwalten von Zugriffs- und Datenrichtlinien, Definieren benutzerdefinierter oder privater Anwendungen, Bearbeiten von Endbenutzeranfragen in Bezug auf Richtlinien und Leseberechtigung für Inventaraspekte (Benutzer, Geräte, Erweiterungen) und Sichtbarkeitsaspekte (Dashboards, Endbenutzerereignisse) in den Verwaltungsabschnitten von Prisma Access Browser	• Prisma Access Browser
Administrator zur Anpassung von PA Browser	Lese- und Schreibzugriff zum Festlegen und Verwalten von Richtlinien zur Browseranpassung sowie Leseberechtigungen für Inventaraspekte (Benutzer, Geräte, Anwendungen, Erweiterungen) und alle Sichtbarkeitsaspekte (Dashboards, Endbenutzerereignisse) in den Verwaltungsabschnitten von Prisma Access Browser.	• Prisma Access Browser
Berechtigungsanforderungsadministrator für PA Browser	Lese- und Schreibzugriff zur Bearbeitung von Endbenutzeranforderungen in Bezug auf Richtlinien und -Leseberechtigungen für Sichtbarkeitsaspekte	• Prisma Access Browser

Rollen im Unternehmen	Berechtigungen	Unterstützte Anwendungen
	(Dashboards, Endbenutzerereignisse) in den Verwaltungsabschnitten von Prisma Access Browser.	
Sicherheitsadministrator für PA Browser	Lese- und Schreibzugriff zum Festlegen und Verwalten von Browser-Sicherheitsrichtlinien sowie Leseberechtigungen für Inventaraspekte (Benutzer, Geräte, Anwendungen, Erweiterungen) und für alle Sichtbarkeitsaspekte (Dashboards, Endbenutzerereignisse) in den Verwaltungsabschnitten von Prisma Access Browser.	• Prisma Access Browser
Sicherheits- und Gerätestatusadministrator für PA Browser	Lese- und Schreibzugriff zum Festlegen und Verwalten von Browser-Sicherheitsrichtlinien, Verwalten von Gerätestatusgruppen und Festlegen von Anmelderegeln. Erteilt auch Leseberechtigungen für Inventaraspekte (Benutzer, Anwendungen, Erweiterungen) und alle Sichtbarkeitsaspekte (Dashboards, Endbenutzerereignisse) in den Verwaltungsabschnitten von Prisma Access Browser.	• Prisma Access Browser
Schreibgeschützte Analysen in PA Browser	Lesezugriff auf alle Sichtbarkeitsaspekte in den Verwaltungsabschnitten von Prisma Access Browser, einschließlich Dashboards, detaillierte Endbenutzerereignisse und Inventaraspekte (Benutzer, Geräte, Anwendungen und Erweiterungen).	• Prisma Access Browser

