paloalto
TECHDOCS

# Erste Schritte mit Strata Cloud Manager

docs.paloaltonetworks.com

### Contact Information

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

### About the Documentation

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

### Copyright



### Last Revised

February 6, 2025

# Table of Contents



# Einführung in Strata Cloud Manager

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden<br>• Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• Prisma SD-WAN | Jede dieser Lizenzen beinhaltet den Zugriff auf Strata Cloud Manager:<br>❑ Prisma Access<br>❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>❑ Prisma SD-WAN<br>❑ Strata Cloud Manager Essentials<br>❑ Strata Cloud Manager Pro<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Palo Alto Networks Strata Cloud Manager ermöglicht Ihnen eine KI-gestützte, einheitliche Verwaltung für Ihre gesamte Netzwerksicherheitsbereitstellung. Mit Strata Cloud Manager können Sie Ihre gesamte Netzwerksicherheitsinfrastruktur von Palo Alto Networks – Ihre NGFWs und SASE-Umgebung – problemlos über eine einzige, optimierte Benutzeroberfläche verwalten. Erhalten Sie umfassende Einblicke in Benutzer, Zweigstellen, Anwendungen und Bedrohungen an allen Durchsetzungspunkten der Netzwerksicherheit. Dadurch erhalten Sie aussagekräftige Erkenntnisse, bessere Sicherheit sowie eine einfache Fehlersuche und Problemlösung.

❑ **Vorhersagen und Verhindern von Netzwerkstörungen**

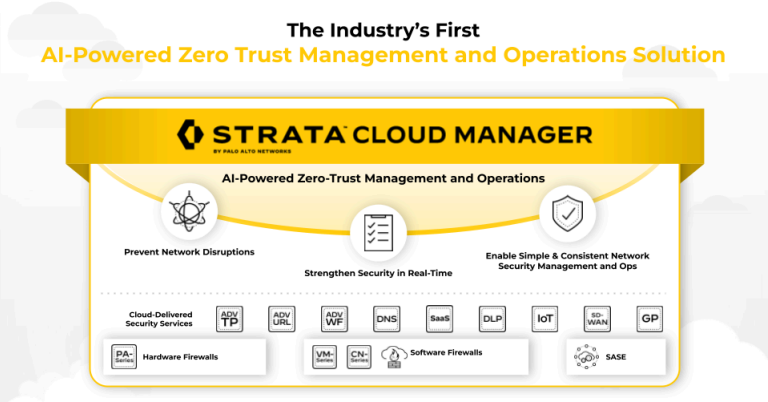
Strata Cloud Manager prognostiziert und verhindert Netzwerkstörungen und behebt Probleme schnell, sodass Sie und Ihre Benutzer ihr Tagesgeschäft fortsetzen und weiter produktiv arbeiten können.

❑ **Gesteigerte Sicherheit dank Echtzeit-Best-Practices**

Strata Cloud Manager identifiziert wichtige und wenig genutzte Sicherheitsfunktionen und unterstützt Sie bei deren Aktivierung – basierend auf Best Practices, die Ihren Anforderungen entsprechen. Stärken Sie Ihren Sicherheitsstatus mit integrierten Best Practices und Inline-Korrekturfunktionen auf Basis von AIOps.

❑ **Einfaches und einheitliches Netzwerksicherheitsmanagement**

Strata Cloud Manager konsolidiert Ihre Sicherheitstools für einen verbesserten Betrieb und bessere Einblicke, sodass Sie eine einfache und einheitliche Verwaltungserfahrung für Ihren gesamten Netzwerksicherheitsstack erreichen können.



# So stärkt Strata Cloud Manager die Sicherheit

**Maximierte Nutzung von Sicherheitsfunktionen**

- Sehen Sie sich die Sicherheitsfunktionen an, die Sie verwenden, und identifizieren Sie Sicherheitsfunktionen, die Sie nicht nutzen, obwohl Sie es könnten. → Funktionsannahme
- Sehen Sie sich die Annahmeraten für Ihre Sicherheitsdienstabonnements an. → Einführung von CDSS
- Sehen Sie, inwieweit Ihre Sicherheitsfunktionen Best Practices entsprechen oder wo Sie Verbesserungen vornehmen können, um Ihren Sicherheitsstatus zu stärken.→ Integrierte Best Practices

**Stärken und Optimieren der bestehenden Konfiguration**

Bereinigen und optimieren Sie Ihre Sicherheitsrichtlinie auf der Grundlage von Nutzungsdaten und automatisch generierten Empfehlungen.

- Bereinigen Sie Objekte, die nicht Teil von Richtlinien und Regeln sind, ohne dass es zu Verkehrsbeeinträchtigungen kommt. Diese Objekte und Regeln können die Leistung beeinträchtigen und die Richtlinienverwaltung erschweren. → Konfigurationsbereinigung
- Zu weit gefasste Regeln führen zu Sicherheitslücken, da sie Anwendungen zulassen, die in Ihrem Netzwerk nicht verwendet werden. Mit der Richtlinienoptimierung können Sie diese unverhältnismäßig toleranten Regeln in spezifischere, fokussiertere Regeln umwandeln, die nur die Anwendungen zulassen, die Sie tatsächlich verwenden. → Richtlinienoptimierer

**Echtzeitanleitung zur sicheren Konfiguration**

- Best-Practice-Leitlinien bieten Ihnen eine Live-Validierung, mit der Sie sicherstellen können, dass Ihre Sicherheitsrichtlinien den Best Practices entsprechen. → Live-Inline-Best-Practice-Konfigurationsprüfungen

# So sagt Strata Cloud Manager Netzwerkstörungen vorher und verhindert sie

**Umfassende Beobachtbarkeit**

- Erfahren Sie, wie Ihr Netzwerk durch die Sicherheitsinfrastruktur geschützt wird. → Command Center
- Informieren Sie sich über den Zustand und die Leistung von Benutzern, Zweigstellen, Anwendungen und der IT-Infrastruktur – alles über

  ein einziges Dashboard. → Dashboard „SASE-Zustand“
- Informieren Sie sich über den Zustand und die Leistung von Geräten über ein einziges Dashboard. → Dashboard „Gerätezustand“

**Zustandsprognose und Störungsbehebung**

Automatische Prognosen beugen potenziellen Störungen vor und wenn Probleme erkannt werden, beschleunigen aussagekräftige Erkenntnisse die Lösung.

- Erhalten Sie maschinengestützte Vorhersagen drohender Ausfälle, mit Empfehlungen für Abhilfemaßnahmen. → Prognosen und Anomalieerkennung
- Reduzieren Sie die Zeit bis zur Lösung mit einer Analyse der wahrscheinlichen Ursachen. → Anzeigen möglicher Ursachen

**Planung für dynamische Sicherheitsanforderungen**

- Verbessern Sie die Stabilität, indem Sie potenzielle Kapazitäten proaktiv identifizieren. → Kapazitätsanalyse

# So funktioniert Strata Cloud Manager überall einheitlich

**Einheitliche Konfiguration**

Wenden Sie mit optimierten Prozessen an allen Durchsetzungspunkten einheitliche Richtlinien an und vermeiden Sie die Notwendigkeit individueller Änderungen für NGFWs und SASE-Bereitstellungen.

- Richten Sie mobile NGFWs und Prisma Access-Benutzer sowie Remote-Netzwerke ein, binden Sie sie ein und planen Sie Software-Upgrades für NGFWs. → Workflows in Strata Cloud Manager
- Konfigurieren Sie eine Sicherheitsrichtlinie, die von Ihren NGFWs und Prisma Access gemeinsam genutzt wird. → Gemeinsame Verwaltung für NGFW und Prisma Access

**Flexible Konfigurationsorganisation**

Vereinfachen Sie das flächendeckende Konfigurationsmanagement mit einfachen Workflows zur Ordner- und Geräteverwaltung.

- Wenden Sie Konfigurationseinstellungen an und setzen Sie Richtlinien global in Ihrer gesamten Umgebung durch oder richten Sie Einstellungen und Richtlinien auf bestimmte Teile Ihrer Organisation aus. → Konfigurationsumfang
- Gruppieren Sie Ihre Firewalls oder Bereitstellungstypen (mobile Prisma Access-Benutzer, Remote-Netzwerke oder Dienstverbindungen) logisch, um die Konfigurationsverwaltung zu vereinfachen. → Ordnerverwaltung
- Gruppieren Sie Konfigurationen, die Sie schnell an Ihre Firewalls oder Bereitstellungen übertragen können. → Snippets
- Sie erhalten auch die nötige Flexibilität, um eindeutige Konfigurationswerte zu berücksichtigen, die geräte- oder bereitstellungsspezifisch sind. → Variablen

**Einheitlicher Überblick über Bedrohungen**

- Erhalten Sie umfassende Transparenz über Netzwerkverkehr, Abonnements, Benutzer, Anwendungen, Netzwerke, Bedrohungen und mehr. → Überwachung
- Erhalten Sie eine interaktive Ansicht der Anwendungen, ION-Geräte, Bedrohungen, Benutzer und Sicherheitsabonnements, die in Ihrem Netzwerk im Einsatz sind. Die Dashboards bieten Einblick in den Zustand, den Sicherheitsstatus und die Aktivitäten Ihrer Bereitstellung und helfen Ihnen, Leistungs- und Sicherheitsprobleme in Ihrem Netzwerk zu verhindern oder zu beheben.→ Dashboards
- Erhalten Sie Berichte zu Netzwerkverkehrsmustern, Bandbreitennutzung, Ihren Sicherheitsabonnementdaten und mehr. Berichte bieten aussagekräftige Einblicke in Ihr Netzwerk, die Sie für Planungs- und Überwachungszwecke verwenden können.→ Berichte

# Produkte, die Strata Cloud Manager unterstützt

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden<br>• Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• Prisma SD-WAN | Jede dieser Lizenzen beinhaltet den Zugriff auf Strata Cloud Manager:<br>❑ Prisma Access<br>❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>❑ Prisma SD-WAN<br>❑ Strata Cloud Manager Essentials<br>❑ Strata Cloud Manager Pro<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Strata Cloud Manager bietet KI-gestütztes, einheitliches Management für Ihre NGFWs und Ihr SASE-Netzwerk. Welche Strata Cloud Manager-Funktionen Ihnen hierbei zur Verfügung stehen, hängt von Ihren Lizenzen ab. Hier sind die nötigen Lizenzen, um in Strata Cloud Manager NGFWs und SASE zu verwalten und Strata Cloud Manager-Netzwerksicherheitsfunktionen freizuschalten.
→ So validieren Sie Ihre Lizenzen

**Table 1:**

| | |
|---|---|
| **Strata Cloud Manager Essentials** | Strata Cloud Manager Essentials bietet Verwaltungs- und Sicherheitsfunktionen, die Ihnen mit folgenden Produkten kostenlos zur Verfügung stehen:<br>• Next-Generation Firewalls (NGFWs)<br>• Prisma Access<br>Der Strata-Protokollierungsdienst ist als optionales Add-on für Strata Cloud Manager Essentials verfügbar.<br>*Strata Cloud Manager Essentials und Strata Cloud Manager Pro können in Kunden-Support-Portal-Konten (Customer Service Portal, CSP) aktiviert werden, die nicht über Folgendes verfügen: Strata-Protokollierungsdienst mit dimensioniertem Speicher, AIOps für NGFW Free bzw. Premium oder Prisma Access.* |

| | |
|---|---|
| **Strata Cloud Manager Pro** | Strata Cloud Manager Pro ist die kostenpflichtige Stufe, die neben allen Funktionen von Strata Cloud Manager Essentials auch erweiterte Funktionen zur Verbesserung des Betriebszustands, zur Vermeidung von Netzwerkstörungen und zur Stärkung des Echtzeit-Sicherheitsstatus sowie Autonomous Digital Experience Management (ADEM) zur Überwachung der Benutzererfahrung umfasst. Strata Cloud Manager Pro umfasst den Strata-Protokollierungsdienst mit einer Protokollaufbewahrung von einem Jahr und mit unbegrenztem Speicherplatz. Das ermöglicht eine zentrale Protokollierung und einen nahtlosen Datenabruf in Ihrer gesamten Bereitstellung. Sie können Strata Cloud Manager Pro für die folgenden Produkte erwerben:<br>• Next-Generation Firewalls (NGFWs)<br>• VM-Series, finanziert durch Software-NGFW-Credits<br>• Prisma Access |
| **AIOps für NGFW Premium** | Bei NGFWs mit einer „AIOps für NGFW Premium“-Lizenz bietet Strata Cloud Manager Ihnen einen Gesamtüberblick über den Zustand und die Sicherheit Ihrer NGFWs und kann proaktive Prüfungen erzwingen, um Sicherheitslücken zu schließen.<br>• **NGFW (Managed by PAN-OS or Panorama)** → Verwenden Sie für PAN-OS- und von Panorama verwaltete NGFWs mit einer „AIOps für NGFW Premium“-Lizenz Strata Cloud Manager, um den Zustand und den Sicherheitsstatus Ihrer Bereitstellung zu überwachen.<br>• **NGFW (Managed by Strata Cloud Manager)** → Mit einer „AIOps für NGFW“-Lizenz können Sie Strata Cloud Manager auch zur **Cloud-Verwaltung für NGFWs** verwenden.<br><br>• *Wenden Sie sich an Ihr Account-Team, um Cloud-Verwaltung für NGFWs mithilfe von Strata Cloud Manager zu aktivieren.*<br>• *Strata Cloud Manager bietet einheitliche Verwaltung und einheitlichen Betrieb ausschließlich für NGFWs, die die „AIOps für NGFW Premium“-Lizenz verwenden. Verwenden Sie weiterhin die AIOps für NGFW Free-App für die in AIOps für NGFW Free eingebundenen NGFWs.* |
| **Software-NGFW-Credits** | Bei der VM-Series, die mit Software-NGFW-Credits finanziert wird, unterstützt Strata Cloud Manager die Funktionen |

| | |
|---|---|
| | von AIOps für NGFW Premium, einschließlich der Cloud-Verwaltung für NGFWs. |
| **Prisma Access** | Es gibt zwei Möglichkeiten, Prisma Access zu verwalten: Strata Cloud Manager oder Panorama. Strata Cloud Manager bietet Sichtbarkeitsfunktionen von Prisma Access, die unabhängig von der verwendeten Verwaltungsschnittstelle unterstützt werden. Selbst wenn Sie Panorama zur Verwaltung von Prisma Access verwenden, können Sie also weiterhin Strata Cloud Manager zur umfassenden Überwachung der Prisma Access-Umgebung nutzen.<br><br>**Prisma Access (Managed by Strata Cloud Manager)**<br><br>Verwenden Sie Strata Cloud Manager für das vollständige Onboarding, die Verwaltung und Überwachung Ihrer Prisma Access-Umgebung.<br><br>Dazu gehört die Verwendung von Strata Cloud Manager, um die in Prisma Access enthaltenen cloudbasierten Sicherheitsdienste zu verwalten und zu überwachen.<br><br>Strata Cloud Manager bietet Ihnen umfassende Überwachung, Benachrichtigungen sowie Einblicke in Ihre Prisma Access-Umgebung:<br>• KI-gestütztes Autonomous DEM<br>• Überwachung von Prisma Access in Strata Cloud Manager<br>• Strata Cloud Manager-Dashboards<br>• Strata Cloud Manager-Überwachung<br>• Strata Cloud Manager-Berichte<br><br>**Prisma Access (Managed by Panorama)**<br><br>Wenn Sie Panorama zur Verwaltung von Prisma Access verwenden, müssen Sie es auch weiterhin zur Verwaltung Ihrer Umgebung verwenden. Sie können jedoch Strata Cloud Manager für umfassende Überwachung, Benachrichtigungen und Einblicke in Ihre Prisma Access-Umgebung verwenden:<br>• KI-gestütztes Autonomous DEM<br>• Überwachung von Prisma Access in Strata Cloud Manager<br>• Strata Cloud Manager-Dashboards<br>• Strata Cloud Manager-Überwachung<br>• Strata Cloud Manager-Berichte |
| **KI-gestütztes ADEM** | KI-gestütztes ADEM ist eine Zusatzlizenz von Prisma Access, die komplexe IT-Vorgänge automatisiert, um die Produktivität zu steigern und die Zeit zur Problemlösung zu verkürzen. |

| | |
|---|---|
| | Strata Cloud Manager unterstützt KI-gestütztes ADEM für alle Prisma Access-Benutzer (sowohl Panorama-verwaltetes Prisma Access als auch Prisma Access Cloud Management).<br><br>*Wenn Sie Panorama zur Verwaltung von Prisma Access verwenden, müssen Sie es auch weiterhin zur Verwaltung Ihrer Umgebung verwenden. Sie können jedoch Strata Cloud Manager zur ADEM-Überwachung nutzen.* |
| **Prisma SD-WAN** | Verwenden Sie Strata Cloud Manager für Prisma SD-WAN. Prisma SD-WAN ist ein cloudbasierter Dienst, der App-definiertes, autonomes SD-WAN implementiert, um Ihnen dabei zu helfen, Ihre Zweigstellen, Rechenzentren und großen Campus-Standorte zu schützen und zu verbinden, ohne hierdurch Kosten oder Komplexität zu erhöhen. Das AppFabric verbindet Ihre Standorte sicher, erkennt Anwendungen und gibt Ihnen die Freiheit, jedes WAN und jede Cloud zu verwenden, um eine Thin-Branch-Lösung (Sicherheit aus der Cloud) aufzubauen. |
| **Cloud Delivered Security Services (CDSS)**<br>• **Fortschrittliche Bedrohungsabwehr**<br>• **Erweiterte URL-Filterung**<br>• **Advanced WildFire**<br>• **DNS Security**<br>• **Enterprise DLP**<br>• **IoT Security**<br>• **SaaS-Sicherheit** | Wenn Sie entweder eine Prisma Access- oder AIOps für NGFW Premium-Lizenz haben, können Sie Strata Cloud Manager verwenden, um Ihre Sicherheitsabonnements zu verwalten und zu überwachen. Strata Cloud Manager stellt den Schutz, den Ihre Sicherheitsabonnements bieten, durchgängig für Ihren gesamten Unternehmensdatenverkehr bereit.<br><br>Welche Strata Cloud Manager-Funktionen Ihnen für Sicherheitsabonnements zur Verfügung stehen, hängt von Ihrer Lizenz ab. Sie können Folgendes umfassen:<br>• Strata Cloud Manager-Dashboards und -Berichte für Sicherheitsabonnements<br>• einheitliche Strata Cloud Manager-Verwaltung für Sicherheitsabonnements. Wenn Sie Strata Cloud Manager verwenden, um eine gemeinsame Sicherheitsrichtlinie für alle NGFWs und/oder Prisma Access-Bereitstellungen durchzusetzen, können Sie eine einzige, zentrale Konfiguration für Ihre Sicherheitsabonnements verwenden. |

# Erster Blick auf Strata Cloud Manager

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden<br>• Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• Prisma SD-WAN | Jede dieser Lizenzen beinhaltet den Zugriff auf Strata Cloud Manager:<br>❑ Prisma Access<br>❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>❑ Prisma SD-WAN<br>❑ Strata Cloud Manager Essentials<br>❑ Strata Cloud Manager Pro<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Hier erhalten Sie einen ersten Blick auf Strata Cloud Manager. Die Strata Cloud Manager-Benutzeroberfläche bietet eine umfassende Ansicht Ihres Netzwerks und ermöglicht einen einheitlichen Workflow zur Verwaltung von NGFWs und SASE. Nutzen Sie die neue, vereinfachte und einheitliche Navigation, um mit all Ihren Netzwerkdaten zu interagieren, um automatisch angezeigte, umsetzbare Erkenntnisse zu erhalten und um Prisma Access, Ihre NGFWs und Ihre cloudbasierten Sicherheitsdienste gemeinsam zu verwalten und zu überwachen.

Erkunden Sie jedes Menü in der linken Navigationsleiste – diese Pfade sind jetzt Standard für alle Produkte oder Abonnements von Palo Alto Networks, die Sie mit Strata Cloud Manager verwenden. Das erleichtert Folgendes:

- Einführung neuer Funktionen und Abonnements
- Onboarding neuer Benutzer, Geräte oder Standorte

– denn sie fügen sich direkt in Ihr vorhandenes Verwaltungssetup ein.

***Wichtig***

*Welche Funktionen Ihnen in Strata Cloud Manager zur Verfügung stehen, hängt von Ihren Abonnements ab. In der Strata Cloud Manager-Dokumentation finden Sie alle Lizenzanforderungen für Strata Cloud Manager-Funktionen.*

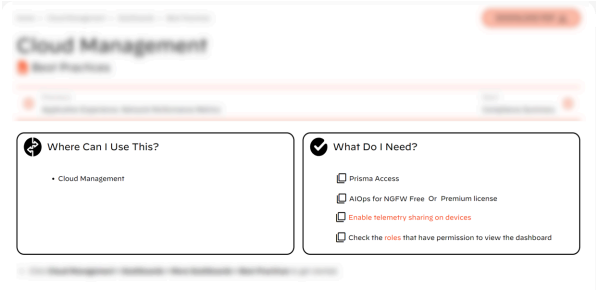
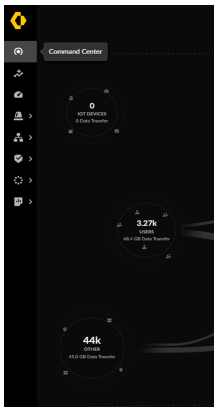
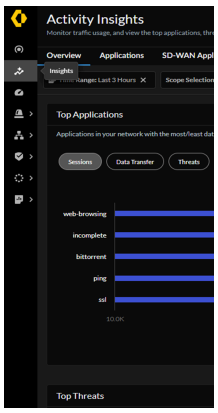
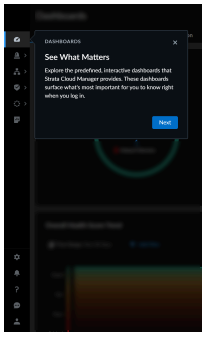
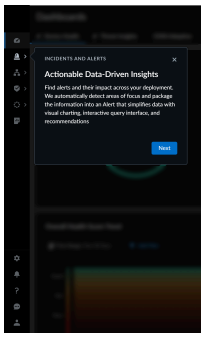
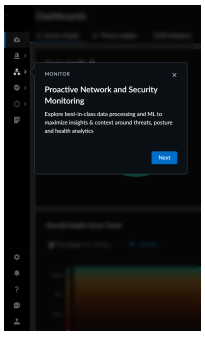


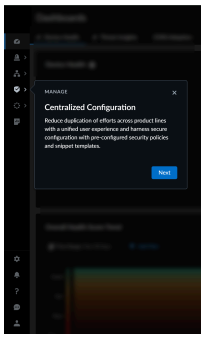
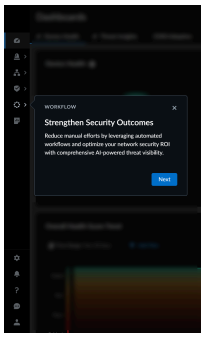

**Table 2:**

| | | |
|---|---|---|
| **Command Center** | **Ihre erste Anlaufstelle zur Beurteilung der Integrität, Sicherheit und Effizienz Ihres Netzwerks**<br><br>Das Command Center ist eine visualisierte Übersicht Ihrer Netzwerk- und Sicherheitsinfrastruktur. Es bietet Ihnen vier verschiedene Ansichten, jede mit ihren eigenen erfassten Daten, Metriken und aussagekräftigen Einblicken, die Sie untersuchen können.<br><br>• Command Center: Strata Cloud Manager |  |
| **Activity Insights** | **Einheitliche Netzwerkdaten, alle an einem Ort**<br><br>Activity Insights gibt Ihnen einen detaillierten Überblick über Ihre Netzwerkaktivitäten in Prisma Access- und NGFW-Bereitstellungen. Activity Insights vereint Ihre Netzwerkdaten an einem Ort, darunter Netzwerkverkehr, Anwendungsnutzung, Bedrohungen und Benutzeraktivitäten.<br><br>• Insights: Activity Insights |  |

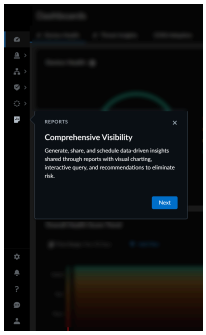
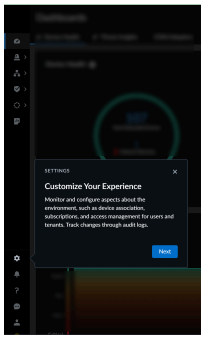
 

| | | |
|---|---|---|
| **Dashboards** | **Sehen Sie sofort, was wichtig ist**<br><br>Direkt nach der Anmeldung werden Ihnen in den Dashboards die wichtigsten Informationen angezeigt. Jedes Dashboard ist so konzipiert, dass es Bereiche hervorhebt, in denen Sie Maßnahmen ergreifen können, um Ihren Sicherheitsstatus oder Ihre Netzwerkintegrität zu verbessern.<br><br>Erkunden Sie alle bereitgestellten vordefinierten, interaktiven Dashboards und heften Sie Ihre Favoriten an.<br><br>• Dashboards: Strata Cloud Manager |  |
| **Vorfälle und Benachrichtigungen** | **Aussagekräftige, datengestützte Erkenntnisse**<br><br>Strata Cloud Manager bietet ein einheitliches Framework für Vorfälle und Benachrichtigungen. Sie können die Benachrichtigungen und Vorfälle in Ihrem Netzwerk an einem Ort anzeigen, untersuchen und beheben und direkt zu Ihren Protokollen springen, um die zugehörige Aktivität zu untersuchen.<br><br>• Vorfälle und Benachrichtigungen: Strata Cloud Manager |  |
| **Überwachen** | **Proaktive Netzwerk- und Sicherheitsüberwachung**<br><br>Überwachen Sie die Integrität und Sicherheit aller Elemente in Ihrem Netzwerk und verwenden Sie die IoC-Suche, um den Verlauf eines Artefakts in Ihrem Netzwerk zu untersuchen und die Ergebnisse globaler Analysen zu überprüfen. Abhängig von den von Ihnen verwendeten Abonnements und Produkten können Sie Folgendes überwachen:<br><br>• NGFW-Geräte<br>• Prisma Access<br>• Anwendungen<br>• Benutzer |  |

| | | |
|---|---|---|
| | • Zweigstellen<br>• Rechenzentren<br>• Netzwerkdienste (wie GlobalProtect und DNS)<br>• Ihre Palo Alto Networks-Abonnements<br>• Ihre Prisma Access-Standorte<br>• Prisma SD-WAN<br>• Assets | |
| **Verwalten** | **Zentralisierte Konfiguration**<br>Verwalten Sie eine gemeinsame Richtlinie für all Ihre Netzwerksicherheitsprodukte und -abonnements. So können Sie gleich ab dem ersten Tag mit einer sicheren Konfiguration beginnen, die auf vordefinierten Best-Practice-Richtlinien und -Einstellungen sowie Inline-Best-Practice-Überprüfungen basiert.<br>• Verwalten: NGFW und Prisma Access<br>• Verwalten: Empfehlung für IoT-Richtlinien<br>• Verwalten: Enterprise DLP<br>• Verwalten: SaaS-Sicherheit |  |
| **Workflows** | **Verbesserte Sicherheitsergebnisse**<br>Wenn Sie zum ersten Mal zu Ihren Workflows navigieren, werden im **Discovery**-Dashboard wichtige und empfohlene Maßnahmen angezeigt, mit denen Sie Ihren Sicherheitsstatus oder Ihr Konfigurationsmanagement verbessern können, sobald diese für Sie verfügbar sind. Fahren Sie hier fort, um mobile NGFWs und Prisma Access-Benutzer sowie Remote-Netzwerke einzurichten und einzubinden und Software-Upgrades für NGFWs zu planen.<br>• Prisma Access einrichten<br>• NGFWs einrichten |  |

| | | |
|---|---|---|
| | • Software-Upgrade-Planer (AIOps für NGFW) | |
| **Berichte** | **Umfassende Transparenz**<br>Generieren, teilen und planen Sie datengesteuerte Einblicke in Berichten mit visuellen Diagrammen, interaktiven Abfragen und Empfehlungen zur Risikominderung.<br>• Berichte: Strata Cloud Manager |  |
| **Einstellungen** | **Onboarding- und Aktivierungseinstellungen**<br>Diese Einstellungen werden Sie regelmäßig nutzen, um neue Benutzer, Lizenzen oder Administratoren – oder auch sich selbst – hinzuzufügen, wenn Sie mit Strata Cloud Manager beginnen:<br>• Abonnements<br>• Mandanten<br>• Gerätezuordnungen<br>• Identität und Zugriff<br>• Auditierungslogs |  |

# Starten von Strata Cloud Manager

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden<br>• Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• Prisma SD-WAN | Jede dieser Lizenzen beinhaltet den Zugriff auf Strata Cloud Manager:<br>❑ Prisma Access<br>❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>❑ Prisma SD-WAN<br>❑ Strata Cloud Manager Essentials<br>❑ Strata Cloud Manager Pro<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Die Strata Cloud Manager-App ist im Palo Alto Networks-Hub verfügbar und Sie können auch direkt unter stratacloudmanager.paloaltonetworks.com darauf zugreifen.

Eine Prisma Access-Lizenz, eine „AIOps für NGFW Premium"-Lizenz oder eine Prisma SD-WAN-Lizenz ist eine Grundvoraussetzung für das einheitliche Management und den einheitlichen Betrieb mit Strata Cloud Manager. Wenn Sie über mindestens eine dieser Lizenzen verfügen, können Sie auf Strata Cloud Manager zugreifen, um Einblick in Ihre Produkte zu erhalten oder diese zu verwalten.

Wenn Sie mehr als eine dieser Lizenzen besitzen, bietet Strata Cloud Manager Ihnen eine zentrale Oberfläche zur Interaktion mit diesen Produkten sowie zusätzliche Lizenzen oder Add-on-Abonnements (wie Ihre Palo Alto Networks-Sicherheitsabonnements). → Sehen Sie sich die Produkte und Lizenzen an, *die für das einheitliche Management und den einheitlichen Betrieb mit Strata Cloud Manager unterstützt werden.*

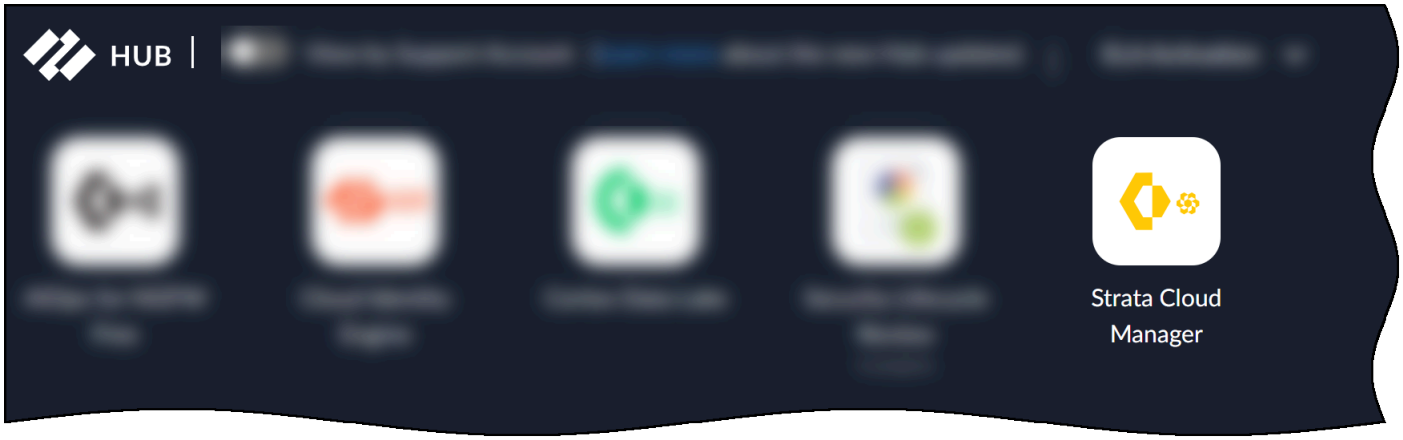
**So starten Sie Strata Cloud Manager bzw. greifen darauf zu:**

- Wenn Sie Prisma Access, AIOps für NGFW Premium oder Prisma SD-WAN ab Oktober 2023 zum ersten Mal nutzen, erfahren Sie hier, wie Sie Strata Cloud Manager zum ersten Mal starten.
- Wenn Sie bisher separate, eigenständige Apps im Hub verwendet haben, um Ihre Produkte zu verwalten, finden Sie hier weitere Informationen zum Umstieg auf Strata Cloud Manager von einer dedizierten Produkt-App.

## Strata Cloud Manager zum ersten Mal starten

Nachdem Sie eine Prisma Access-, AIOps für NGFW Premium- oder Prisma SD-WAN-Lizenz aktiviert haben, steht Ihnen die Strata Cloud Manager-App im Palo Alto Networks-Hub zur

Verfügung. Alternativ können Sie direkt unter stratacloudmanager.paloaltonetworks.com darauf zugreifen.




Starten Sie die App und werfen Sie einen Erster Blick auf Strata Cloud Manager. Fahren Sie mit dem Onboarding für Ihr Produkt fort:

- Erste Schritte mit AIOps für NGFW Premium, einschließlich Cloud Management für NGFWs
- Erste Schritte mit Prisma Access
- Erste Schritte mit Prisma SD-WAN

## Umstieg auf Strata Cloud Manager von einer dedizierten Produkt-App

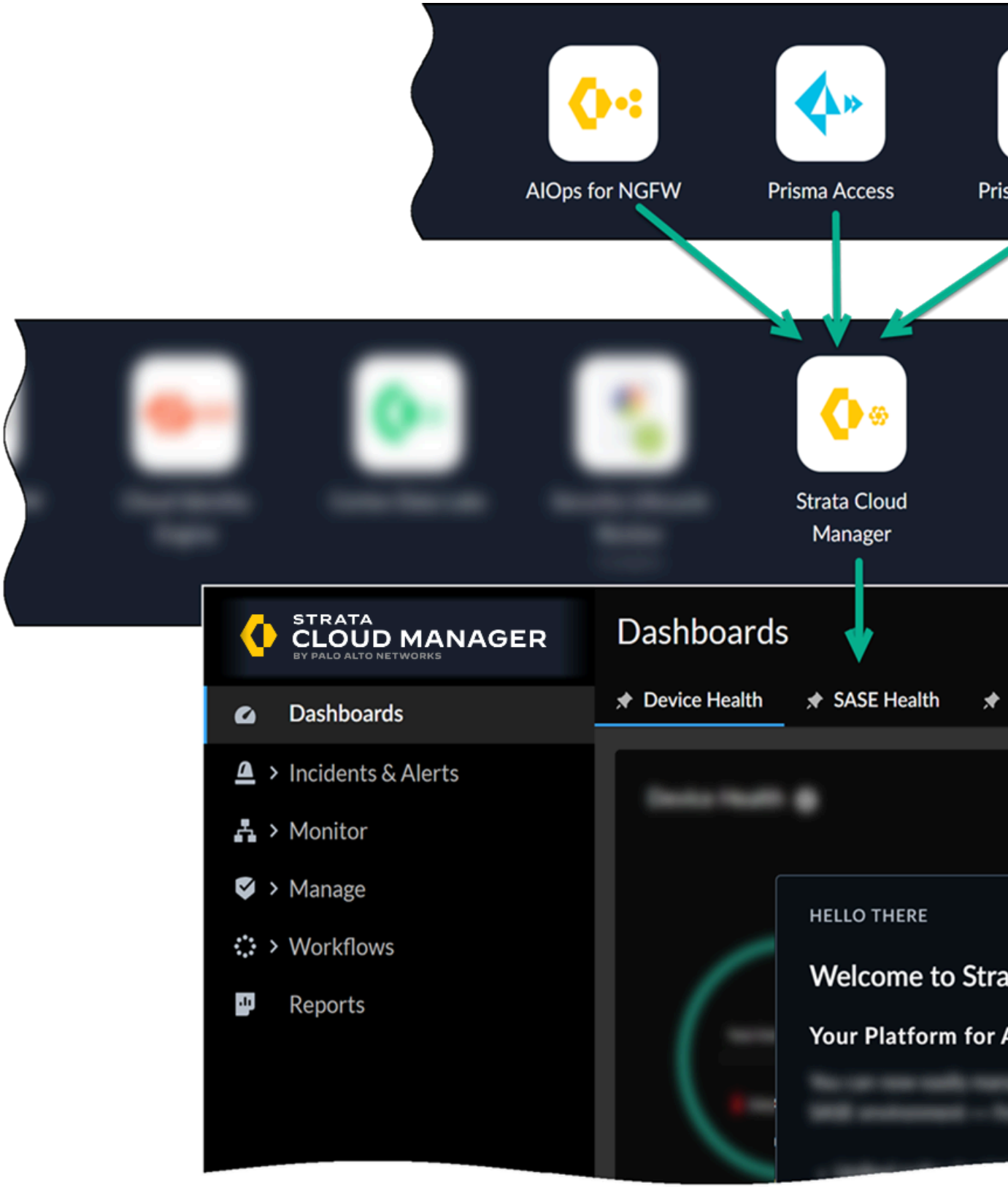
***Wichtig***

*Dies gilt nur, wenn Sie zuvor eine eigenständige App zur Verwaltung oder Interaktion mit Ihrem Produkt verwendet haben: die Prisma Access-App, die „AIOps für NGFW Premium"-App oder die Prisma SD-WAN-App. Diese Apps wurden aktualisiert – oder werden bald aktualisiert –, um Ihnen einheitliches Management und einheitlichen Betrieb über Strata Cloud Manager zu ermöglichen.*

**Was Sie bei einem Umstieg auf Strata Cloud Manager von einer dedizierten Produkt-App erwartet:**

- Strata Cloud Manager bietet einheitliches Management und einheitlichen Betrieb durch die Unterstützung verschiedener Lizenzen. Hier sind die Produkte, die Sie mit Strata Cloud Manager überwachen oder verwalten können.
- Produktinterne Benachrichtigungen informieren Sie im Voraus über ein bald verfügbares Update, mit dem Ihnen Strata Cloud Manager bereitgestellt wird.
- Das Update erfolgt nahtlos und hat keine Auswirkungen auf Ihre Daten, Benachrichtigungen oder Assets.

- Nach dem Update melden Sie sich bei der Strata Cloud Manager-App im Hub an. Sie werden nicht mehr separate Apps im Hub für Prisma Access, AIOps für NGFW Premium oder Prisma SD-WAN verwenden.



- Ihre Produkt-App leitet Sie automatisch zu stratacloudmanager.paloaltonetworks.com weiter. Dies ist die Strata Cloud Manager-URL.

  *Wenn Sie zuvor mehr als eine Produkt-App verwendet haben, die für Strata Cloud Manager aktualisiert wird, werden die aktualisierten Produkt-Apps alle auf dieselbe Strata Cloud Manager-Instanz umgeleitet.*

- Strata Cloud Manager bietet Ihnen eine brandneue Navigation, die für all Ihre Netzwerksicherheitsprodukte einheitlich ist. Werfen Sie einen ersten Blick auf Strata Cloud Manager und entdecken Sie die neue Navigationserfahrung und die neuen Funktionen.
- **Finden Sie Ihre Produktfunktionen in der neuen, einheitlichen Verwaltungsoberfläche:**
  - AIOps für NGFW: Wo sind meine Funktionen in Strata Cloud Manager?
  - Prisma SD-WAN: Wo sind meine Funktionen in Strata Cloud Manager?
  - Prisma Access Insights: Wo sind meine Funktionen in Strata Cloud Manager?
  - Prisma Access: Wo sind meine Funktionen in Strata Cloud Manager?

# Erste Schritte mit Strata Cloud Manager

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden<br>• Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• Prisma SD-WAN | Jede dieser Lizenzen beinhaltet den Zugriff auf Strata Cloud Manager:<br>❑ Prisma Access<br>❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>❑ Prisma SD-WAN<br>❑ Strata Cloud Manager Essentials<br>❑ Strata Cloud Manager Pro<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Strata Cloud Manager bietet Ihnen KI-gestützte, einheitliche Verwaltungs- und Betriebsfunktionen für Ihre NGFWs und Ihr SASE-Netzwerk. Hier ist ein Spickzettel für die ersten Schritte mit Strata Cloud Manager.

Wenn Sie planen, mit Strata Cloud Manager Prisma Access, NGFWs (erfordert AIOps für NGFW Premium) oder beides zu integrieren und zu verwalten, finden Sie hier alle nötigen Informationen, um mit Gemeinsames Management für Prisma Access und NGFWs loszulegen.

❑ **(Im Hub) Aktivieren Ihrer Lizenzen**

Nach dem Erwerb einer Lizenz erhalten Sie eine E-Mail mit einem Aktivierungslink. Der Link startet einen geführten Workflow im Hub. Folgen Sie dem Aktivierungsworkflow für jede Lizenz, die Sie aktivieren möchten:

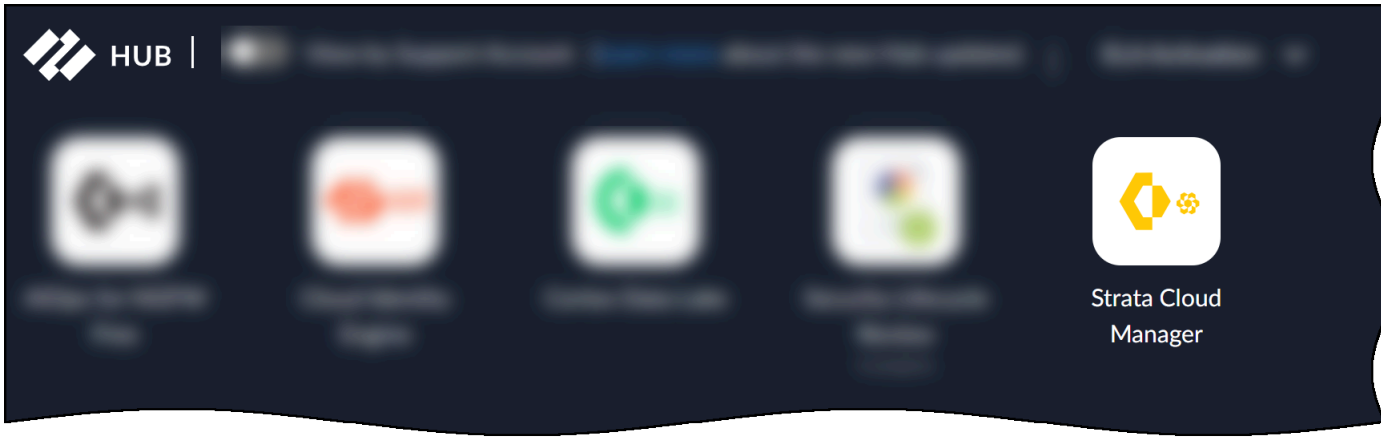
- „AIOps für NGFW Premium“-Lizenz
- Prisma Access-Lizenz aktivieren
- Prisma SD-WAN

Durch die Aktivierung einer dieser Lizenzen wird Strata Cloud Manager aktiviert. Nachdem Sie mindestens eine dieser Lizenzen aktiviert haben, fahren Sie mit der Aktivierung aller weiteren Lizenzen oder Add-on-Abonnements fort.

❑ **Starten von Strata Cloud Manager**

Nachdem Sie eine Prisma Access-, AIOps für NGFW Premium- oder Prisma SD-WAN-Lizenz aktiviert haben, steht Ihnen die Strata Cloud Manager-App im Palo Alto Networks-Hub zur

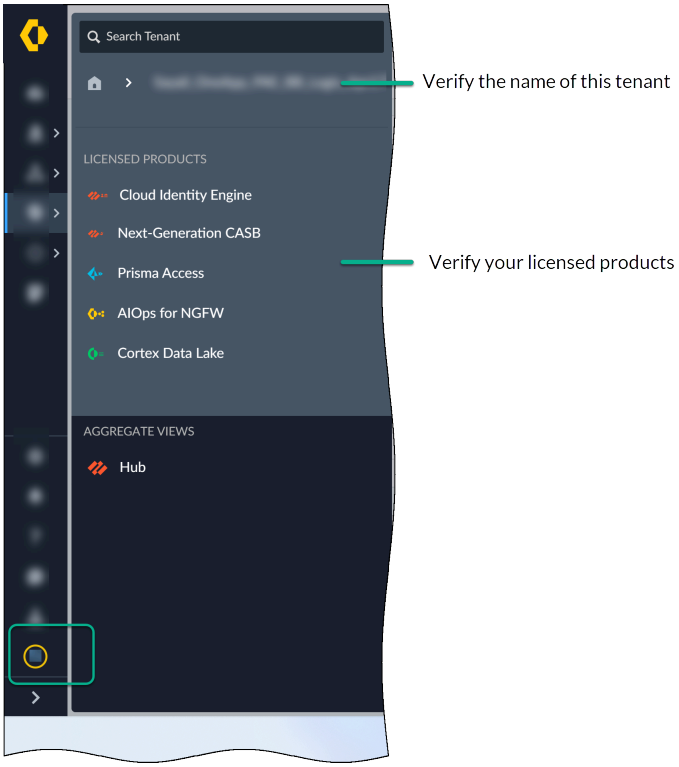
Verfügung. Alternativ können Sie direkt unter stratacloudmanager.paloaltonetworks.com darauf zugreifen.



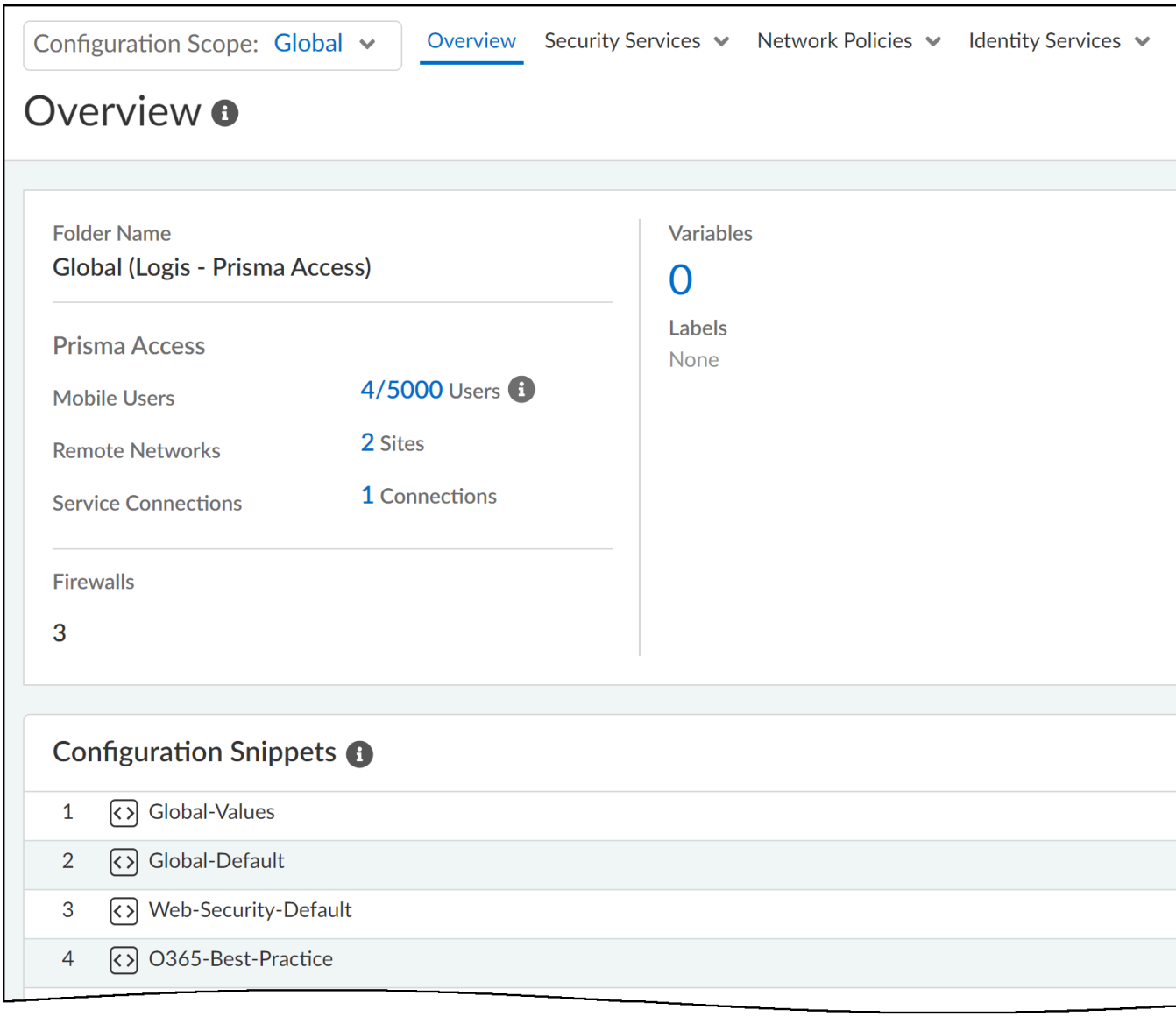
### Validieren Ihrer Lizenzen

- Wählen Sie unten im Navigationsmenü Ihre Mandantendetails aus und überprüfen Sie den Namen des von Ihnen verwendeten Mandanten sowie Ihre lizenzierten Produkte. Hier erfahren Sie mehr zum Mandanten- und Abonnementmanagement.




- Gehen Sie zu **Verwalten** > **Konfiguration** > **NGFW und Prisma Access**, um den Status und die Details Ihrer Prisma Access-Lizenz zu überprüfen und zu sehen, welche weiteren Details möglicherweise verfügbar sind.

> *Es kann sein, dass Sie hier noch nicht viele Daten sehen, wenn Sie NGFWs noch nicht integriert haben oder Ihre Prisma Access-Umgebung noch bereitgestellt wird. Wenn dies der Fall ist, schauen Sie erneut vorbei, nachdem Sie die restlichen Schritte abgeschlossen haben.*




- **Überwachung und Transparenz mit Strata Cloud Manager**
  - Erkunden Sie mit dem Command Center eine visualisierte Darstellung Ihrer Netzwerk- und Sicherheitsinfrastruktur.
  - Überprüfen Sie wichtige Netzwerkdaten in Activity Insights.
  - Entdecken Sie die Strata Cloud Manager-Dashboards, die Ihnen zur Verfügung stehen. Viele Dashboards unterstützen auch Berichte, die Sie planen oder mit Stakeholdern teilen können.
  - Überwachen Sie Ihre Prisma Access-Umgebung, Prisma SD-WAN und Ihre NGFWs.
  - Überprüfen Sie Ihre Vorfälle und Benachrichtigungen hinsichtlich Prisma Access, NGFWs und Prisma SD-WAN.
- **Inline-Best-Practice-Empfehlungen und -Workflows**

  Erfahren Sie mehr über die Best-Practice-Anleitung und -Automatisierung, die direkt in Strata Cloud Manager integriert ist.

- **Strata Cloud Manager-Onboarding-Einstellungen**

  Strata Cloud Manager vereint allgemeine Dienste im Menü **Einstellungen**. Gehen Sie zu **Einstellungen**, um Folgendes zu verwalten:

  - Rollen und Berechtigungen – Erfahren Sie mehr über die in Strata Cloud Manager verfügbaren Rollen und zugehörigen Berechtigungen.
  - Gerätezuordnungen – Ordnen Sie unterstützte Cloud-Anwendungen Ihren Geräten zu.
  - Mandantverwaltung – Erstellen und verwalten Sie Ihre Hierarchie von Geschäftsorganisationen und -einheiten, dargestellt durch Mandanten.

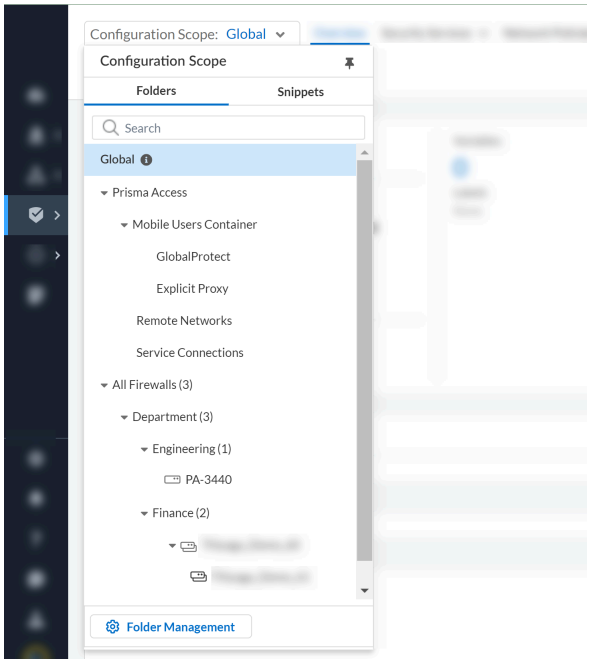
## Gemeinsames Management für Prisma Access und NGFWs

Für Prisma Access und NGFWs bietet Strata Cloud Manager gemeinsames Management; binden Sie NGFWs und Prisma Access-Benutzer, Remote-Netzwerke und Dienstverbindungen in Strata Cloud Manager ein und setzen Sie eine gemeinsame Sicherheitsrichtlinie durch.

- **Onboarding von NGFWs und Prisma Access in Strata Cloud Manager**
  - Richten Sie Prisma Access ein und binden Sie mobile Benutzer, Remote-Netzwerke und Dienstverbindungen ein:
    - Einrichten der Prisma Access-Dienstinfrastruktur
    - Einrichten mobiler Prisma Access-Benutzer, einschließlich Verbindungen per GlobalProtect und explizitem Proxy
    - Einrichten von Prisma Access-Remote-Netzwerken
    - Einrichten von Prisma Access-Dienstverbindungen
  - Onboarding und Einrichtung von NGFWs:
    - Onboarding und Einrichtung für NGFW-Cloud-Verwaltung
- **Organisieren Ihrer Konfiguration**

  Bei der Arbeit in den Strata Cloud Manager-Konfigurationseinstellungen ist der aktuelle Verwalten: Konfigurationsumfang für Sie immer sichtbar und Sie können Ihre Ansicht umschalten, um eine umfassendere oder detailliertere Konfiguration zu verwalten. Der

Konfigurationsumfang ermöglicht Ihnen die globale Anwendung von Richtlinien oder die gezielte Durchsetzung in bestimmten NGFWs oder Prisma Access-Bereitstellungen.




Hier erfahren Sie mehr darüber, wie Sie mit der Organisation Ihrer Strata Cloud Manager-Konfiguration beginnen können:

- **Workflows: Ordnerverwaltung**

  Verwenden Sie Ordner, um NGFWs logisch zu gruppieren und so die Konfigurationsverwaltung zu vereinfachen. Die Prisma Access-Ordner sind basierend auf dem Bereitstellungstyp vordefiniert. Sie können Websicherheit (eine vereinfachte Verwaltungserfahrung für Administratoren, die den Zugriff auf Internet und SaaS-Anwendungen verwalten) auch auf Ordnerebene aktivieren.

- **Verwalten: Snippets**

  Verwenden Sie Snippets, um Konfigurationen zu gruppieren, die Sie schnell an Ihre NGFWs oder Prisma Access-Bereitstellungen übertragen können.

- **Verwalten: Variablen**

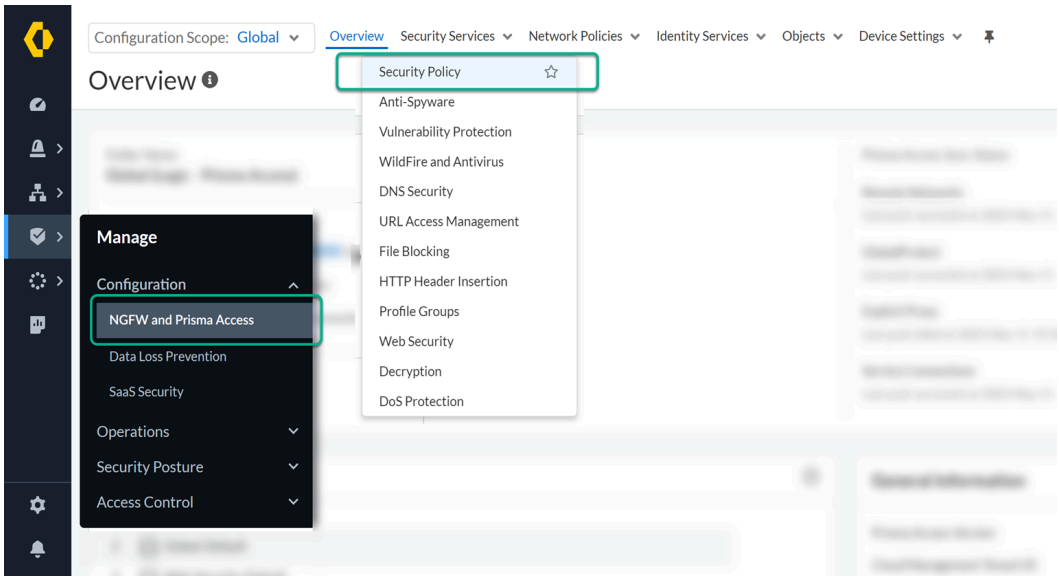
  Verwenden Sie Variablen für Ihre Konfigurationen, um geräte- oder bereitstellungsspezifische Konfigurationsobjekte zu berücksichtigen.

- **Gemeinsame Sicherheitsrichtlinie für NGFWs und Prisma Access**

  Strata Cloud Manager bietet Ihnen eine einheitliche Verwaltung für Prisma Access und Ihre NGFWs. Ihre Strata Cloud Managervsecurity-Richtlinie wird gemeinsam genutzt und Sie

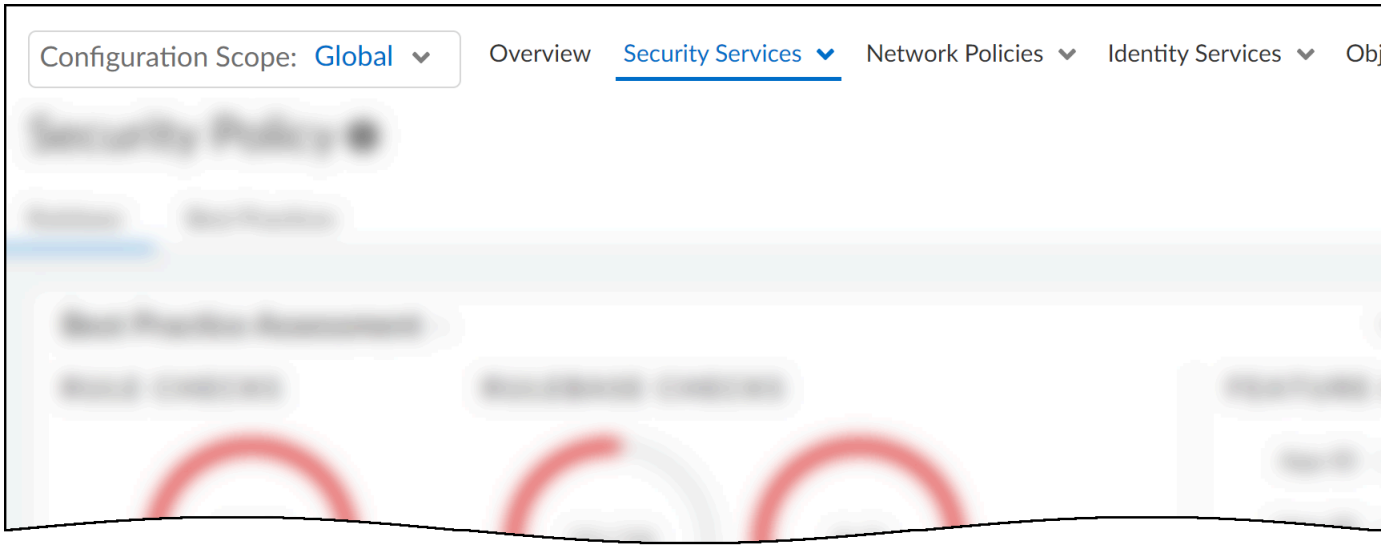
können sie global auf Prisma Access und NGFWs anwenden oder bestimmte Einstellungen auf Prisma Access-Bereitstellungen oder bestimmte Firewall-Gruppen ausrichten.

Gehen Sie zu **Verwalten > Konfiguration > NGFW und Prisma Access**, um zu beginnen.




- **Übertragen von Konfigurationsänderungen an NGFWs und Prisma Access**

  Wählen Sie bei der Verwaltung Ihrer Strata Cloud Manager-Konfiguration **Konfiguration übertragen** aus, um Konfigurationsänderungen an Ihre NGFWs und Prisma Access zu übertragen:




Sie werden aufgefordert, den Umfang der Konfigurationsübertragung basierend auf Ihren Ordnern festzulegen. Hier finden Sie weitere Informationen:

- Übertragen Ihrer Konfigurationsänderungen
- Überprüfen des Status eines Konfigurationsübertragung
- Bereinigen Ihrer Konfiguration

# Integrierte Best Practices in Strata Cloud Manager

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden<br>• Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• Prisma SD-WAN | Jede dieser Lizenzen beinhaltet den Zugriff auf Strata Cloud Manager:<br>❑ Prisma Access<br>❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>❑ Prisma SD-WAN<br>❑ Strata Cloud Manager Essentials<br>❑ Strata Cloud Manager Pro<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Die Best Practices von Palo Alto Networks sollen Ihnen dabei helfen, Ihr Netzwerk bestmöglich zu schützen, indem sie den Prozess der Konformitätsprüfung Ihrer Netzwerkinfrastruktur optimieren. Wir haben Best-Practice-Überprüfungen direkt in Strata Cloud Manager integriert, damit Sie eine Live-Auswertung Ihrer Konfiguration erhalten. Verbessern Sie Ihren Sicherheitsstatus durch die Einhaltung von Best Practices. Sie können Strata Cloud Manager nutzen, um Ihre Sicherheitskonfigurationen von Panorama, NGFW und von Panorama verwaltetem Prisma Access anhand von Best Practices zu bewerten und fehlgeschlagene Best-Practice-Überprüfungen zu korrigieren.

Mithilfe der Best-Practice-Anleitungen können Sie nicht nur Ihren Sicherheitsstatus verbessern, sondern gleichzeitig Ihre Umgebung effizient verwalten und die Benutzerproduktivität optimal unterstützen. Bewerten Sie Ihre Konfiguration kontinuierlich anhand dieser Inline-Überprüfungen – und ergreifen Sie sofort Maßnahmen, wenn Sie Möglichkeiten zur Verbesserung Ihrer Sicherheit finden.

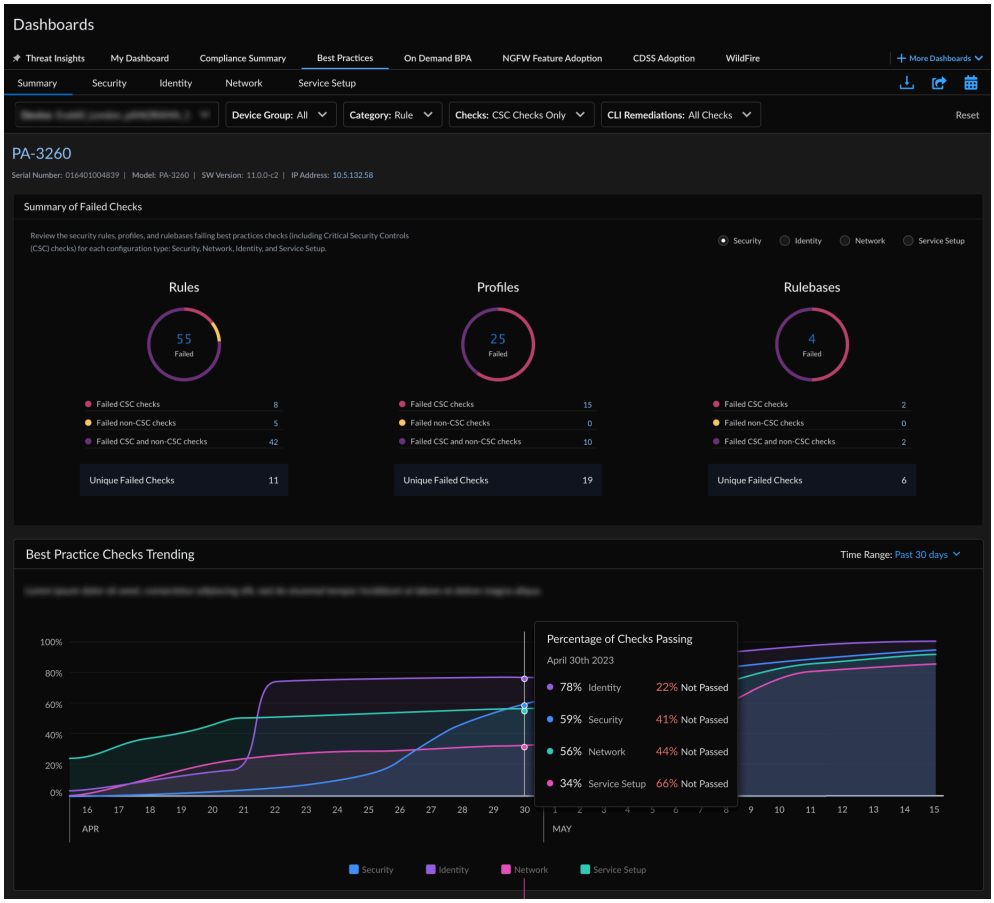
#### Einblick in die Einführung und Einhaltung von Best Practices

Um zu beginnen, können Sie Ihren allgemeinen Sicherheitsstatus schnell beurteilen, indem Sie die folgenden Status-**Dashboards** überprüfen.

Prüfen Sie den Sicherheitsstatus auf übergeordneter Ebene und ermitteln Sie die Bereiche, in denen Sie möglicherweise Maßnahmen ergreifen sollten.

- Im Dashboard: Best Practices-Dashboard finden Sie tägliche Best-Practice-Berichte und deren Zuordnung zu den Critical Security Controls (CSC) des Center for Internet Security. So können Sie Bereiche identifizieren, in denen Sie Änderungen vornehmen können, um die Einhaltung

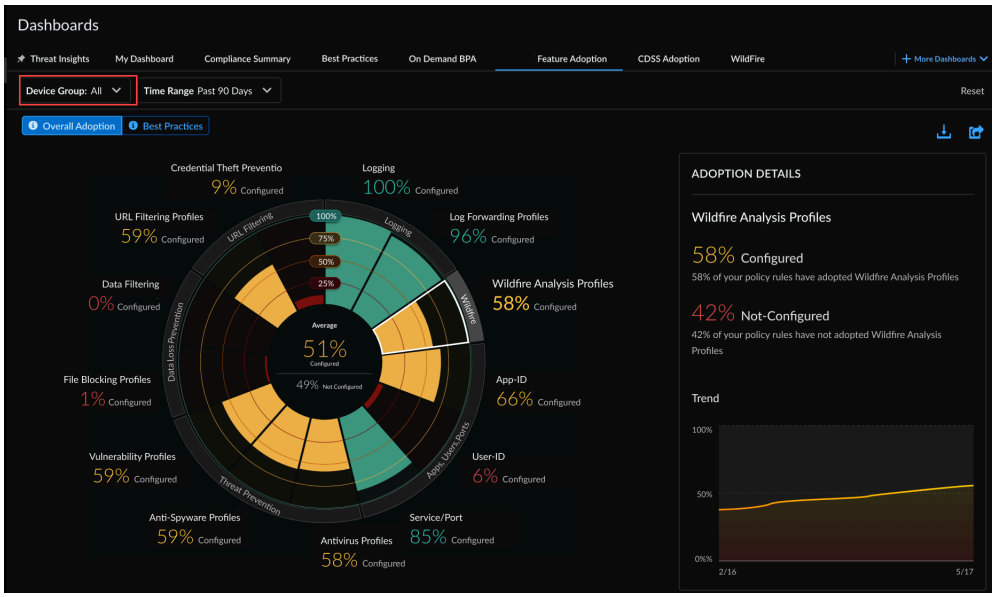
Ihrer Best Practices zu verbessern. Teilen Sie den Best-Practice-Bericht als PDF und planen Sie die regelmäßige Zustellung in Ihren Posteingang.



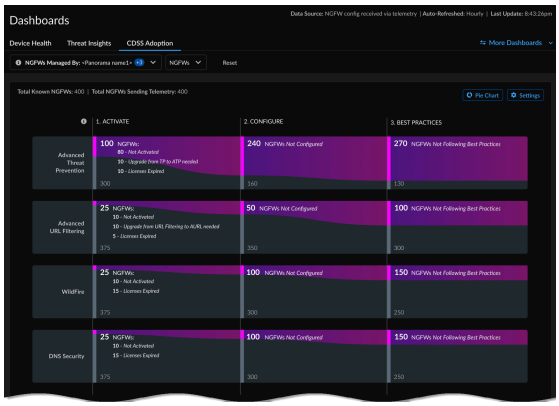

- Im Dashboard Zusammenfassung der Konformität können Sie den Änderungsverlauf der Sicherheitsüberprüfungen anzeigen, die vor bis zu 12 Monaten vorgenommen wurden, gruppiert nach den CIS- (Center for Internet Security) und NIST-Frameworks (National Institute of Standards and Technology).

- Überwachen Sie Dashboard: Funktionsannahme und behalten Sie im Blick, welche Sicherheitsfunktionen Sie in Ihrer Bereitstellung verwenden und welche potenziellen Abdeckungslücken bestehen.




- Überwachen Sie Dashboard: Einführung von CDSS – Zeigen Sie Sicherheitsdienste oder Funktionsabonnements und deren Lizenznutzung auf Ihren Geräten an, um Sicherheitslücken zu identifizieren und den Sicherheitsstatus Ihres Unternehmens zu verbessern.

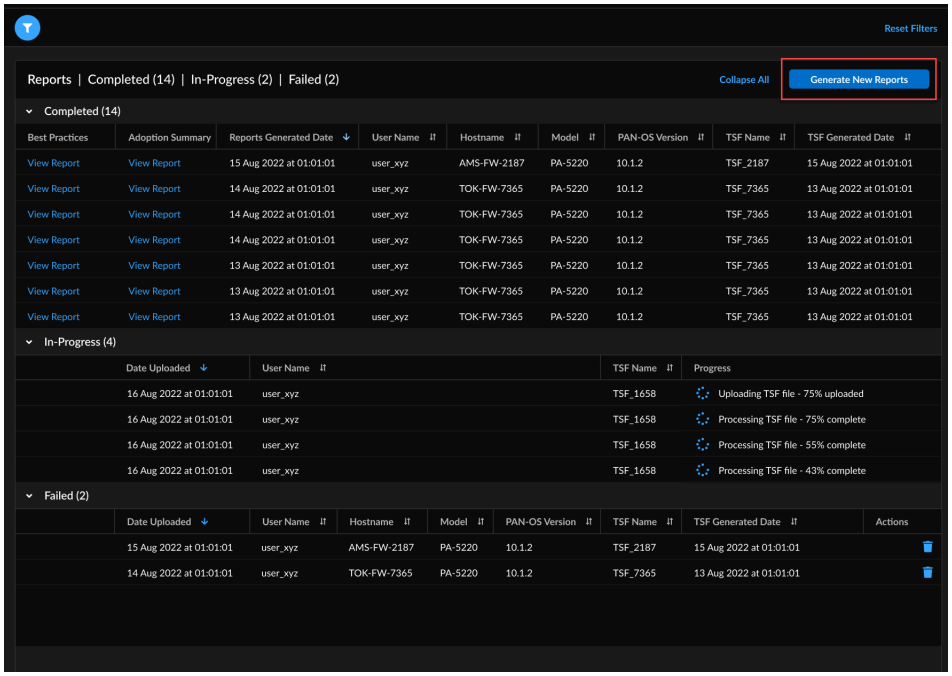



- Erhalten Sie mit Dashboard: Einblicke in den Sicherheitsstatus Einblick in den Sicherheitsstatus und -trend Ihrer Bereitstellung, basierend auf dem Sicherheitsstatus der eingebundenen

NGFW-Geräte, und lassen Sie sich benachrichtigen, wenn Vorfälle auftreten oder Ihre Sicherheitseinstellungen einer genaueren Überprüfung bedürfen.


- Erstellen Sie BPA-Berichte für (nicht telemetrische) PAN-OS-Geräte mit Version 9.1 und höher, jetzt einschließlich Metriken zur Funktionsannahme.




### Best-Practice-Tools zur Stärkung des Sicherheitsstatus

Hier finden Sie eine Sammlung von Tools, die Ihnen dabei helfen, Ihren Sicherheitsstatus zu verbessern.

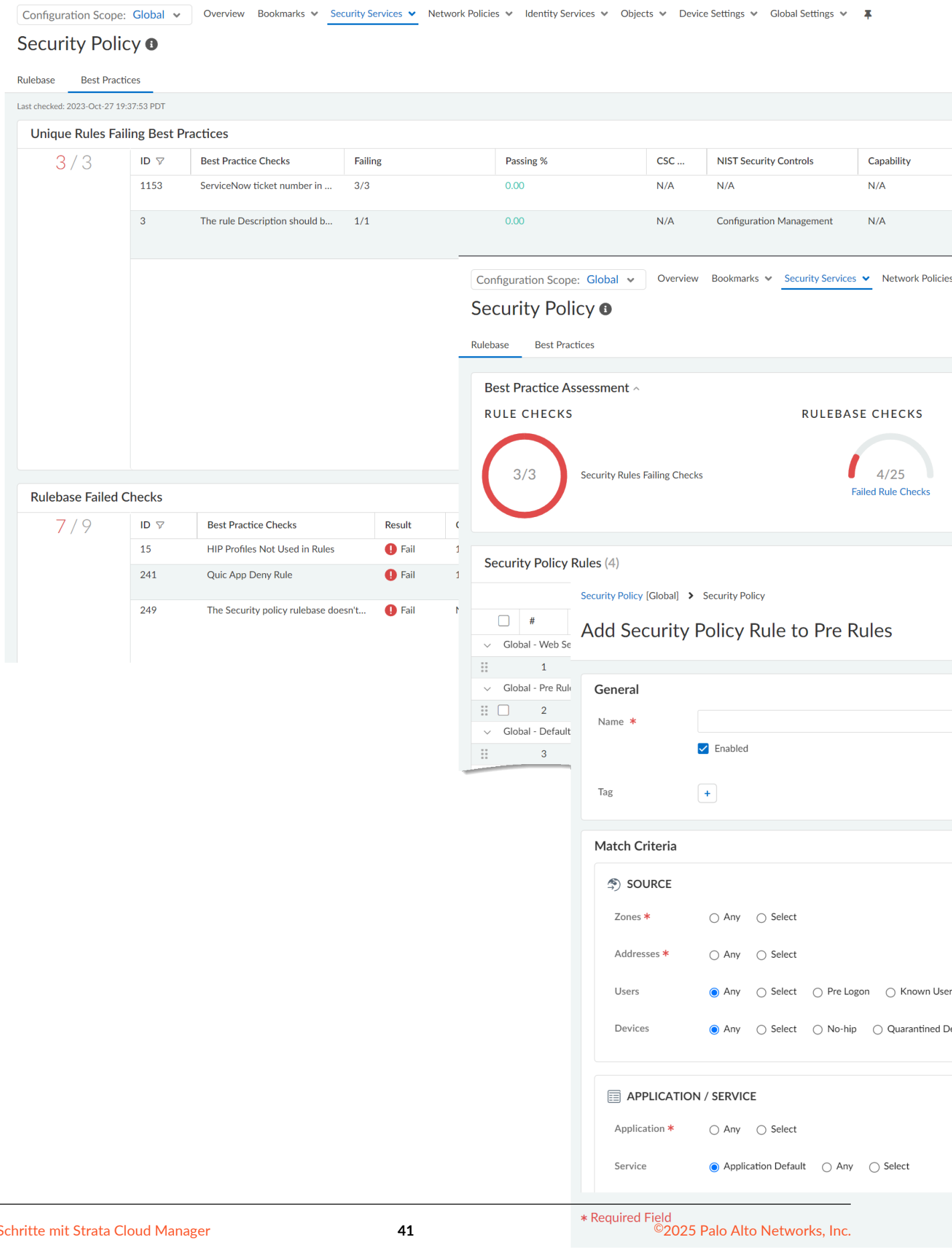
- Passen Sie Sicherheitsstatusprüfungen für Ihre Bereitstellung an, um relevante Empfehlungen in Verwalten: Einstellungen für den Sicherheitsstatus zu maximieren.
- Verwenden Sie die Konfigurationsbereinigung, um nicht verwendete Konfigurationsobjekte und Richtlinienregeln zu identifizieren und zu entfernen.
- Konfigurieren Sie die Einstellungen des Richtlinienoptimierers, um unverhältnismäßig tolerante Sicherheitsregeln zu verfeinern und zu optimieren, sodass nur Anwendungen zugelassen werden, die in Ihrem Netzwerk tatsächlich verwendet werden.

- Erstellen Sie Ihre eigenen Compliance-Prüfungen – passen Sie vorhandene Best-Practice-Überprüfungen an und erstellen und verwalten Sie spezielle Ausnahmen, um eine bessere Anpassung an die Geschäftsanforderungen Ihres Unternehmens zu gewährleisten.
- Verwenden Sie die Richtlinienanalyse, um schnell sicherzustellen, dass die Aktualisierungen Ihrer Sicherheitsrichtlinienregeln Ihren Anforderungen entsprechen und keine Fehler oder Fehlkonfigurationen verursachen (z. B. Änderungen, die zu doppelten oder widersprüchlichen Regeln führen).

**Live-Inline-Best-Practice-Konfigurationsprüfungen**

Mithilfe der Best-Practice-Anleitungen können Sie nicht nur Ihren Sicherheitsstatus verbessern, sondern gleichzeitig Ihre Umgebung effizient verwalten und die Benutzerproduktivität optimal unterstützen. Bewerten Sie Ihre Konfiguration kontinuierlich anhand dieser Inline-Überprüfungen – und ergreifen Sie sofort Maßnahmen, wenn Sie Möglichkeiten zur Verbesserung Ihrer Sicherheit finden.



- **Best-Practice-Scores**

  Die Best-Practices-Scores werden in einem Funktions-Dashboard angezeigt (beispielsweise Sicherheitsrichtlinie, Entschlüsselung oder URL-Zugriffssteuerung). Diese Scores bieten Ihnen einen schnellen Einblick in Ihre Best-Practice-Fortschritte. Sie können auf einen Blick Bereiche erkennen, die einer weiteren Untersuchung bedürfen oder in denen Sie Maßnahmen zur Verbesserung Ihres Sicherheitsstatus ergreifen sollten.
- **Best-Practice-Feldüberprüfungen**

  Überprüfungen auf Feldebene zeigen Ihnen genau, wo Ihre Konfiguration nicht den Best Practices entspricht. Best-Practice-Anleitungen werden inline bereitgestellt, sodass Sie sofort Maßnahmen ergreifen können.
- **Best-Practice-Bewertung**

  Hier erhalten Sie einen umfassenden Überblick darüber, inwieweit die Implementierung einer Funktion den Best Practices entspricht. Untersuchen Sie fehlgeschlagene Überprüfungen, um festzustellen, wo Sie Verbesserungen vornehmen können (Sie können auch bestandene Überprüfungen prüfen). Regelwerküberprüfungen heben Konfigurationsänderungen hervor, die Sie außerhalb einzelner Regeln vornehmen können, beispielsweise an einem Richtlinienobjekt, das in mehreren Regeln verwendet wird.

Best-Practice-Überprüfungen gibt es für folgende Elemente:

- **Ihr Sicherheitsrichtlinien-Regelsatz**

  Regelwerküberprüfungen untersuchen, wie die Sicherheitsrichtlinie organisiert und verwaltet wird, einschließlich der Konfigurationseinstellungen, die für mehrere Regeln gelten.
- **Sicherheitsregeln**
- **Sicherheitsprofile**
  - Anti Spyware
  - Schutz vor Sicherheitslücken
  - WildFire und Antivirus
  - URL-Zugriffsverwaltung
  - DNS Security
- **Authentifizierung**
- **Entschlüsselung**
- **GlobalProtect**

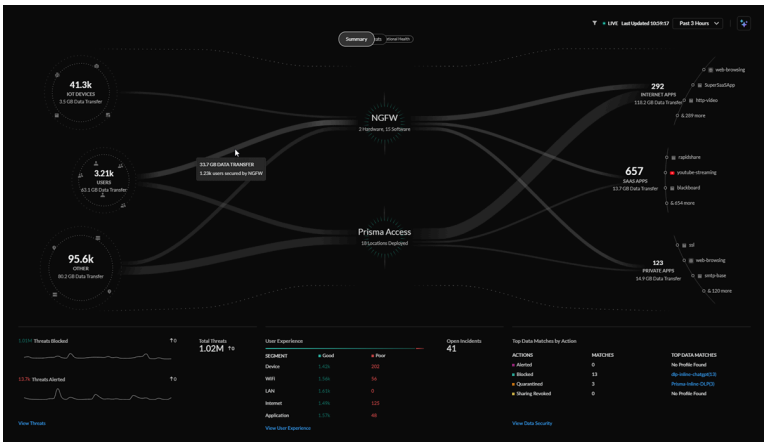
***Suchen Sie nach weiteren Best Practices von Palo Alto Networks?***

*Dann besuchen Sie unsere Homepage zu Best Practices, wo Sie Ressourcen finden, die Ihnen bei der Implementierung von Best Practices helfen.*

# Command Center: Strata Cloud Manager

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden<br>• Prisma SD-WAN | Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>❑ Prisma Access<br>❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>❑ Strata Cloud Manager Pro<br>❑ Strata Cloud Manager Essentials<br>❑ Prisma SD-WAN<br>Weitere Lizenzen und Voraussetzungen für den Zugriff auf das Command Center:<br>❑ Strata Logging Service<br>❑ eine spezifische Lizenz zum Anzeigen bestimmter, unten beschriebener Metriken im Command Center<br>❑ eine Rolle mit der Berechtigung zum Anzeigen des Command Center<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Das Strata Cloud Manager Command Center ist Ihre neue Homepage für Netzwerksicherheit: Es bietet eine interaktive visuelle Zusammenfassung, die Ihnen hilft, den Zustand, die Sicherheit und die Effizienz Ihres Netzwerks zu beurteilen. Das Command Center bietet eine konsolidierte Ansicht der NetSec-Plattform und bietet Ihnen einen umfassenden Überblick über Ihre Quellen, Anwendungen, die Prisma Access-Bereitstellung, Ihre NGFWs und Ihre Sicherheitsdienste – alles an einem einzigen Ort.




Hier können Sie mit den Daten interagieren und die Beziehungen zwischen Ereignissen im Netzwerk visualisieren, sodass Sie sofort Maßnahmen ergreifen können, um Ihre Sicherheit zu erhöhen.

Das Command Center ist in die neuen Activity Insights-Dashboards **(Insights > Activity Insights)** integriert. Es hebt anhand aussagekräftiger Einblicke Anomalien hervor, die von Ihren integrierten Lizenzen und Abonnements erkannt wurden, und bietet einen Pfad zur Behebung dieser Anomalien.

Auf der neuen Homepage sehen Sie Folgendes:

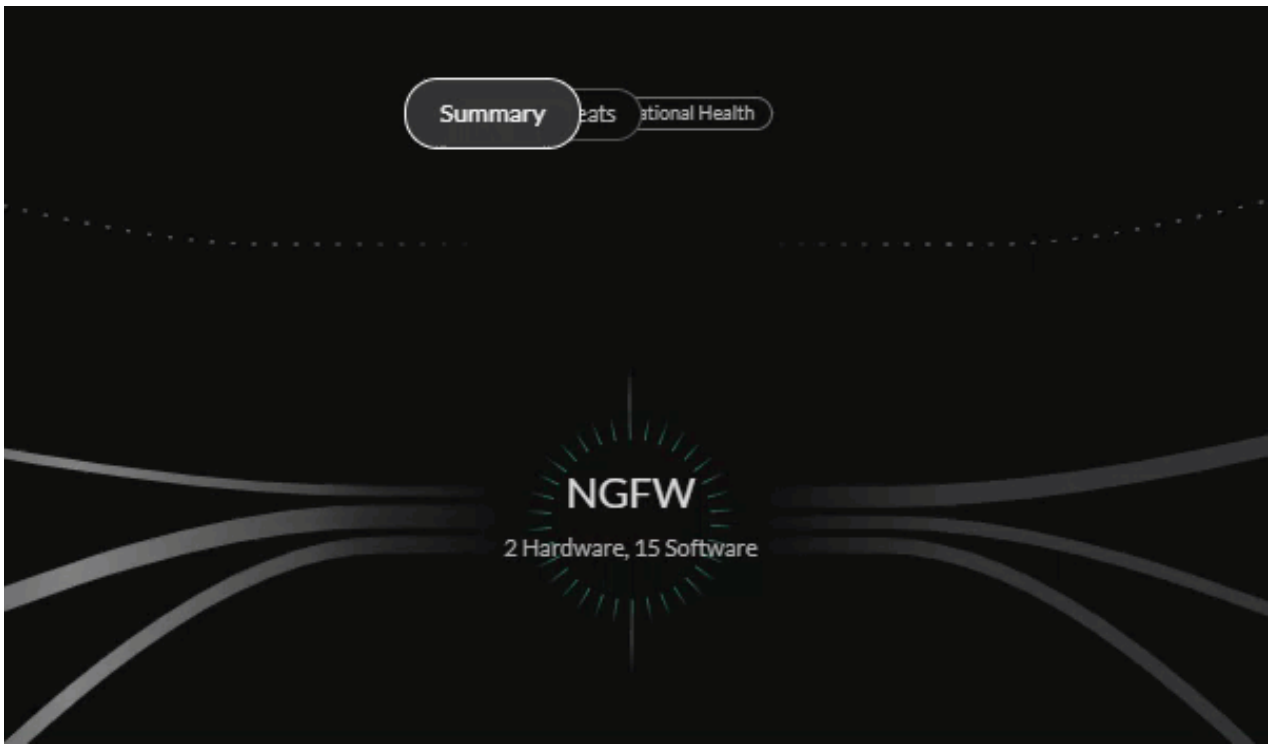
- umfassender Überblick über den gesamten Datenverkehr in Ihrem Netzwerk, der zwischen Quellen (Benutzer, IoT, externe Hosts) zu Anwendungen (Internet, SaaS, privat) fließt
- wie auf Ressourcen wie Benutzer, Geräte und Anwendungen zugegriffen wird und wie diese geschützt werden
- Navigation zu spezifischen Dashboards mit Kontext, um ein tieferes Verständnis der Probleme zu erhalten, die sich auf Ihr Netzwerk auswirken
- Arten von Bedrohungen, auf die Benutzer bei der Arbeit stoßen

Starten Sie Strata Cloud Manager und klicken Sie auf **Command Center (** **)**, um loszulegen.

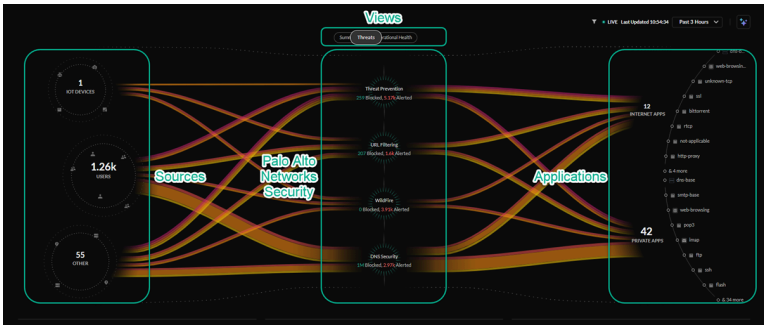
# So interagieren Sie mit dem Strata Cloud Manager Command Center

In jeder Ansicht im Command Center werden alle Informationen, die Sie benötigen, um den Zustand und die Sicherheit Ihres Netzwerks zu beurteilen, übersichtlich aufgeschlüsselt.




Die Daten im Command Center werden alle fünf Minuten aktualisiert und standardmäßig werden Daten der letzten 24 Stunden angezeigt. Sie können diese Daten auch nach der letzten Stunde, den letzten 3 Stunden, 7 Tagen oder 30 Tagen filtern.

In jeder Command Center-Ansicht werden verschiedene Arten visueller Daten angezeigt, die in Ihrer Umgebung übertragen werden: von den Quellen über Prisma Access, NGFWs oder in Ihrem Netzwerk bereitgestellte Sicherheitsabonnements bis hin zu den verschiedenen Anwendungen in Ihrem Netzwerk.




Die Quellenblasen (hybride Mitarbeiter, Bürobenutzer, IoT-Geräte und andere) befinden sich auf der linken Seite und die Anwendungsblasen (auf die über das Internet [SaaS] zugegriffen wird

oder die On-Premises oder in der Cloud gehostet werden) befinden sich auf der rechten Seite. Die Anwendungsblasen zeigen die drei am häufigsten verwendeten Anwendungen in jeder Kategorie.

Zu den Quellen gehören:

- **IoT-Geräte** – Geräte, die durch eine aktive IoT Security-Lizenz erkannt und aktiviert wurden
- **Benutzer** – Remote- und Zweigstellenbenutzer
- **Sonstige** – interne und externe Hosts, die auf Ressourcen im Internet zugreifen

Zu den Anwendungen gehören:

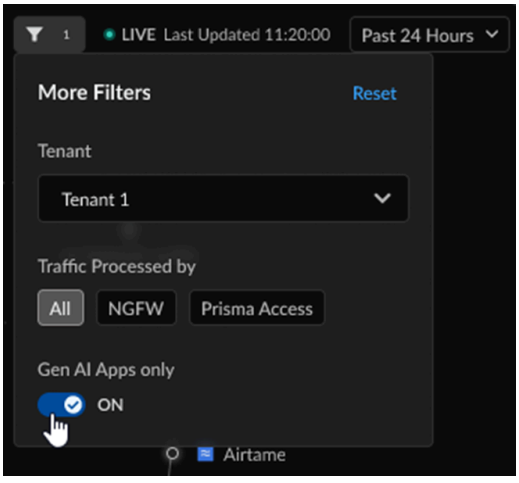
- **Internetanwendungen** – Anwendungen, auf die über einen Webbrowser zugegriffen wird
- **SaaS-Apps** – Cloud-Anwendungen, die einem Anwendungsdienstanbieter gehören und von diesem verwaltet werden
- **private Anwendungen** – Anwendungen, die in einem Rechenzentrum gehostet werden

Sie können die Daten in der zentralen Ansicht filtern, indem Sie auf die Blasen für Quellen, Bereitstellungen oder Anwendungen klicken. Dadurch erhalten Sie eine detailliertere Ansicht der erfassten Daten für die ausgewählte Blase.

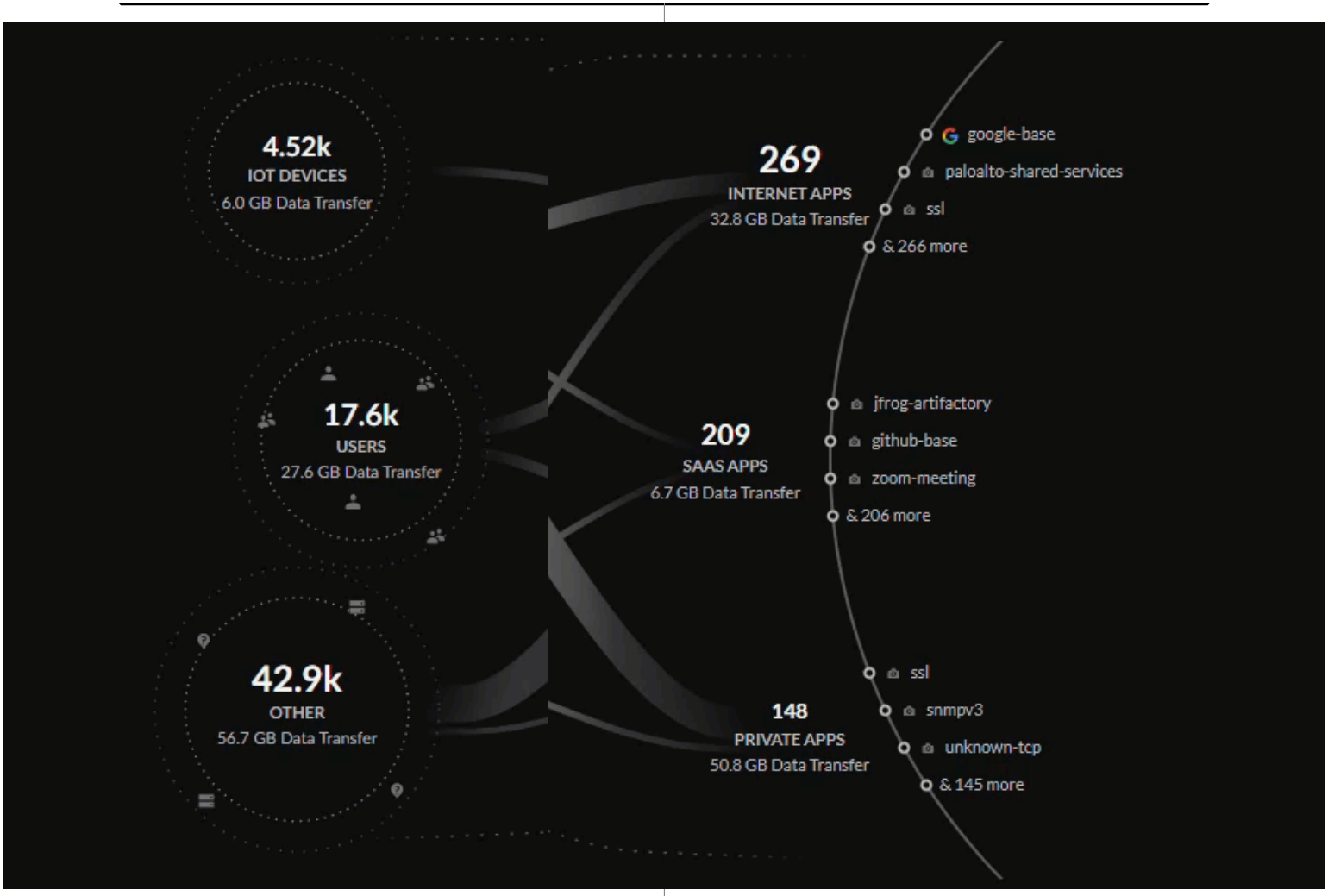
Durch die Auswahl von Filtern (▼) können Sie die Daten in den Command Center-Ansichten nach **Mandanten** bzw. nach **NGFW**- oder **Prisma Access**-spezifischen Daten filtern.

Mit einer Lizenz für KI-Zugriff können Sie den Datenverkehr in allen Command Center-Ansichten mit **nur GenAI-Apps** filtern, um besser einschätzen zu können, wie sich GenAI-Anwendungen, die von Benutzern in Ihrem Netzwerk verwendet werden, auf Ihre Datensicherheit auswirken könnten.

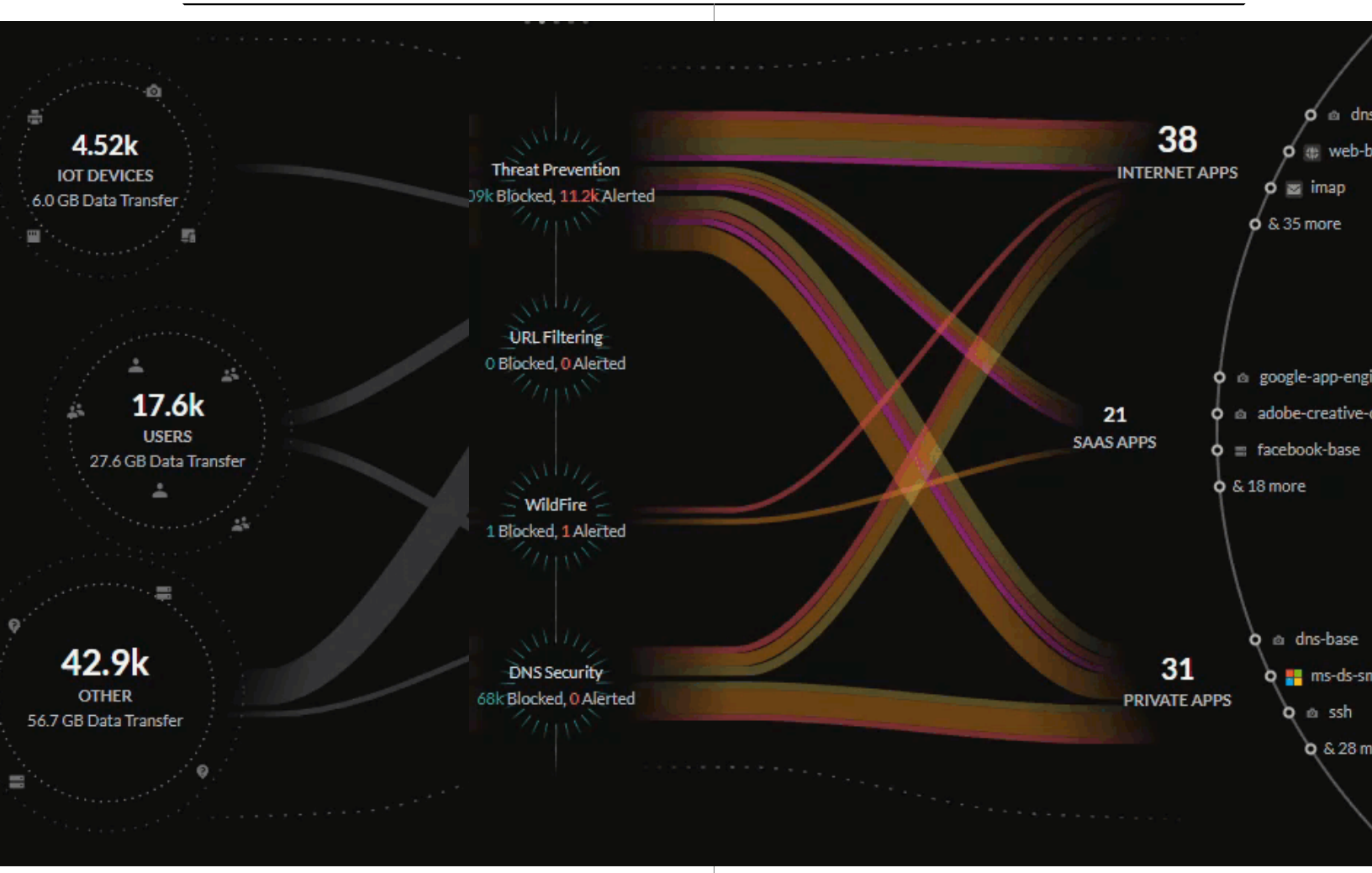
*Weitere Informationen zu KI-Zugriffssicherheit und entsprechenden Lizenzen finden Sie hier.*



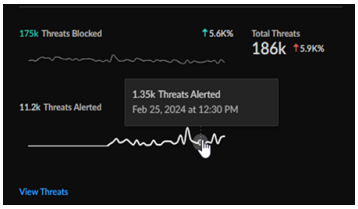

 




Wenn Sie sich eine der Ansichten ansehen, können Sie mit der Maus über die Linien fahren, um weitere Informationen über Ihr Netzwerk zu erhalten, z. B. über den Datenverkehr oder die in Ihrem Netzwerk blockierten oder zugelassenen Bedrohungen.




Unter der zentralen visuellen Zusammenfassung befinden sich mehrere wichtige Metriken, die von Ihren aktivierten Abonnements erfasst werden und verwertbare Einblicke in Ihr Netzwerk bieten. Diese wichtigen Metriken bieten die Möglichkeit, zu einer von mehreren detaillierten Kontextseiten zu navigieren, auf denen Sie weitere Informationen zu den erfassten Metriken finden und im Detail mögliche Lösungen untersuchen können.





# Ansichten von Strata Cloud Manager Command Center

Das Command Center bietet Ihnen vier verschiedene Ansichten, jede mit ihren eigenen erfassten Daten und Metriken, die Sie untersuchen und mit denen Sie interagieren können.

- Zusammenfassung
- Bedrohungen
- Betriebszustand
- Datensicherheit

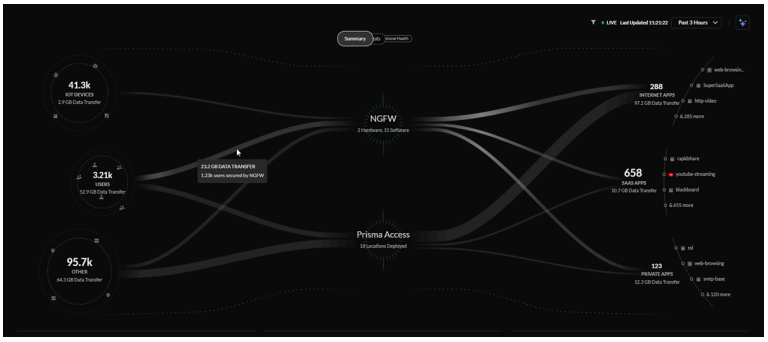
# Command Center (Zusammenfassung)

Die Ansicht **Zusammenfassung** bietet Ihnen einen Überblick über den gesamten Datenverkehr Ihrer Benutzer, externen Hosts, IoT-Geräte und Anwendungen sowie eine Vorschau einiger Probleme und Anomalien in Ihrem Netzwerk, die in den anderen Ansichten hervorgehoben werden. Mithilfe dieser Ansicht können Sie sich täglich auf einen Blick einen Überblick über die Integrität Ihres Netzwerks verschaffen.

| | |
|---|---|
| Lizenzzusammenfassung | • Sie müssen mindestens eine dieser Lizenzen besitzen, die eine Strata Logging Service-Lizenz zur Nutzung des Strata Command Center umfassen:<br>❑ Prisma Access-Lizenz<br>❑ „AIOps für NGFW Premium“-Lizenz<br>• oder eine „AIOPs für NGFW Free“-Lizenz zusammen mit einer Strata Logging Service-Lizenz<br>• Lizenzen, die für zusätzliche Metriken in der Übersicht benötigt werden:<br>❑ CDSS-Abonnements (Cloud-Delivered Security Services)<br>❑ Datensicherheitsabonnements<br>❑ ADEM-Lizenz<br>❑ KI-Zugriffslizenz |

## Zentrale Übersicht

Die zentrale Übersicht bietet einen Einblick in die Daten, die zwischen IoT-Geräten, Benutzern, externen Hosts, die auf Ressourcen aus dem Internet zugreifen, Internet-Apps, SaaS-Apps und privaten Anwendungen in Ihrem Netzwerk übertragen werden.



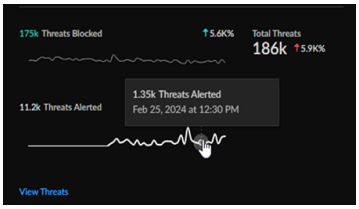

Die Linien in der zentralen Übersichtsansicht stellen die Datenübertragungen und den Datenverkehr in Ihrem Netzwerk dar, wobei die Dicke der Linien das von Quellen und Anwendungen übertragene Datenvolumen widerspiegelt.

Sie können sehen, wie diese Quellen durch Ihre Netzwerkinfrastruktur geschützt werden:

- Prisma Access-Bereitstellungen
- Next-Generation Firewalls aus Ihrem Strata Logging Service-Bestand

## Bedrohungen insgesamt

Mit dem Widget **Bedrohungen insgesamt** erhalten Sie schnell einen Überblick über die Gesamtzahl der in Ihrem Netzwerk erkannten Bedrohungen, einschließlich Informationen dazu, wie viele Bedrohungen blockiert wurden, wie viele Bedrohungen gemeldet wurden und wie sich die Bedrohungen im ausgewählten Zeitbereich verändert haben.




Navigieren Sie zum Activity Insights-Bildschirm **(Insights > Activity Insights > Bedrohungen),** um eine detailliertere Aufschlüsselung der Bedrohungen in Ihrem Netzwerk zu erhalten.

## Offene Vorfälle und Benutzererfahrung

Das Widget **Offene Vorfälle und Benutzererfahrung** bietet Ihnen einen Überblick über die Gesamtzahl der offenen Vorfälle, über die Aufschlüsselung der guten und potenziell beeinträchtigten Benutzererfahrung einzelner Segmente der Servicebereitstellungskette (von einem Benutzergerät zu einer Anwendung) sowie über die Veränderung bei offenen Vorfällen in einem ausgewählten Zeitbereich.


Navigieren Sie zum Dashboard „Anwendungserfahrung“ **(Dashboards > Anwendungserfahrung)**, um eine detailliertere Aufschlüsselung des Zustands und der Benutzererfahrung in Ihrem Netzwerk sowie entsprechende Leistungsmetriken zu erhalten.

## Top-Datenprofile nach Aktion

Mit den Widgets für **Top-Datenprofile** erhalten Sie Einblick in die wichtigsten vordefinierten Datenfilterprofile, die Anzahl der im Netzwerkverkehr gefundenen Übereinstimmungen und die auf Grundlage dieser Datenprofile ausgeführten Aktionen für vertrauliche Daten.

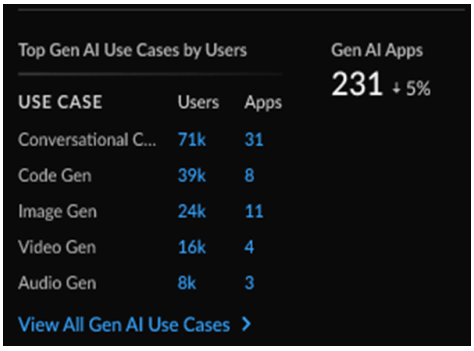

 

Klicken Sie durch bis zur Ansicht „Datensicherheit“ **(Command Center > Datensicherheit),** um eine detailliertere Aufschlüsselung der vertraulichen Daten in Ihrem Netzwerk zu erhalten.

## Top-GenAI-Anwendungsfälle nach Benutzern und GenAI-Apps

Das Widget **Top-GenAI-Anwendungsfälle nach Benutzer** bietet Ihnen einen Überblick über die Top-Anwendungsfälle für GenAI-Apps, die von Benutzern in Ihren Netzwerken verwendet werden. Außerdem erfahren Sie hier, wie viele Benutzer jeden Anwendungsfall verwenden und wie viele GenAI-Apps in jeden Anwendungsfall fallen.

Sie können auch die Gesamtzahl der GenAI-Apps in Ihren Netzwerken sowie die prozentuale Verschiebung der Apps basierend auf dem Zeitfilter sehen.




Navigieren Sie zum Dashboard „KI-Zugriffssicherheit“ **(Insights > KI-Zugriff)** in Activity Insights, um eine detailliertere Aufschlüsselung der GenAI-App-Einführung in Ihrem Netzwerk sowie Empfehlungen für einen besseren Schutz Ihrer Daten zu erhalten.

*Weitere Informationen zur KI-Zugriffssicherheit und dazu, wie Ihr Unternehmen GenAI-Anwendungen sicher einführen und gleichzeitig Risiken für Ihre Datensicherheit minimieren kann, finden Sie hier.*

# Bedrohungen

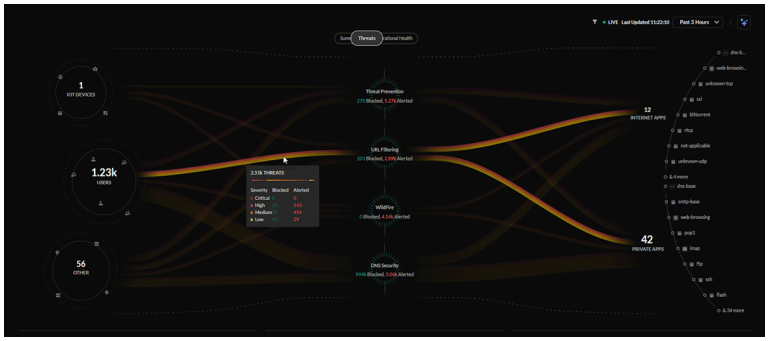
Die Ansicht **Bedrohungen** zeigt den Datenverkehr in Ihrem Netzwerk sowie die Bedrohungen, die von Ihren CDSS-Abonnements erkannt wurden. Mithilfe dieser Ansicht können Sie die blockierten und benachrichtigungsauslösenden Bedrohungen in Ihrem Netzwerk überwachen oder Bereiche in Ihrem Netzwerk untersuchen, die aktualisierte Richtlinien benötigen, um entsprechende Bedrohungen besser zu blockieren.

| | |
|---|---|
| Bedrohungslizenzen | • Bedrohungslizenzen, einschließlich:<br>❑ Bedrohungsabwehr-Lizenz<br>❑ URL-Filterungslizenz<br>❑ WildFire-Lizenz<br>❑ DNS Security-Lizenz |

## Zentrale Bedrohungsansicht

Die zentrale Bedrohungsansicht bietet einen Einblick in alle Bedrohungen in Ihrem Netzwerk, die von Ihren aktiven CDSS-Abonnements identifiziert wurden.

Die Bedrohungsansicht zeigt, wie Ihre Palo Alto Networks CDSS-Abonnements Ihren Datenverkehr schützen, indem sie potenzielle Bedrohungen in Ihrem Netzwerk überwachen. Das Command Center gibt Ihnen Einblick in den Prozentsatz des Datenverkehrs, der für Ihre IoT-Geräte, Benutzer und Anwendungen geprüft wurde, sowie in die Gesamtzahl der zugelassenen oder benachrichtigungsauslösenden Bedrohungen.

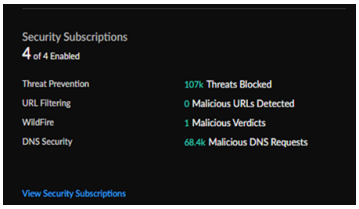



Die Linien in der zentralen Bedrohungsansicht stellen den Datenverkehr dar, der von Ihren Sicherheitsabonnements überwacht wird. Die Dicke steht für das Volumen der erkannten Bedrohungen und die Farbe für kritische, hohe, mittlere oder niedrige Bedrohungen.

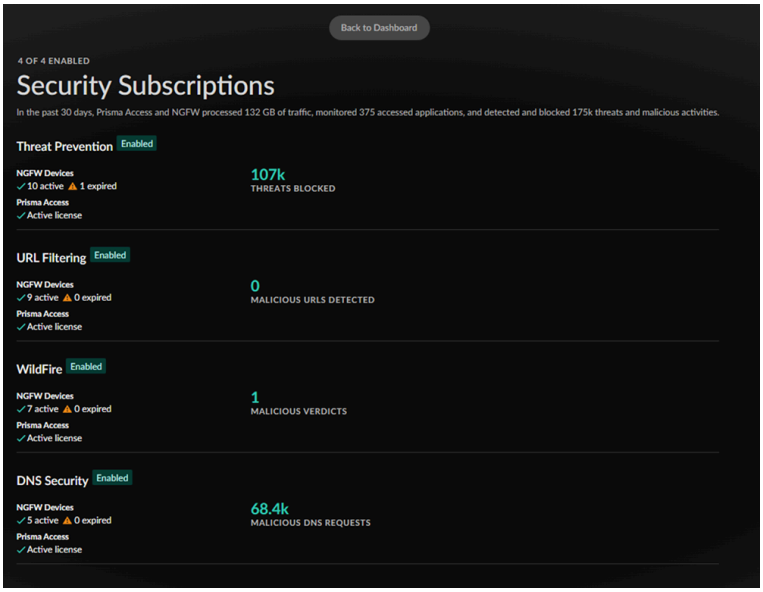
## Sicherheitsabonnements

Das Widget **Sicherheitsabonnements** gibt Ihnen einen Überblick über Ihre CDSS-Abonnements, verrät Ihnen, welche davon aktiv sind, und bietet einen Überblick darüber, wie sie Ihr Netzwerk schützen.

| Abonnement | Beschreibung |
|---|---|
| **Bedrohungsabwehr** | Die Bedrohungsabwehr schützt Ihr Netzwerk sowohl vor gängigen Bedrohungen, die weit verbreitet, aber nicht anspruchsvoll sind, als auch vor gezielten, fortschrittlichen Bedrohungen organisierter Cyberkrimineller. |
| **URL-Filterung** | Die erweiterte URL-Filterung ist unsere umfassende URL-Filterlösung, die Ihr Netzwerk und Benutzer vor webbasierten Bedrohungen schützt. |
| **WildFire** | Der cloudbasierte WildFire-Dienst zur Malware-Analyse nutzt Daten und Bedrohungsinformationen aus der größten globalen Community der Branche und wendet erweiterte Analysen an, um unbekannte Bedrohungen automatisch zu identifizieren und Angriffe im Keim zu ersticken. |
| **DNS Security** | Sichern Sie Ihren DNS-Verkehr automatisch mit dem DNS-Sicherheitsdienst von Palo Alto Networks. |



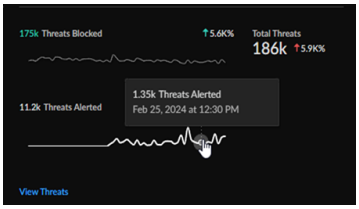

Wenn Sie auf das Widget **Sicherheitsabonnements (Command Center > Sicherheitsabonnements anzeigen)** klicken, erhalten Sie einen detaillierten Bericht über den Status Ihrer Abonnements in Bezug auf Ihre NGFW- und Prisma Access-Bereitstellungen. Klicken Sie auf **Zurück zum Dashboard**, um zur Ansicht **Bedrohungen** zurückzukehren.



## Bedrohungen insgesamt

Mit dem Widget **Bedrohungen insgesamt** erhalten Sie schnell einen Überblick über die Gesamtzahl der in Ihrem Netzwerk erkannten Bedrohungen, einschließlich Informationen dazu, wie viele Bedrohungen blockiert wurden, wie viele Bedrohungen gemeldet wurden und wie sich die Bedrohungen im ausgewählten Zeitbereich verändert haben.




Navigieren Sie zu Activity Insights **(Insights > Activity Insights > Bedrohungen)**, um eine detailliertere Aufschlüsselung der Bedrohungen in Ihrem Netzwerk zu erhalten.

## Blockierte und benachrichtigungsauslösende Bedrohungen

Das Widget **Blockierte und benachrichtigungsauslösende Bedrohungen** gibt Ihnen eine Übersicht über die Bedrohungen, die in Ihrem Netzwerk erkannt werden, und organisiert sie nach Kategorie, Bedrohungsstufe (kritisch, hoch, mittel und niedrig) und danach, ob die Bedrohungen blockiert wurden oder eine Benachrichtigung ausgelöst haben.


Sie können auch eine detaillierte Tabelle aller Bedrohungen anzeigen, die Ihr Netzwerk betreffen **(Insights > Activity Insights > Bedrohungen)**.

# Betriebszustand

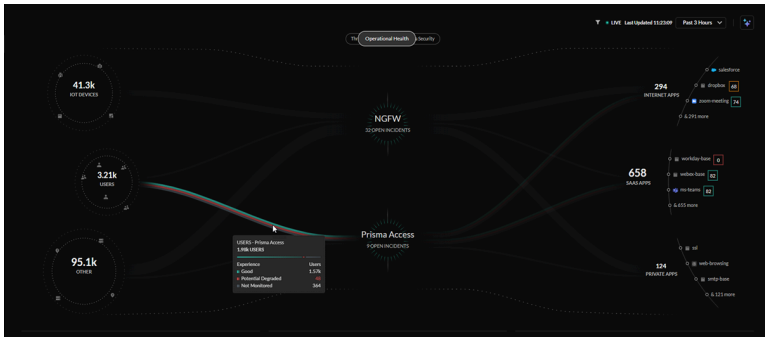
Die Ansicht **Betriebszustand** zeigt den Zustand der Infrastruktur und der Benutzererfahrung in Ihrem Netzwerk an. Mit dieser Ansicht können Sie den Zustand Ihrer NGFWs und Prisma Access-Bereitstellungen sowie die Benutzererfahrung in Ihrem Netzwerk überwachen und den Schweregrad offener Vorfälle in jedem Bereich überprüfen.

| | |
|---|---|
| Betriebszustand-Lizenzen | • Überwachungsabonnements, einschließlich:<br>❑ ADEM Observability<br>❑ KI-gestütztes ADEM<br>❑ AIOps für NGFW Premium |

## Zentrale Betriebszustandsansicht

Die zentrale Betriebszustandsansicht bietet einen Einblick in den Zustand der Infrastruktur und der Benutzererfahrung in Ihrem Netzwerk. Wenn Benutzer über eine ADEM-Lizenz (Autonomous Digital Experience Management) verfügen, erhalten sie in dieser Ansicht erweiterte Daten.

In der zentralen Betriebszustandsansicht wird angezeigt, wie Ihr Palo Alto Networks ADEM-Abonnement die digitale Erfahrung aller Benutzer und Anwendungen in Ihrer SASE-Umgebung überwacht.




Die Zeilen in der zentralen Betriebszustandsansicht repräsentieren alle Benutzer in Ihrem Netzwerk. Die Benutzer sind nach Benutzererfahrungsscore geordnet, wobei die Farben der Linien eine Bewertung von gut, schlecht oder unüberwacht darstellen.

## Offene Vorfälle insgesamt und Vorfälle nach Schweregrad

Das Widget **Offene Zustandsvorfälle nach Schweregrad** gibt Ihnen einen Einblick in alle offenen Vorfälle in Ihrem Netzwerk, aufgeschlüsselt nach Umfang (NGFW, Prisma Access und Prisma SD-WAN), Schweregrad und Anzahl der Vorfälle.

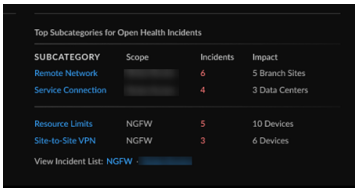

Das Widget verfolgt die prozentuale Änderung der offenen Vorfälle basierend auf dem ausgewählten Zeitraum.

Navigieren Sie zum Dashboard **Vorfälle und Benachrichtigungen** für jeden verfügbaren Umfang **(Vorfälle und Benachrichtigungen > Prisma Access / NGFW > Alle Vorfälle)**.

## Top-Unterkategorien für offene Zustandsvorfälle

Das Widget **Top-Unterkategorien für offene Zustandsvorfälle** gibt Ihnen einen Einblick in die Top-Unterkategorien der offenen Zustandsvorfälle in Ihrem Netzwerk, geordnet nach Umfang, Unterkategorie, Anzahl der Vorfälle und betroffenen Komponenten (Rechenzentren, Standorte, Geräte usw.).

Das Widget zeigt die fünf Top-Unterkategorien für einen einzelnen Umfang oder die beiden Top-Unterkategorien für mehrere Umfänge an, sofern verfügbar.




Navigieren Sie zum Dashboard **Vorfälle und Benachrichtigungen (Vorfälle und Benachrichtigungen > Prisma Access / NGFW / Prisma SD-WAN)**, um weitere Details zu den Vorfällen zu erhalten.

## Überprüfte Benutzer und Benutzererfahrung

Das Widget **Offene Vorfälle und Benutzererfahrung** bietet Ihnen einen Überblick über die Gesamtzahl der offenen Vorfälle, über die Aufschlüsselung der guten und potenziell beeinträchtigten Benutzererfahrung einzelner Segmente der Servicebereitstellungskette (von einem Benutzergerät zu einer Anwendung) sowie über die Veränderung bei offenen Vorfällen in einem ausgewählten Zeitbereich.


Navigieren Sie zum Dashboard **Anwendungserfahrung (Dashboards > Anwendungserfahrung)**, um eine detailliertere Aufschlüsselung der Erfahrung in Ihrem Netzwerk sowie entsprechende Leistungsmetriken zu erhalten.

# Best Practices

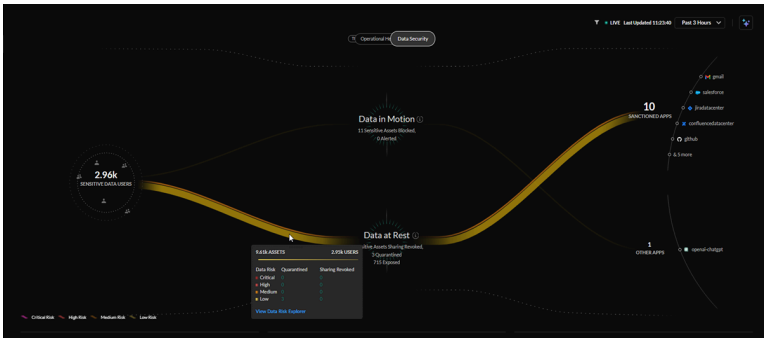
# Datensicherheit

In der Ansicht **Datensicherheit** werden alle vertraulichen Daten angezeigt, die in Ihrem Netzwerk und in verschiedenen verbundenen SaaS-Anwendungen erkannt wurden. Sie können sie verwenden, um hochriskante Datenflüsse in Ihrem Unternehmen zu überwachen und zu identifizieren.

| | |
|---|---|
| Datensicherheitslizenzen | • Datensicherheitslizenzen, einschließlich:<br>❑ SaaS-Sicherheitslizenz<br>❑ Datensicherheitslizenz<br>❑ Enterprise DLP-Lizenz |

## Zentrale Datensicherheitsansicht

Die zentrale Datensicherheitsansicht bietet eine Übersicht über sensible und hochriskante Daten in Ihrem Netzwerk sowie über verbundene SaaS-Anwendungen. Das Command Center gibt Ihnen Einblick in die Benutzer sensibler Daten innerhalb der Organisation, in die spezifischen sanktionierten, nicht sanktionierten, tolerierten oder ungetaggten Anwendungen, bei denen Aktivitäten mit sensiblen Daten erkannt wurden (Hochladen, Herunterladen oder offengelegte Assets), sowie in die Anzahl der erlaubten, blockierten, isolierten und widerrufenen Freigaben oder Offenlegungen von Inhalten.



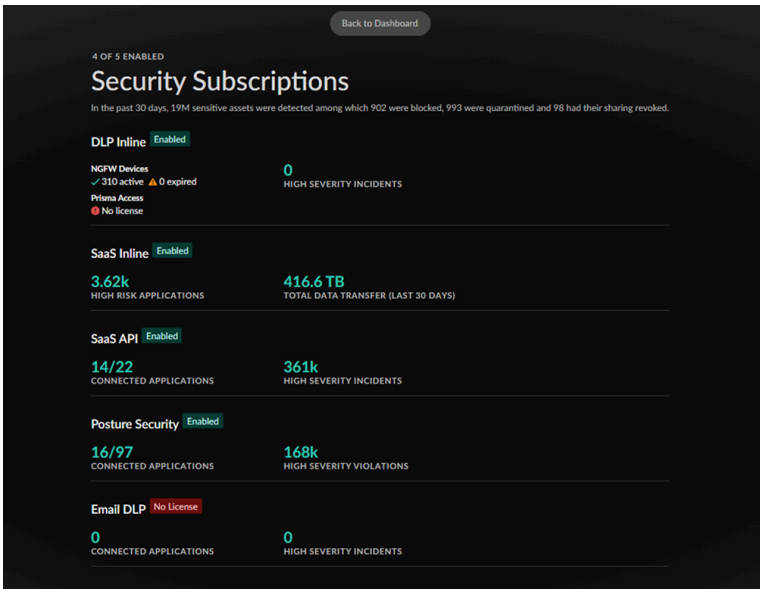

Die Linien in der zentralen Datensicherheitsansicht stellen sensible Daten dar, die durch Sicherheitslösungen für gespeicherte und übertragene Daten erkannt werden. Die Dicke der Linien steht für die Datenmenge und die Farbe gibt an, ob das Risiko dieser Daten als kritisch, hoch, mittel oder niedrig eingestuft wurde.

## Sicherheitsabonnements

Das Widget **Sicherheitsabonnements** gibt Ihnen einen Überblick über Ihre Datensicherheitsabonnements, verrät Ihnen, welche davon aktiv sind, und bietet einen Überblick darüber, wie sie Ihr Netzwerk schützen.

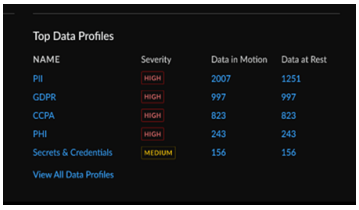
| Abonnement | Beschreibung |
|---|---|
| **DLP Inline** | Enterprise DLP ist ein cloudbasierter Dienst, der mithilfe von Algorithmen für überwachtes maschinelles Lernen sensible Dokumente in Kategorien einteilt, um sie vor Gefahren, Datenverlust und Datenexfiltration zu schützen. |
| **SaaS Inline** | Die SaaS Inline-Lösung arbeitet mit Strata Logging Service, um alle SaaS-Anwendungen zu ermitteln, die in Ihrem Netzwerk verwendet werden. |
| **SaaS-API** | Die SaaS-API ist ein cloudbasierter Dienst, den Sie über die API der Cloud-App direkt mit Ihren sanktionierten SaaS-Anwendungen verbinden können. So können Sie innerhalb der Anwendung Datenklassifizierung, Freigabe- oder Berechtigungstransparenz sowie Bedrohungserkennung bereitstellen. |
| **Sicherheitsstatus** | SaaS Security Posture Management (SSPM) hilft durch kontinuierliche Überwachung dabei, falsch konfigurierte Einstellungen in sanktionierten SaaS-Anwendungen zu erkennen und zu korrigieren. |
| **Email DLP** | Email DLP ist ein Add-on für Enterprise DLP, das durch KI-/ML-gestützte Datenerkennungen die Exfiltration von E-Mails mit vertraulichen Informationen verhindert. |


Wenn Sie auf das Widget **Sicherheitsabonnements (Command Center > Sicherheitsabonnements anzeigen)** klicken, erhalten Sie einen detaillierten Bericht über den Status Ihrer Abonnements in Bezug auf Ihre NGFW- und Prisma Access-Bereitstellungen. Klicken Sie auf **Zurück zum Dashboard**, um zur Ansicht **Datensicherheit** zurückzukehren.




## Top-Datenprofile

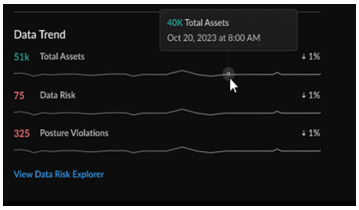
Das Widget **Top-Datenprofile** zeigt neben den wichtigsten Datenprofilen, die bei allen überprüften sensiblen Daten erkannt wurden, auch den Schweregrad des jeweiligen Datenprofils sowie einen Vergleich zwischen der Anzahl von Asset-Übereinstimmungen in übertragenen Daten und der Anzahl in gespeicherten Daten an.




Navigieren Sie zum Dashboard **Data Loss Prevention (Verwalten > Konfiguration > Data Loss Prevention)**, um alle vordefinierten Datenprofile zu überprüfen und benutzerdefinierte Datenprofile hinzuzufügen.

## Datentrend

Das Widget **Datentrend** zeigt den Trend bei vertraulichen Daten, die von Ihren Datensicherheitsabonnements überwacht werden. Es ist nach der prozentualen Veränderung der Gesamt-Assets, der Datenrisiken und der Sicherheitsverstöße geordnet.




Navigieren Sie zum Dashboard **Datenrisiko (Verwalten > Konfiguration > Data Loss Prevention > Datenrisiko)**, um Ihre allgemeine Datenrisikobewertung zu verstehen und praktische Empfehlungen zur Verbesserung der Datensicherheitsstatus Ihres Unternehmens zu erhalten.

# Insights: Activity Insights

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden<br>• Prisma SD-WAN | Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>☐ Prisma Access<br>☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>☐ Prisma SD-WAN<br>☐ Strata Cloud Manager Essentials<br>☐ Strata Cloud Manager Pro<br>Weitere Lizenzen und Voraussetzungen, die für den Zugriff auf bestimmte Activity Insights-Ansichten erforderlich sind:<br>☐ Strata Logging Service<br>☐ Cloud-Delivered Security Services (CDSS)<br>☐ ADEM-Beobachtbarkeit<br>☐ WAN Clarity-Berichterstattung<br>☐ eine Rolle mit der Berechtigung zum Anzeigen des Dashboards<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Activity Insights gibt Ihnen einen detaillierten Überblick über Ihre Netzwerkaktivitäten in Prisma Access- und NGFW-Bereitstellungen. Diese Ansicht vereint Ihre Netzwerkdaten an einem Ort, darunter Netzwerkverkehr, Anwendungsnutzung, Bedrohungen und Benutzeraktivitäten. Activity Insights bietet Visualisierungs-, Überwachungs- und Berichtsfunktionen, damit Sie Ihre Aufgaben problemlos ausführen können. Nachdem Sie mit dem Strata Cloud Manager Command Center die Bereiche identifiziert haben, auf die Sie sich konzentrieren müssen, navigieren Sie über die Kontextlinks zu Activity Insights oder anderen Dashboards, um dort weitere Analysen durchzuführen.

Activity Insights verfügt über erweiterte Filter, die Ihnen helfen, sich auf die Sicherheitsaspekte zu konzentrieren, die für Ihre Bereitstellung wichtig sind. Mit der Funktion Erweiterte Berichterstattung in Activity Insights können Sie aus den Daten auf der Registerkarte „Übersicht“ Berichte erstellen, herunterladen, teilen und planen. Der Bericht stellt die Daten für jeden im Dashboard angewendeten Filter separat dar. Alternativ können Sie Berichte für Activity Insights und Dashboards über das Menü **Strata Cloud Manager** > **Berichte** abrufen.

Starten Sie Strata Cloud Manager und klicken Sie auf **Insights** (), um zu beginnen.

**Was wird Ihnen in Activity Insights angezeigt?**

Activity Insights zeigt aggregierte Daten für jeden Strata Logging Service-Mandanten, der in Prisma Access- und NGFW-Umgebungen bereitgestellt wurde. Sie können die Daten für eine bestimmte Bereitstellung filtern. Activity Insights umfasst verschiedene Registerkarten. Jede dieser Registerkarten bietet eine einheitliche Ansicht der Netzwerkdaten hinsichtlich Anwendungen, Benutzern, Bedrohungen, URLs und Netzwerknutzung.

- **Übersicht** – zeigt die Daten für Anwendungen, Bedrohungen, Benutzer, URLs und Sitzungen, einschließlich der maximalen Anzahl an Aktivitäten innerhalb des ausgewählten Zeitbereichs. Durch einen Blick auf diese Ansicht können Sie schnell Unregelmäßigkeiten in Ihrem Netzwerk erkennen und dann tiefer in die Aktivitäten eintauchen, die eine Untersuchung erfordern.
- **Anwendungen** – Übersicht über die gesamte Anwendungsnutzung im Netzwerk, einschließlich Datenübertragung, Anwendungsrisiken und ADEM-Funktionen zur Überwachung der Anwendungserfahrung.
- **SD-WAN-Anwendungen** – zeigen Sie die Leistung von Prisma SD-WAN-Anwendungen an, einschließlich Transaktionsstatistiken, Metriken zur Bandbreitennutzung sowie Details zum Integritätsindex über einen bestimmten Zeitbereich.
- **Bedrohungen** – bietet eine ganzheitliche Ansicht aller Bedrohungen, die die Sicherheitsdienste von Palo Alto Networks in Ihrem Netzwerk erkannt und blockiert haben.
- **Benutzer** – bietet tiefere Einblicke in den Datenverkehr und die Aktivitäten eines Benutzers, einschließlich der ADEM-Funktionen zur Überwachung der Benutzererfahrung.
- **URLs** – zeigt die in Ihrem Netzwerk aufgerufenen URLs an. Das umfasst nicht nur Informationen dazu, wie viele davon bösartig sind und welche Benutzer und Anwendungen auf die URLs zugreifen, sondern auch zu den Regeln, die die URLs in Ihrem Netzwerk zulassen, sowie zur Durchsetzung durch Ihre Sicherheitsdienste.
- **Regeln** – bietet Einblicke in die Sicherheitsrichtlinien-Regeln, die den von Benutzern und Anwendungen generierten Datenverkehr zulassen; in die Bedrohungen, die in Datenverkehrssitzungen erkannt wurden; sowie in die URLs, die sich auf die jeweilige Regel auswirken.
- **Regionen** – zeigt die Netzwerkverkehrsdetails hinsichtlich Anwendungen, Benutzern, Bedrohungen und URLs.

**Wie können Sie die Daten aus dem Dashboard nutzen?**

Sie können die Erkenntnisse für Folgendes nutzen:

- Identifizieren Sie die Anwendungen, die Sie überwachen möchten, verbessern Sie die Benutzererfahrung der Anwendungen mit niedrigen Bewertungen und kontrollieren Sie nicht sanktionierte und riskante Anwendungen.
- Zeigen Sie die relevantesten Bedrohungen für Ihre Bereitstellung an und erhalten Sie Bedrohungskontext für die Untersuchung.
- Optimieren Sie Ihre Sicherheitsrichtlinienregeln und Verkehrsregeln basierend auf Ihren Erkenntnissen aus den Protokollen, um Sicherheitslücken zu schließen.
- Überwachen Sie die Benutzeraktivität, um potenzielle Bedrohungen zu erkennen und aufzuhalten und den Missbrauch vertraulicher Informationen zu verhindern.

# Activity Insights: Übersicht

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden<br>• Prisma SD-WAN | Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>❑ Prisma Access<br>❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>❑ Prisma SD-WAN<br>❑ Strata Cloud Manager Essentials<br>❑ Strata Cloud Manager Pro<br>Weitere Lizenzen und Voraussetzungen, die für den Zugriff auf bestimmte Activity Insights-Ansichten erforderlich sind:<br>❑ Strata Logging Service<br>❑ Cloud-Delivered Security Services (CDSS)<br>❑ ADEM-Beobachtbarkeit<br>❑ WAN Clarity-Berichterstattung<br>❑ eine Rolle mit der Berechtigung zum Anzeigen des Dashboards<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Zeigen Sie die Zusammenfassung der am häufigsten beobachteten Anwendungen, Bedrohungen, Benutzer, URLs und Regeln in Ihrem Netzwerk für den ausgewählten Zeitraum an. Durch einen Blick auf diese Ansicht können Sie schnell Unregelmäßigkeiten in Ihrem Netzwerk erkennen und dann tiefer in die Aktivitäten eintauchen, die eine Untersuchung erfordern. Die Übersicht enthält Folgendes:

- Top-5-Anwendungen und -Anwendungskategorien in Ihrem Netzwerk mit maximaler Aktivität hinsichtlich der Sitzungsanzahl, der Datenübertragung, erkannter Bedrohungen, aufgerufener URLs und Benutzern, die auf die Anwendungen zugegriffen haben. Klicken Sie auf **Alle Anwendungen anzeigen**, um die Anwendungsdetails anzuzeigen.

- Top-5-Bedrohungen und -Bedrohungskategorien, die Sitzungen, Benutzer und Anwendungen am stärksten betreffen. Details zu Sitzungen, Benutzern und Anwendungen können Sie auf den Registerkarten Protokollanzeige, Benutzer und Anwendungen anzeigen.

- Netzwerkverkehrstrend hinsichtlich der blockierten, erlaubten und benachrichtigungsauslösenden Sitzungen, der übertragenen Datenmenge sowie der Nutzer, die den meisten Datenverkehr generieren.

- Top-5-Nutzer mit den meisten Datenverkehrssitzungen, übertragenen Daten, Bedrohungen im Datenverkehr, aufgerufenen URLs und Benutzererfahrungsscores für überwachte Anwendungen.
- Am häufigsten aufgerufene URLs zusammen mit Details zu Sitzung, Benutzern und Anwendungen, die auf die URLs zugreifen.

- Top 5 der am stärksten betroffenen Sicherheitsrichtlinienregeln, die in Ihrer Bereitstellung konfiguriert wurden – mit Filtern, um die Sitzungen, Benutzer, URLs, Bedrohungen, übertragene Daten sowie Anwendungen, die am Datenverkehr beteiligt sind, entsprechend den Regeln zu untersuchen.

Sie können die Filter verwenden, um die Datenpunkte anzuzeigen, auf die Sie sich konzentrieren möchten und die für Ihre Bereitstellung relevant sind. Diese Filter sind in allen Registerkarten des Dashboards verfügbar.

## Filter

Activity Insights verfügt über erweiterte Filter, die Ihnen helfen, sich auf die Sicherheitsaspekte zu konzentrieren, die für Ihre Bereitstellung wichtig sind. Folgende Filter sind verfügbar:

- **Zeitbereich** – Anzeige von Daten für einen bestimmten Zeitraum
- **Auswahl des Umfangs** – bereitstellungsspezifische Daten: Prisma Access, NGFW
- **Untermandant** – die Prisma Access-Instanz, für die die Daten angezeigt werden
- **Benutzername** – Anzeige der Aktivitäten eines einzelnen Benutzers
- **Anwendung** – Netzwerkereignisse zu einer bestimmten Anwendung
- **Anwendungstyp** – Art der Anwendung: SaaS, Internet, privat
- **Bedrohungskategorie** – Daten für eine bestimmte Bedrohungskategorie
- **Bedrohungsaktion** – spezifische Ansicht für erlaubte oder blockierte Bedrohungen
- **URL-Risikostufe** – Daten zu URLs mit einem spezifischen Risikolevel (hoch, mittel oder niedrig)
- **URL-Kategorie** – Filtern der Daten anhand der URL-Kategorien
- **Quellort** – Anzeige der Aktivitäten, die von einem bestimmten Standort stammen
- **Zielort** – Anzeige der Aktivität für eine bestimmte Region
- **URL** – Aktivität in Bezug auf eine bestimmte aufgerufene URL
- **SaaS-Anwendung** – Daten zu einer bestimmten SaaS-Anwendung
- **Sanktionierte Anwendung** – Anzeige von Daten nur für sanktionierte oder nicht sanktionierte Anwendungen

- **Porttyp** – Sortieren des Anwendungsdatenverkehrs, der standardmäßige oder andere Ports durchläuft
- **Protokoll** – Anzeige des Datenverkehrs, der einen bestimmten TCP-, UDP- oder HTTP-Port verwendet
- **Quelltyp** – Anzeige der Aktivitäten, die von bestimmten Geräten, Benutzern oder anderen Elementen generiert wird

## Berichte

Klicken Sie auf der Registerkarte **Übersicht** auf eines der Symbole  , um aus den Daten auf der Registerkarte **Übersicht** Berichte zu erstellen, herunterzuladen, zu teilen und zu planen. Sie können Berichte auch über das Menü**Strata Cloud Manager** > **Berichte** planen; klicken Sie auf das Symbol  und wählen Sie aus dem Dropdown-Menü **Typ** die Option „Activity Insights – Zusammenfassung“ aus.

# Activity Insights: Anwendungen

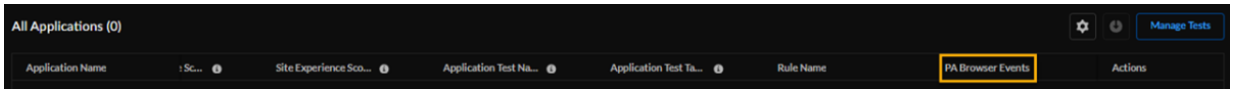
| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)*<br>• NGFWs<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)* | Um Activity Insights nutzen zu können, müssen Sie über mindestens eine der folgenden Lizenzen verfügen:<br>❑ Prisma Access<br>❑ AIOps for NGFW Free (use the AIOps for NGFW Free app) oder AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>Zum Anzeigen der Registerkarte „Activity Insights: Anwendungen“ sind zusätzlich folgende Lizenzen erforderlich:<br>❑ Strata Logging Service<br>❑ ADEM Observability schaltet zusätzliche Prisma Access-Funktionen frei. |

Überwachen Sie die Anwendungen in Ihren Prisma Access- und NGFW-Setups, die Benutzer, die die Anwendung verwenden, Risikoscores sowie die Benutzererfahrung jeder Anwendung an und ermitteln Sie die Sicherheitsauswirkungen riskanter Anwendungen. Erkenntnisse über die Anwendungsnutzung helfen Ihnen bei der Optimierung Ihrer Sicherheitsrichtlinie zur Kontrolle nicht sanktionierter und riskanter Anwendungen. Klicken Sie auf **Activity Insights > Anwendungen**, um die folgenden Informationen anzuzeigen:

- **Anwendungen nach Risikoscore** – die Gesamtzahl der in Ihrer Organisation ausgeführten Anwendungen sowie die Anzahl der Anwendungen mit „Gut“, „Angemessen“ oder „Schlecht“. Die Anwendungen werden auf Grundlage der Bewertung der Anwendungserfahrung in die Kategorien „Gut“, „Angemessen“ und „Schlecht“ eingeteilt.
- **Anwendungsdatenübertragung** – gesamter Daten-Download und -Upload über NGFW- und Prisma Access-Firewalls während des ausgewählten Zeitbereichs. Sie können filtern, um die Datenübertragungen anzuzeigen, die aus der Anwendungskategorie stammen und vom Gerät (Rechenzentrum oder Firewall) aus das Ziel durchlaufen.
- **Alle Anwendungen** – Verwenden Sie dieses Widget, um zu sehen, in welchen überwachten Prisma Access-Anwendungen synthetische Tests ausgeführt werden und welche Anwendungen in Ihren NGFW-Umgebungen ausgeführt werden. In der Tabelle sind auch die Erfahrungsbewertungen aufgeführt, die Aufschluss über den Zustand der einzelnen Anwendungen geben. Wenn Sie ein Prisma Access Browser-Abonnement haben, wird eine

Spalte für **PA Browser-Ereignisse** angezeigt. Wählen Sie die Anzahl der Ereignisse aus, um zu den Prisma Access Browser-Verwaltungsseiten weitergeleitet zu werden.




Sie können die Daten in der Tabelle im CSV-Format herunterladen (nur Prisma Access-Anwendungen). Klicken Sie auf die Schaltfläche **Tests verwalten**, um alle synthetischen Tests anzuzeigen, die für sämtliche Prisma Access-Anwendungen in der Tabelle „Anwendungstests“ eingerichtet sind. Wenn Sie einen Test zum Überwachen einer Anwendung erstellen möchten, klicken Sie in der Spalte „Benutzererfahrung“ auf **Anwendung auf Zustand überprüfen**.

- **Anwendungsdetails** – zeigen Sie allgemeine Details der Anwendung sowie Details zur Anwendungsaktivität und -erfahrung an.
  - Auf der Registerkarte **Aktivität** werden die Gesamtzahl der in der Anwendung erkannten Bedrohungen, die Gesamtzahl der Benutzer, die auf die Anwendung zugreifen, die Daten, die über die Anwendung übertragen werden, PA-Browser-Datenereignisse sowie PA-Browser-Zugriffsereignisse angezeigt.

    Das folgende Bild zeigt Anwendungsdetails zu **PA-Browser-Datenereignissen** und **PA-Browser-Zugriffsereignissen**. In der Standardansicht wird eine **Zusammenfassung** aller Ereignisse und blockierten Ereignisse angezeigt. Sie können sich aber auch eine **Aufschlüsselung** nach **Ereignistyp** und **Anzahl** anzeigen lassen.

  - Auf der Registerkarte **Erfahrung** werden die Bewertung der Anwendungserfahrung, der Bewertungstrend während des ausgewählten Zeitbereichs sowie Netzwerkleistungsmetriken angezeigt.

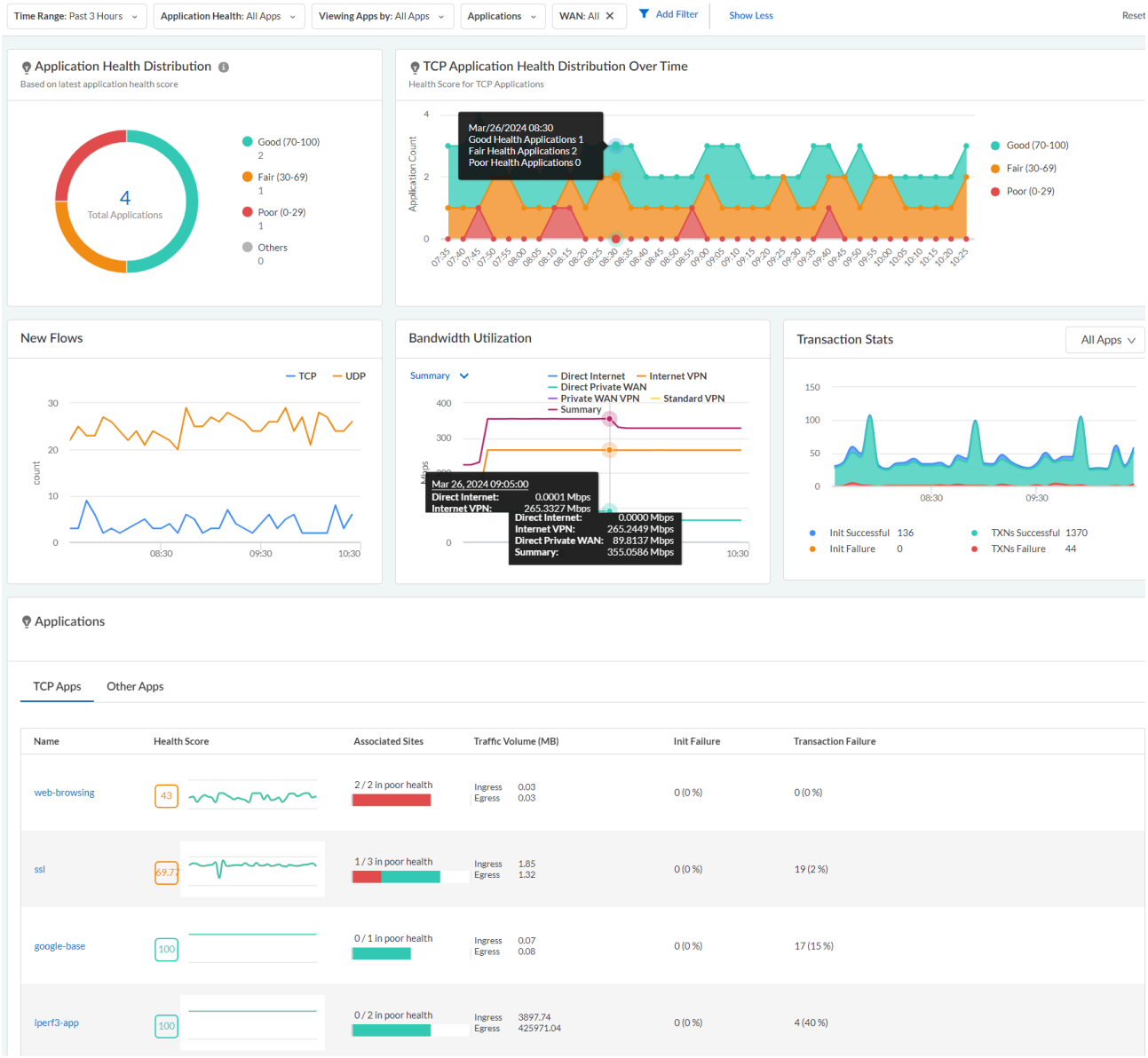
*Wenn es sich bei einer App um eine Container-App handelt, stellen die angezeigten Statistiken eine Zusammenfassung aller Anwendungen im Container dar. Beispielsweise ist Gmail eine Container-App (es gibt keine Anwendungs-ID für Gmail). Die Lösung gruppiert Anwendungen wie gmail-posting, gmail-downloading, gmail-uploading und so weiter. Der für diese Container-App festgelegte Risikoscore ist der höchste Risikoscore, der für die enthaltenen Anwendungen gefunden wurde. Alle anderen Metriken werden berechnet, indem die für die enthaltenen Anwendungen gefundenen Werte summiert werden.*

**Berichte** – Sie können keinen Bericht erstellen, der die Daten in dieser Ansicht abdeckt. Sie können jedoch den Bericht **Anwendungsnutzung** verwenden, um Daten zur Anwendungsnutzung in Ihrem Netzwerk anzuzeigen. Um einen Bericht zu planen, klicken Sie im Menü **Strata Cloud Manager** > **Berichte** auf das Symbol und wählen Sie aus der Dropdown-Liste **Typ** die Option „Anwendungsnutzung“ aus.

# Activity Insights: SD-WAN-Anwendungen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma SD-WAN | ❑ Prisma SD-WAN-Lizenz<br>❑ WAN Clarity Reporting-Lizenz zum Anzeigen bestimmter Widgets |

Sehen Sie sich die Top-Anwendungen an, die in Prisma SD-WAN nicht gut funktionieren. Sehen Sie den ermittelten Zustandsscore aller schlechten Anwendungen, eine Liste der schlechten Anwendungen für einen Mandanten basierend auf dem Zustandsscore sowie den durchschnittlichen Zustandsscore schlechter Anwendungen für die letzten 3 Stunden in 5-Minuten-Intervallen.



- **Anwendungszustandsverteilung** (erfordert Lizenz für WAN Clarity): Die Verteilung von Anwendungen mit den Bewertungen „Gut“, „Angemessen“ und „Schlecht“ für einen bestimmten Mandanten.
- **TCP-Anwendungszustandsverteilung im Zeitverlauf** (erfordert Lizenz für WAN Clarity): Die Verteilung von Anwendungen mit guter, angemessener und schlechter TCP-Anwendungszustandsverteilung in einem bestimmten Zeitraum. Das Zeitreihendiagramm sollte basierend auf der gewählten Dauer berechnet und aktualisiert werden. Unterstützte Dauern sind beispielsweise 1 Stunde, 3 Stunden, 1 Tag, 7 Tage, 30 Tage und 90 Tage; das Intervall beträgt 1 Minute, 5 Minuten, 1 Stunde bzw. 1 Tag.
- **Neue Flüsse**: Zeigt die neuen TCP- und UDP-Datenverkehrsflüsse für eine Anwendung, einen bestimmten Satz von Anwendungen oder alle Anwendungen in einem bestimmten Zeitraum an. Ein TCP-Fluss wird als neuer Datenverkehrsfluss betrachtet, wenn er das erste SYN-Paket erkennt. Ein UDP-Fluss wird als neuer Fluss betrachtet, wenn er das erste UDP-Paket in einer der beiden Richtungen erkennt. Ein Datenverkehrsfluss ist eine Folge von Paketen in beide Richtungen, die durch die Quell- und Ziel-IP-Adresse, den Quell- und Zielport sowie das Protokoll identifiziert werden.
- **Bandbreitennutzung**: Das Diagramm zur Bandbreitennutzung zeigt die Menge der Bandbreite, die auf einem Pfad in einem Netzwerk verwendet wird. Verwenden Sie das Diagramm, um WAN-Überlastungen im Netzwerk zu identifizieren, die die Anwendungsleistung beeinträchtigen können. Es bietet eine visuelle Darstellung der Bandbreitenspitzen, der gesamten von einem bestimmten Standort verbrauchten Bandbreite sowie der Anwendung und gibt an, ob der Upload in Eingangs- oder Ausgangsrichtung erfolgt. Fahren Sie mit dem Mauszeiger über das Diagramm „Bandbreitennutzung“, um eine detailliertere Ansicht der Bandbreitenauslastung einer Anwendung oder eines bestimmten Zeitpunkts zu erhalten. Typischerweise werden die Anwendungen nach ihrer Bandbreitennutzung sortiert.
- **Transaktionsstatistiken**: Bietet Transaktionsstatistiken über TCP-Flüsse, einschließlich Initiierungs-/Transaktionserfolgen und -fehlschlägen für eine bestimmte Anwendung oder alle Anwendungen, für einen bestimmten Pfad oder für alle Pfade sowie für alle Zustandsereignisse.
- **Anwendungen**: Listet alle Anwendungsdetails auf, darunter Name, Anwendungsprofil, Zustandsscore, betroffene Standorte, Datenverkehrsvolumen, Initiierung/Fehlschlag und Transaktion/Fehlschlag. Wenn Sie auf den Anwendungsnamen klicken, sehen Sie die einzelnen Anwendungsdetails auf einer neuen Seite.

# Activity Insights: Bedrohungen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)*<br>• NGFWs<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)* | Um Activity Insights nutzen zu können, müssen Sie über mindestens eine der folgenden Lizenzen verfügen:<br>☐ Prisma Access<br>☐ AIOps for NGFW Free (use the AIOps for NGFW Free app) oder AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>☐ Strata Cloud Manager Essentials<br>☐ Strata Cloud Manager Pro<br>Zum Anzeigen der Registerkarte „Activity Insights: Bedrohungen“ sind zusätzlich folgende Lizenzen erforderlich:<br>☐ Strata Logging Service<br>☐ CDSS-Lizenzen<br>☐ ADEM Observability schalten zusätzliche Prisma Access-Funktionen frei. |

Verschaffen Sie sich einen ganzheitlichen Überblick über die Bedrohungsaktivitäten und die verschiedenen Arten von Bedrohungen, die in Ihrem Netzwerk auftreten. Die Registerkarte zeigt die Gesamtzahl der Bedrohungssitzungen, die in Ihren Prisma Access- und NGFW-Bereitstellungen aufgetreten sind, sowie eine Aufschlüsselung der Zahlen basierend auf der Bedrohungskategorie und dem Schweregrad der Bedrohung für den ausgewählten Zeitraum. Sie können nach einem Sicherheitsartefakt (Datei-Hash, URL, Domäne oder IP-Adresse [IPv4 oder IPv6]) suchen, das mit einer Bedrohung verknüpft ist, um die Bedrohungsdatenanalyse von Palo Alto Networks und die Analyseergebnisse von Drittanbietern zu prüfen.

Überprüfen Sie die folgenden Details zu einzelnen Bedrohungen in Ihrem Netzwerk:

- **Bedrohungsname** – Name der Bedrohungssignatur. Hier finden Sie die neuesten Threat Vault-Informationen über die Bedrohung, einschließlich aller Bedrohungssitzungen während eines bestimmten Zeitbereichs.
- **Bedrohungs-ID** – eindeutige ID der Bedrohungssignatur. Verwenden Sie die Bedrohungs-ID, um nach den neuesten Informationen zu suchen, die die Bedrohungsdatenbank von Palo Alto Networks für diese Signatur enthält.
- **Bedrohungskategorie und Unterkategorie** – der Bedrohungstyp basierend auf Bedrohungssignaturen (Antivirus, Spyware [C2] und Sicherheitslücke).
- **Lizenzen** – die Sicherheitsdienste von Palo Alto Networks, die die Bedrohung erkannt haben.

- **Schweregrad** – Der Schweregrad der Bedrohung wird basierend darauf bestimmt, wie einfach es ist, die Sicherheitslücke auszunutzen, wie weit verbreitet das anfällige Produkt ist, welche Auswirkungen die Sicherheitslücke hat und vieles mehr. Der Schweregrad wird wie folgt kategorisiert:
  - Kritisch – wenn die Sicherheitslücke Standardinstallationen sehr weit verbreiteter Software betrifft und die Exploits dazu führen können, dass der Root kompromittiert wird. Der Exploit-Code (Informationen darüber, wie der Systemcode, die Methoden, der Proof of Concept [POC] ausgenutzt werden können) ist weit verbreitet und leicht zu nutzen. Angreifer benötigen keine speziellen Authentifizierungsdaten oder Kenntnisse über einzelne Opfer.
  - Hoch – Bedrohungen, die kritisch werden können, aber abmildernde Faktoren haben, beispielsweise weil sie schwer auszunutzen sind, nicht zu erhöhten Berechtigungen führen oder es nicht viele potenzielle Opfer gibt.
  - Mittel – kleinere Bedrohungen, bei denen die Auswirkungen minimal sind, wie z. B. DoS-Angriffe, die das Ziel nicht gefährden, oder Exploits, die erfordern, dass sich ein Angreifer im selben LAN wie das Opfer befindet. Sie betreffen nur nicht standardmäßige Konfigurationen, verschleiern Anwendungen lediglich oder bieten sehr eingeschränkten Zugriff.
  - Niedrig – Bedrohungen der Stufe „Warnung“, die nur sehr geringe Auswirkungen auf die Infrastruktur einer Organisation haben. Sie erfordern normalerweise einen lokalen oder physischen Systemzugriff und können häufig zu Datenschutz- oder DoS-Problemen des Opfers sowie zu Informationslecks führen.
  - Informativ – verdächtige Ereignisse, die keine unmittelbare Bedrohung darstellen, die aber gemeldet werden, um die Aufmerksamkeit auf tiefgreifendere Probleme zu lenken, die möglicherweise existieren.
- **Sitzungen insgesamt** – die Anzahl der Sitzungen, in denen die Bedrohung erkannt wurde. Klicken Sie auf den Namen der Bedrohung, um alle zugehörigen Bedrohungssitzungen im angegebenen Zeitbereich anzuzeigen. Die Bedrohungssitzungstabelle enthält Kontext zur Bedrohung, z. B. den Zeitpunkt, zu dem die Sicherheitsdienste von Palo Alto Networks die Bedrohung erkannt haben, die Benutzer, Regeln, Anwendungen und Geräte, die von der Bedrohung betroffen sind, sowie die für die Bedrohung ergriffenen Maßnahmen (Zulassen oder Blockieren).
- **Benutzer insgesamt** – Anzahl der Benutzer, die der Bedrohung ausgesetzt sind.
- **Zulässige und blockierte Bedrohungen** – Überprüfen Sie die für die Bedrohung durchgesetzte Aktion, um sicherzustellen, dass die Aktionen keine Fehlalarme (False Positives) in Ihrem Netzwerk auslösen.
- **Aktionen** – Untersuchen Sie den Protokollverlauf der Bedrohung im Protokoll-Viewer.

**Berichte** – Sie können keinen Bericht erstellen, der die Daten in dieser Ansicht abdeckt.

# Activity Insights: Users (Benutzer)

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)*<br>• NGFWs<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)* | Um Activity Insights nutzen zu können, müssen Sie über mindestens eine der folgenden Lizenzen verfügen:<br>❑ Prisma Access<br>❑ AIOps for NGFW Free (use the AIOps for NGFW Free app) oder AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>❑ Strata Cloud Manager Essentials<br>❑ Strata Cloud Manager Pro<br>Zum Anzeigen der Registerkarte „Activity Insights: Benutzer“ sind zusätzlich folgende Lizenzen erforderlich:<br>❑ Strata Logging Service<br>❑ Advanced URL Filtering-Lizenz<br>❑ Cloud Identity Engine-Lizenz<br>❑ Advanced Threat Prevention-Lizenz<br>❑ ADEM Observability schaltet zusätzliche Prisma Access-Funktionen frei. |

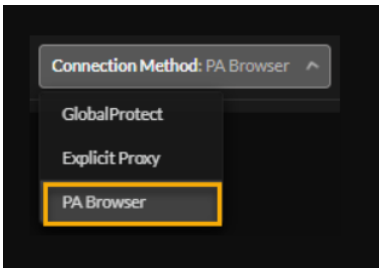
Überwachen Sie die Benutzeraktivität in Ihren Prisma Access- und NGFW-Umgebungen. Sie können Daten für Benutzer anzeigen, die eine Verbindung zu den Prisma Access- und NGFW-Sicherheitsdiensten herstellen – entweder über die GlobalProtect-App auf ihren Geräten oder per explizitem Proxy über einen Webbrowser auf ihren Geräten. Durch die Überwachung der Benutzeraktivität können Sie potenzielle Bedrohungen erkennen und aufhalten, den Missbrauch vertraulicher Informationen verhindern und Ihre Sicherheitsrichtlinienregeln anpassen, um Sicherheitslücken zu schließen.

Sie können die Benutzerdaten wie folgt filtern:

- Bereitstellung: Prisma Access, NGFW
- Verbindungsmethoden und Versionen: GlobalProtect, expliziter Proxy, Prisma Access Browser
- Benutzername
- Gerätename
- Ursprungsort des Datenverkehrs und Prisma Access-Standorte
- Von Benutzern aufgerufene Anwendungen und Benutzererfahrungsscore-Filter

Sehen Sie sich hier die folgenden Details an:

- **Verbundene/aktive Benutzer** – Überwachen Sie aggregierte Daten zu Benutzern, die derzeit über GlobalProtect, explizites Proxy für mobile Benutzer und Prisma Access Browser verbunden sind.




  Zeigen Sie die Anzahl der Benutzer an, die zum Zeitpunkt des Datenabrufs oder Zeitstempels mit Ihrem Netzwerk verbunden waren. Sie können **Trends anzeigen nach Benutzern** oder nach **Benutzergeräten**. Wählen Sie die Nummer aus, um in der Tabelle **Verbundene Benutzer | Verbundene Benutzergeräte** Details zu allen verbundenen Benutzern und all ihren Geräten anzuzeigen.

  Zeigen Sie Daten zum Zugriff mit dynamischen Rechten in **Trends anzeigen nach Benutzern** oder **Benutzergeräten**, **Verbundene Benutzer | Verbundene Benutzergeräte** und **Projektverteilung nach Schauplatz** an.
- **Überwachte Benutzer** – Zeigen Sie die Gesamtzahl der von ADEM überwachten Benutzer oder Benutzergeräte sowie ihre durchschnittliche Benutzererfahrung an. Dabei handelt es sich um den aggregierten Erfahrungsscore aller von ADEM überwachten Benutzer. Klicken Sie auf die Zahl, um Benutzeraktivitätsdetails in Bezug auf die Benutzererfahrung anzuzeigen.
- **Riskante Benutzer** – Zeigen Sie die Anzahl der Benutzer an, die von Bedrohungen betroffen sind. Der Aufwärts- oder Abwärtspfeil vergleicht diesen Zeitbereich mit einem vorherigen Zeitbereich, um die prozentuale Differenz der Anzahl verbundener Geräte anzugeben. Wählen Sie „Weitere Details anzeigen“ für „GlobalProtect-Versionen“ oder „IP-Pool-Auslastung“ aus, um Details zu riskanten Benutzern in Ihrer Umgebung anzuzeigen.
- **GlobalProtect-Versionsdetails** zeigt die GlobalProtect-Versionen, die auf Ihren Geräten installiert sind. Sie können sehen, wie viele Benutzer mit jeder Version eine Verbindung herstellen. Verwenden Sie die Daten, um die Einhaltung der neuesten GlobalProtect-App-Version durchzusetzen. Bewegen Sie den Mauszeiger über die Verteilungstrendlinien, um die IP-Adressen der zu diesem Zeitpunkt verbundenen Benutzer anzuzeigen.
- **Zeigen Sie die IP-Pool-Auslastung** nach verschiedenen IP-Pool-Zuweisungsschauplätzen an, basierend auf der Anzahl der zu diesem Zeitpunkt verbundenen Benutzer. Der Prozentsatz der IP-Pool-Auslastung im Diagramm gibt die Anzahl der genutzten IP-Pool-Blöcke im Verhältnis zu allen IP-Pool-Blöcken an, die in allen Subnetzen verfügbar sind. Sie können proaktiv Maßnahmen ergreifen, indem Sie Subnetze hinzufügen, wenn Sie sehen, dass eine IP-Pool-Leiste die maximale Kapazität für eine beliebige Region erreicht.
- In der Tabelle **Benutzer** werden Informationen zu den Benutzern angezeigt, die im angegebenen Zeitbereich angemeldet waren. Klicken Sie auf den Benutzernamen, um Einblick in die Browsingmuster einzelner Benutzer zu erhalten: die am häufigsten besuchten Websites,

die Websites, über die sie Daten übertragen, sowie Versuche, auf Websites mit hohem Risiko zuzugreifen.

- **Bedrohungen**
  - **Browsingübersicht** – Sehen Sie, an welche Websitetypen der Benutzer die meisten Daten übertragen hat, sowie die Anzahl der Websitebesuche des Benutzers.
  - **Top 10 der am meisten besuchten URL-Kategorien** – Zeigen Sie die beliebtesten URL-Kategorien für den Benutzer basierend auf der Datenübertragung an. Sie können auch die Anzahl der eindeutigen besuchten URLs sehen, die in jede URL-Kategorie fallen.
  - **URL-Browsingübersicht** – Überwachen Sie die vom Benutzer besuchten eindeutigen URLs auf Besuche bösartiger und riskanter URLs. Diese Websites können Ihr Netzwerk Bedrohungen, Datenverlusten und Complianceverstößen aussetzen. Wenn Sie mehr Besuche auf diesen Seiten feststellen, als Sie erwarten würden, passen Sie Ihre Sicherheitsrichtlinienregeln an, um die Lücken zu schließen.
  - **Top-10-URLs** – überprüfen Sie die Risikostufe der vom Benutzer am häufigsten besuchten Websites. URLs mit hohem Risiko müssen überwacht werden, da sie Ihr Netzwerk wahrscheinlich Bedrohungen aussetzen.
  - **Blockierte URLs nach Risiko** – Dies sind die blockierten URLs, auf die der Benutzer am häufigsten zuzugreifen versucht hat. Überprüfen Sie die URL-Filterprotokolle und prüfen Sie, ob Sie die Sicherheitsrichtlinienregel anpassen müssen, um die Aktion zu ändern.
  - **Schwerwiegende Bedrohungen** – Zeigen Sie die Gesamtzahl der für den Benutzer erkannten Bedrohungen sowie Statistiken zum Schweregrad der Bedrohungen an. Vergleichen Sie die Zahlen mit anderen Benutzern. Passen Sie die Sicherheitsrichtlinie an, wenn die Zahlen ungewöhnlich hoch sind.
  - **Schwerste Bedrohungen** – Dies sind die für den Benutzer am häufigsten erkannten Bedrohungen.
- **Konnektivität** – zeigt den Trend der Geräte, bei denen der Benutzer während eines bestimmten Zeitraums angemeldet ist, sowie die Geräteverbindungsdetails für jedes An- und Abmeldeereignis des Benutzers.
- **Erfahrung** – stellt die Benutzererfahrungsdaten für das Gerät, den Erfahrungsscore und -trend für jede der überwachten Anwendungen sowie Leistungsmetriken für den überwachten Benutzer und die überwachten Anwendungen für einzelne Geräte bereit.

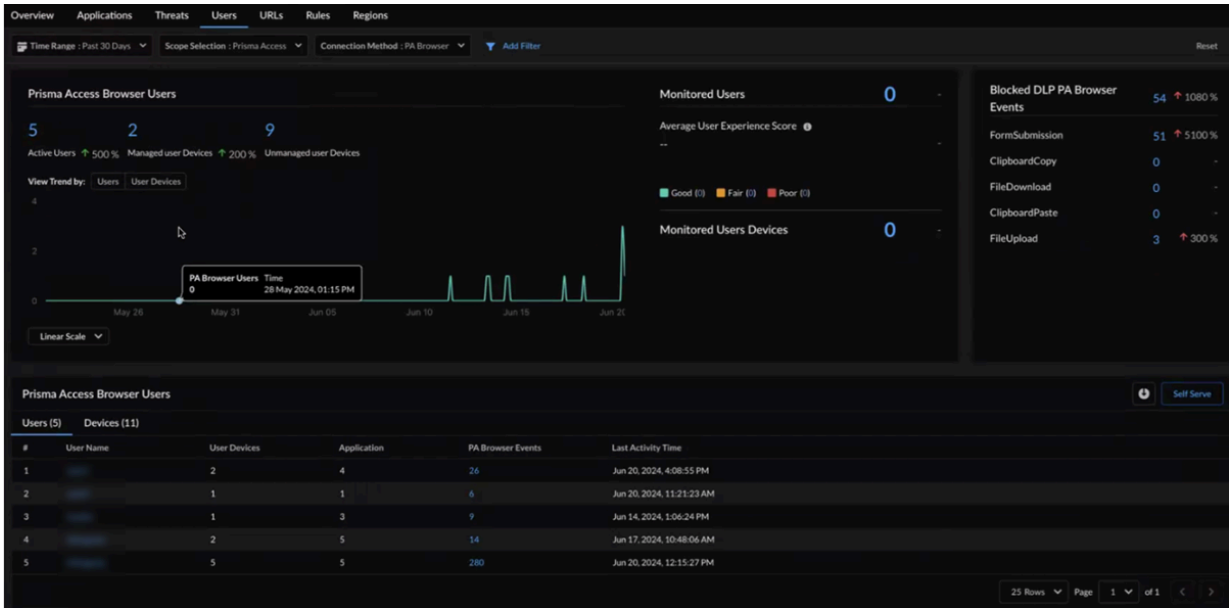
- Prisma Access Browser – Wählen Sie die **Prisma Access Browser-Verbindungsmethode** aus, um Informationen zu Ihren Prisma Access Browser-Benutzern anzuzeigen.

  Das Aktivitätstrenddiagramm der **Prisma Access Browser-Benutzer** zeigt die Anzahl der Benutzer, die irgendwann im ausgewählten Zeitbereichsfilter aktiv waren. Das Diagramm zeigt die Aufschlüsselung der Geräte dieser aktiven Benutzer, auf denen ein Prisma Access-Konnektivitätsagent installiert ist (verwaltete Geräte) bzw. auf denen kein Agent installiert ist (nicht verwaltete Benutzer).

  Der Prisma Access Browser bietet unübertroffene Einblicke in die Aktionen eines Browserbenutzers und zeigt an, ob die Aktionen des Benutzers auf seinem Gerät in Bezug auf die Datenbestände des Unternehmens durch die DLP-Richtlinie des Unternehmens zugelassen oder blockiert werden. Das Widget **Blockierte PA Browser-DLP-Ereignisse** zeigt Ereignisse an,

die auf im Browser ausgeführte Benutzeraktionen hinweisen, die durch die Richtlinie blockiert werden.

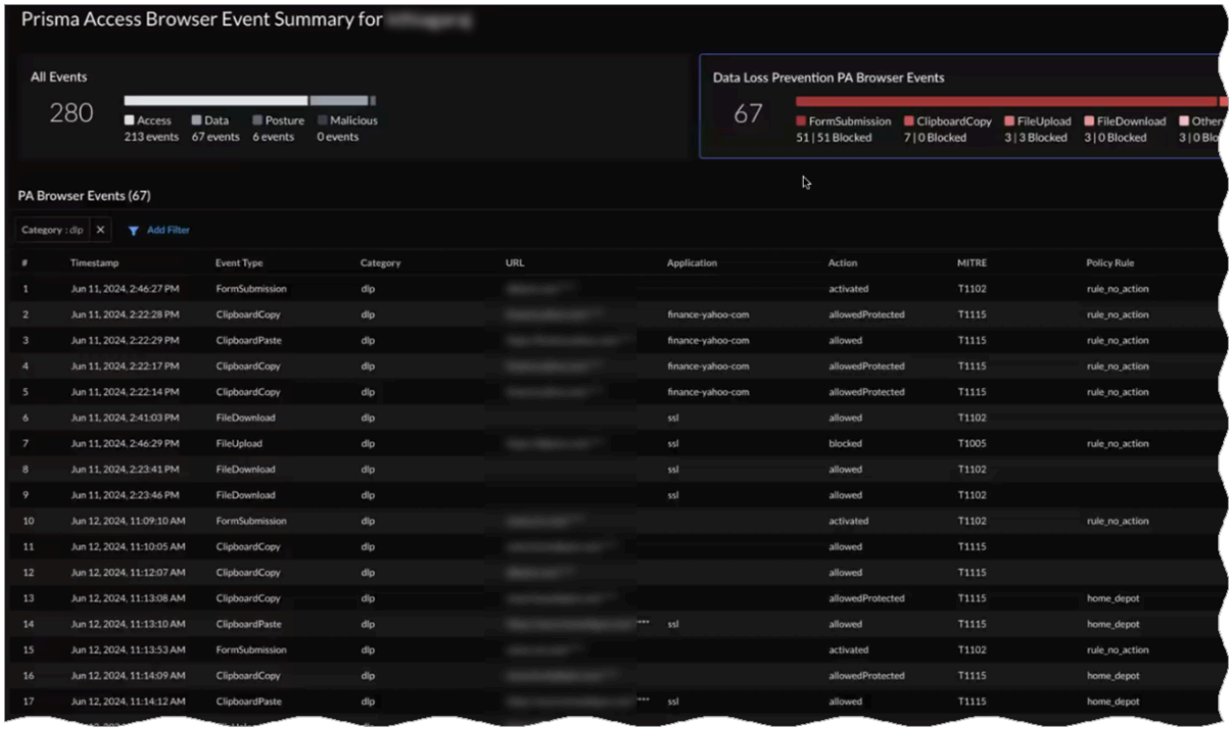



Die Tabelle **Prisma Access Browser-Benutzer** zeigt die Liste der aktiven Benutzer, die über den Prisma Access Browser auf Anwendungen zugreifen. Klicken Sie auf einen beliebigen **Benutzernamen**, um die **Aktivität** dieses Benutzers auf der Seite **Benutzerdetails** > **Aktivität** anzuzeigen.

Auf der Seite **Prisma Access Browser-Ereignisübersicht** werden alle Browseraktionen aufgelistet, die der Benutzer im ausgewählten Zeitintervall über den Browser ausgeführt hat. Die Standardansicht der Tabelle **PA Browser-Ereignisse** zeigt die Liste aller DLP-**Browserereignisse**, unabhängig davon, ob sie durch die Richtlinie zugelassen oder blockiert werden. Sie können die Ansichten auf andere Ereigniskategorien umstellen, beispielsweise **Zugriffsereignisse**, **Statusereignisse** oder **Böswillige Ereignisse**, indem Sie die entsprechende Ereigniskategorie auswählen. In jeder **Ereigniskategorie** können Sie die Aufschlüsselung der Ereignistypen anzeigen, zusammen mit dem Zeitstempel, der angibt, wann

das Browserereignis ausgeführt wurde, mit Informationen zur aufgerufenen Anwendungs-URL, mit den Anwendungsnamen sowie mit allen relevanten zugehörigen MITRE-Angriffshinweisen.



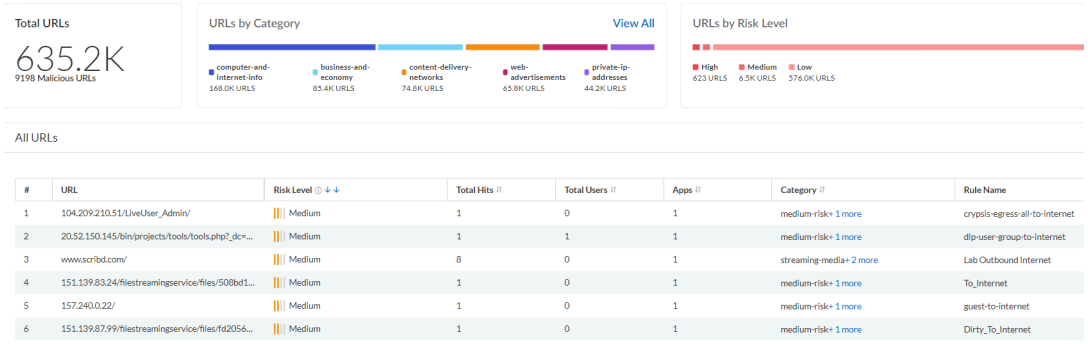

**Berichte** – Sie können keinen Bericht erstellen, der die Daten in dieser Ansicht abdeckt. Mit dem Bericht „Benutzeraktivität“ können Sie jedoch die spezifische Aktivität eines Benutzers in Ihrem Netzwerk anzeigen. Um einen Bericht zu planen, klicken Sie im Menü **Strata Cloud Manager** > **Berichte** auf das Symbol und wählen Sie aus der Dropdown-Liste **Typ** die Option „Benutzer“ aus.

# Activity Insights: URLs

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)*<br>• NGFWs<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)* | Um Activity Insights nutzen zu können, müssen Sie über mindestens eine der folgenden Lizenzen verfügen:<br>❑ Prisma Access<br>❑ AIOps for NGFW Free (use the AIOps for NGFW Free app) oder AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>❑ Strata Cloud Manager Essentials<br>❑ Strata Cloud Manager Pro<br>Zum Anzeigen der Registerkarte „Activity Insights: Auf der Registerkarte „URLs“ finden Sie:<br>❑ Strata Logging Service<br>❑ Advanced URL Filtering Lizenz |

Diese Ansicht fasst die URL-Aktivität in Ihren Prisma Access- und NGFW-Bereitstellungen zusammen, die der Dienst Erweiterte URL-Filterung erkannt hat. Sie erhalten Einblick in die Gesamtzahl der URLs, die im angegebenen Zeitraum in Ihrem Netzwerk erkannt wurden, und erhalten eine Aufschlüsselung dieser URLs nach URL-Kategorie und Risikostufe. Verwenden Sie die Filteroptionen, um die Ansicht im Dashboard zu filtern.




Nutzen Sie die hier angegebenen Daten, um …

- die am häufigsten aufgerufenen URL-Kategorien, die eindeutigen URLs in der URL-Kategorie, den URL-Verlauf in Ihrem Netzwerk sowie die Ergebnisse der globalen Analyse einzusehen. Basierend auf den vom URL-Filterdienst gefilterten bösartigen URLs setzen diese URL-Kategorien Ihr Netzwerk wahrscheinlich schädlichen Inhalten aus. Es empfiehlt sich, diese URL-Kategorien zu blockieren.

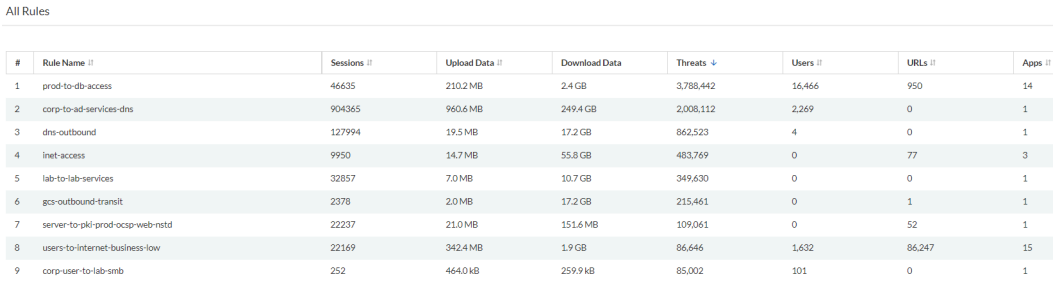
- URLs mit hohem Risiko und ihre Auswirkungen auf Benutzer, Anwendungen und Regeln zu überprüfen. URLs mit hohem Risiko werden nicht als bösartig bestätigt. Sie können Ihr Netzwerk jedoch weiterhin Bedrohungen aussetzen (eine Website, die nicht bösartig ist, aber von einem kugelsicheren ISP gehostet wird, ist ein Beispiel für eine Website mit hohem Risiko). Erwägen Sie, diese Websites mit strengen Entschlüsselungs- und Sicherheitsrichtlinienregeln ins Visier zu nehmen.

**Berichte** – Sie können keinen Bericht erstellen, der die Daten in dieser Ansicht abdeckt.

# Activity Insights: Regeln

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)*<br>• NGFWs<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)* | Um Activity Insights nutzen zu können, müssen Sie über mindestens eine der folgenden Lizenzen verfügen:<br>☐ Prisma Access<br>☐ AIOps for NGFW Free (use the AIOps for NGFW Free app) oder AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>☐ Strata Cloud Manager Essentials<br>☐ Strata Cloud Manager Pro<br>Zum Anzeigen der Registerkarte „Activity Insights: Regeln“ sind zusätzlich folgende Lizenzen erforderlich:<br>☐ Strata Logging Service |

Sehen Sie sich die Sicherheitsrichtlinienregeln an, die auf den gesamten Datenverkehr in Ihrem Netzwerk angewendet werden. Sicherheitsrichtlinienregeln bestimmen, ob eine Sitzung auf Grundlage von Datenverkehrsattributen wie Quell- und Ziel-IP-Adresse, Anwendung, Benutzer und Dienst blockiert oder zugelassen wird. Der gesamte Datenverkehr, der Ihr Netzwerk passiert, wird mit einer Sitzung abgeglichen und jede Sitzung wird mit einer Sicherheitsrichtlinienregel abgeglichen. Wenn eine Sitzung übereinstimmt, wird die Sicherheitsrichtlinienregel angewendet.


All Rules

| # | Rule Name | Sessions | Upload Data | Download Data | Threats | Users | URLs | Apps |
|---|---|---|---|---|---|---|---|---|
| 1 | prod-to-db-access | 46635 | 210.2 MB | 2.4 GB | 3,788,442 | 16,466 | 950 | 14 |
| 2 | corp-to-ad-services-dns | 904365 | 960.6 MB | 249.4 GB | 2,008,112 | 2,269 | 0 | 1 |
| 3 | dns-outbound | 127994 | 19.5 MB | 17.2 GB | 862,523 | 4 | 0 | 1 |
| 4 | inet-access | 9950 | 14.7 MB | 55.8 GB | 483,769 | 0 | 77 | 3 |
| 5 | lab-to-lab-services | 32857 | 7.0 MB | 10.7 GB | 349,630 | 0 | 0 | 1 |
| 6 | gcs-outbound-transit | 2378 | 2.0 MB | 17.2 GB | 215,461 | 0 | 1 | 1 |
| 7 | server-to-pki-prod-ocsp-web-nstd | 22237 | 21.0 MB | 151.6 MB | 109,061 | 0 | 52 | 1 |
| 8 | users-to-internet-business-low | 22169 | 342.4 MB | 1.9 GB | 86,646 | 1,632 | 86,247 | 15 |
| 9 | corp-user-to-lab-smb | 252 | 464.0 kB | 259.9 kB | 85,002 | 101 | 0 | 1 |

Das Dashboard zeigt die folgenden Details des Netzwerkereignisses, das der Sicherheitsrichtlinienregel entspricht:

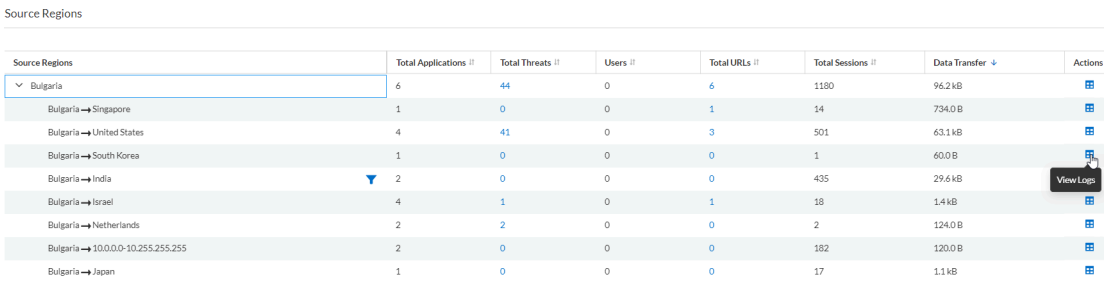
Datenverkehrssitzungen, übertragene Daten, in den Sitzungen erkannte Bedrohungen, betroffene Benutzer, aufgerufene URLs und aufgerufene Anwendungen. Prüfen Sie die Regeln, die am häufigsten auf die Datenverkehrssitzungen angewendet werden; analysieren Sie diese Sitzungen, um herauszufinden, ob die Regel unverhältnismäßig tolerant ist, und optimieren Sie die Regel bei Bedarf.

**Berichte** – Sie können keinen Bericht erstellen, der die Daten in dieser Ansicht abdeckt.

# Activity Insights: Regionen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)*<br>• NGFWs<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)* | Um Activity Insights nutzen zu können, müssen Sie über mindestens eine der folgenden Lizenzen verfügen:<br>☐ Prisma Access<br>☐ AIOps for NGFW Free (use the AIOps for NGFW Free app) oder AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>☐ Strata Cloud Manager Essentials<br>☐ Strata Cloud Manager Pro<br>Zum Anzeigen der Registerkarte „Activity Insights: Regionen“ sind zusätzlich folgende Lizenzen erforderlich:<br>☐ Strata Logging Service |

Dies sind die Regionen, aus denen der Datenverkehr in Ihrem Netzwerk stammt. Die Ansicht bietet Informationen zu Bedrohungen, Benutzern, URLs, Netzwerksitzungen und Datenübertragungen, die von diesen Standorten ausgehen. Sie können auch ins Detail gehen, um den Zielort des Datenverkehrs zu ermitteln. Klicken Sie auf „Aktionen“, um die Verkehrsprotokolle für die Sitzung anzuzeigen. Mithilfe der Daten können Sie Regionen identifizieren und eingrenzen, die Ziele für Bedrohungen darstellen, die versuchen, in Ihr Netzwerk einzudringen. Optimieren Sie die Regel, die auf die Zielregionen angewendet wird.




Es gibt Filteroptionen, um den Verkehr von und zu bestimmten Quell- und Zielregionen einzugrenzen. Zu den weiteren Filteroptionen gehören:

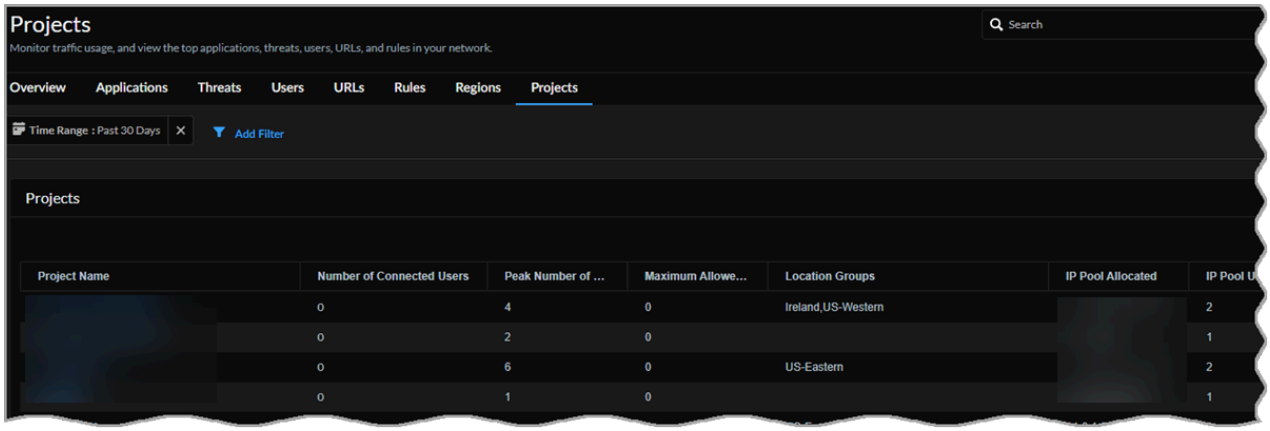
- Datenverkehr in einer bestimmten Bereitstellung: Prisma Access, NGFW
- Datenverkehr zu und von sanktionierten oder nicht sanktionierten Anwendungen
- Datenverkehr über bestimmte Ports und Protokolle
- Datenverkehr mit bestimmten Bedrohungsarten, Bedrohungskategorien, URLs und URL-Kategorien

**Berichte** – Sie können keinen Bericht erstellen, der die Daten in dieser Ansicht abdeckt. Sie können jedoch den Bericht „Netzwerknutzung“ nutzen, um Details zu Ihrem Netzwerkverkehr zu erfahren. Um einen Bericht zu planen, klicken Sie im Menü **Strata Cloud Manager** > **Berichte** auf das Symbol und wählen Sie aus der Dropdown-Liste **Typ** die Option „Netzwerknutzung“ aus.

# Activity Insights: Projekte

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)*<br>• NGFWs<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)* | Sie müssen mindestens eine der folgenden Lizenzen besitzen, um Activity Insights nutzen zu können:<br>☐ Prisma Access<br>☐ AIOps for NGFW Free (use the AIOps for NGFW Free app) oder AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>☐ Strata Cloud Manager Essentials<br>☐ Strata Cloud Manager Pro<br>. |

Verschaffen Sie sich einen Einblick in Ihre Prisma Access Agent-Bereitstellung, indem Sie Strata Cloud Manager verwenden, um Ihre Projektaktivitäten hinsichtlich des Zugriffs mit dynamischen Rechten zu überwachen.




- Die Tabelle **Projekte** bietet einen Überblick über die Projekte, auf die Ihre Benutzer mit Prisma Access zugreifen. Wählen Sie einen Projektnamen aus, um die Detailseite anzuzeigen.
- Die Detailseite des Projekts zeigt Folgendes:
  - **Übersicht** – Hier sehen Sie die maximal zulässigen Benutzer und die Spitzenanzahl der Benutzer während des ausgewählten Zeitbereichs für dieses Projekt.
  - **IP-Poolauslastung** – Zeigen Sie die Anzahl der verwendeten IPs und die Anzahl der IPs an, die für die Pools in diesem Projekt noch verfügbar sind.
  - **Verbundener Benutzer** – Zeigen Sie eine Grafik der im ausgewählten Zeitbereich verbundenen Benutzer an.
  - **Verbundene Benutzer nach Standortgruppe** – Hier sehen Sie die Anzahl der Benutzer nach der Prisma Access-Standortgruppe, in der sie sich befinden.

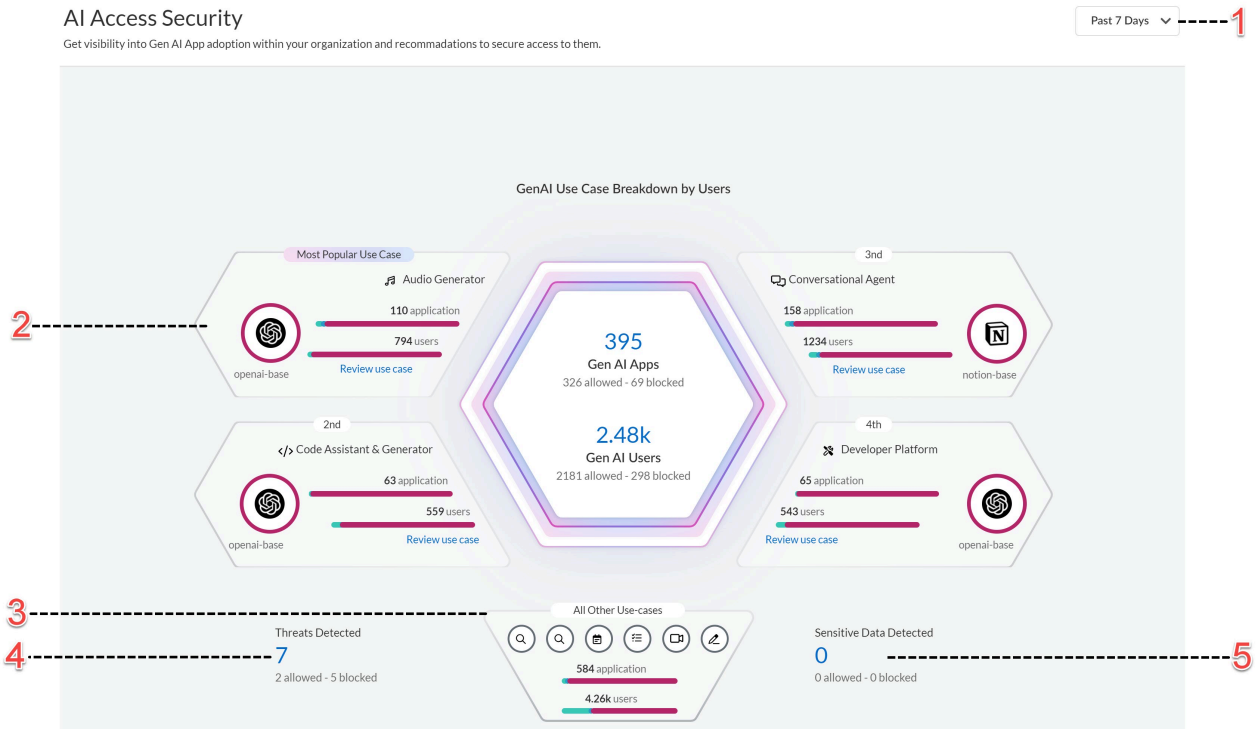
# Insights: KI-Zugriff

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)*<br>• NGFWs<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)* | Eine der folgenden Lizenzen:<br>❑ AI Access Security-Lizenz<br>❑ CASB-PA-Lizenz<br>❑ CASB-X-Lizenz<br>Weitere Informationen zu Lizenzen, die KI-Zugriffssicherheit unterstützen, finden Sie hier. |

GenAI-Anwendungen (Generative künstliche Intelligenz) sind KI-Anwendungen, die in der Lage sind, als Reaktion auf Benutzeraufforderungen (sogenannte „Prompts“) Texte, Bilder, Videos und andere Datenformen zu generieren und auf Grundlage der Benutzerdateneingaben kontinuierlich zu lernen. Ihre Nutzung nimmt in erstaunlichem Tempo zu und bietet Unternehmen grenzenlose Möglichkeiten. Allerdings stellt die Art und Weise, wie sich GenAI-Anwendungen fortlaufend verbessern, eine neue Gefahr für Unternehmen und Sicherheitsadministratoren dar: Wie können Sie sicherstellen, dass Ihre Mitarbeiter GenAI-Apps keine vertraulichen oder geschützten Daten preisgeben?

Deshalb stellt Palo Alto Networks KI-Zugriffssicherheit vor, um die sichere Einführung von GenAI-Anwendungen in Ihrem Unternehmen zu ermöglichen.

Verwenden Sie das Dashboard Einblicke in die KI-Zugriffssicherheit, um die GenAI-Anwendungsnutzung in Ihrem Netzwerk zu filtern. Das Dashboard „Einblicke in die KI-Zugriffssicherheit“ bietet ausführliche Details, die Ihnen helfen zu verstehen, welche GenAI-Apps von wem verwendet werden.




*Klicken Sie hier, um mehr darüber zu erfahren, wie Sie Ihre vertraulichen Daten vor GenAI-Anwendungen schützen können.*

# Insights: KI-Laufzeitsicherheit

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)*<br>• NGFWs<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)* | ❑ Aktivieren Ihrer KI-Laufzeitsicherheit-Lizenz<br>❑ Voraussetzungen für die Einrichtung der KI-Laufzeitsicherheit<br>❑ Onboarding und Aktivierung eines Cloud-Kontos in SCM |

Die KI-Laufzeitsicherheit von Palo Alto Networks ist eine speziell entwickelte zentralisierte Sicherheitslösung zum Schutz der Cloud-Netzwerkarchitektur Ihres Unternehmens vor KI-spezifischen und herkömmlichen Netzwerkangriffen, und zwar durch den Einsatz KI-gestützter Echtzeitsicherheit. Sie schützt Ihre KI-Modelle, KI-Anwendungen und KI-Datensätze der nächsten Generation vor Netzwerkbedrohungen wie Prompt Injections, vor dem Verlust vertraulicher Daten, vor unsicheren Ausgaben (z. B. Malware und URLs) und vor DoS-Angriffen auf Modelle.

Verwenden Sie das Dashboard Einblicke in die KI-Laufzeitsicherheit, um die Angriffsfläche Ihres Cloud-Netzwerks zu verstehen und Ihre Cloud-Assets vor Bedrohungen zu schützen.

*Klicken Sie hier, um mehr darüber zu erfahren, wie Sie Ihren KI- und anderen Netzwerkverkehrsfluss vor potenziellen Angriffen schützen können.*

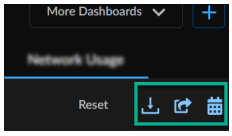
# Dashboards: Strata Cloud Manager

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden<br>• Prisma SD-WAN | Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>☐ Prisma Access<br>☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>☐ Strata Cloud Manager Essentials<br>☐ Strata Cloud Manager Pro<br>☐ Prisma SD-WAN<br>Weitere Lizenzen und Voraussetzungen für den Zugriff auf bestimmte Dashboards:<br>☐ Cloud-Delivered Security Services (CDSS)<br>☐ ADEM-Beobachtbarkeit<br>☐ eine Rolle mit der Berechtigung, das Dashboard anzuzeigen<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Strata Cloud Manager bietet eine Reihe interaktiver Dashboards, die Ihnen einen umfassenden Überblick über die in Ihrem Netzwerk genutzten Anwendungen, ION-Geräte, Bedrohungen, Benutzer und Sicherheitsabonnements geben. Die Dashboards bieten Einblick in den Zustand, den Sicherheitsstatus und die Aktivitäten Ihrer Bereitstellung und helfen Ihnen, Leistungs- und Sicherheitsprobleme in Ihrem Netzwerk zu verhindern oder zu beheben. Die Dashboard-Unterstützung erstreckt sich auf alle Produkte und Abonnements von Palo Alto Networks, die für die Cloud-Verwaltung unterstützt werden, sowie auf andere Quellen, darunter Traps, Cortex XDR, Prisma SaaS und Proofpoint. Die angezeigten Daten hängen häufig von Ihrem Abonnement ab. Sie können jedes Dashboard-Thema überprüfen, um zu sehen, welche Lizenzanforderungen für dieses Dashboard gelten, ob Rollenberechtigungen Auswirkungen darauf haben könnten oder welche Daten sichtbar sind, und um mehr über die verschiedenen Datentypen zu erfahren, die durch jedes Abonnement freigeschaltet werden.

Sie können über das Menü **Dashboards** im linken Navigationsbereich auf Dashboards zugreifen. Das SASE Health-Dashboard ist standardmäßig an die Landingpage angeheftet. Klicken Sie auf **Mehr Dashboards** und aktivieren oder deaktivieren Sie das Kontrollkästchen neben einem jeweiligen Dashboard-Namen, um das Dashboard an die Dashboard-Landingpage anzuheften oder die Anheftung aufzuheben. Sie können mit der Option **Mein Dashboard erstellen** auch Ihr eigenes Dashboard erstellen. Einige der Dashboards bieten auch die Möglichkeit, Berichte herunterzuladen, die Sie offline teilen können, oder Berichte für regelmäßige Updates zu planen.

Um festzustellen, ob Berichte für ein Dashboard unterstützt werden, achten Sie auf diese Symbole:



# Integration der Cloud Identity Engine

Wir empfehlen die Einrichtung der Cloud Identity Engine (Verzeichnissynchronisierung), um Dashboards optimal zu nutzen. Cloud Identity Engine ist eine kostenlose App von Palo Alto Networks, die anderen Apps schreibgeschützten Zugriff auf Ihre Active Directory-Informationen gewährt und Ihnen Folgendes ermöglicht:

- **Daten zur Benutzeraktivität abrufen** – Mit der Cloud Identity Engine können Sie den Benutzer angeben, für den Sie einen Bericht ausführen möchten.
- **Sie können mit der eingerichteten Cloud Identity Engine Berichte freigeben, um sie einfach und sicher mit anderen Mitgliedern Ihrer Organisation zu teilen**. Sie können Empfänger auch ganz einfach einem geplanten Bericht hinzufügen. Ihre Berichtsempfänger werden mit der Cloud Identity Engine abgeglichen. Wenn keine Übereinstimmung gefunden wird, wird ein zusätzlicher Validierungsschritt ausgeführt, indem ihre E-Mail-Domäne mit den E-Mail-Domänen abgeglichen wird, die Ihrem Supportkonto zugeordnet sind. Diese Prüfungen stellen sicher, dass keine Berichte außerhalb Ihrer Organisation gesendet werden.

Integrierte Anwendungen müssen in derselben Region bereitgestellt werden. Sie können jederzeit zum Hub gehen, um die Cloud Identity Engine in Prisma Access oder die Verzeichnissynchronisierung zu integrieren. # Palo Alto Networks-Anwendungen integrieren

# Unterstützung für Dashboards

*Bei einigen der Dashboard-Unterstützungen im Produkt steht die Migration auf Strata Cloud Manager noch aus.*

| Merkmal | Unterstützt in | | | | Lizenzen und andere Anforderungen | Umfang der aggregierten Daten |
|---|---|---|---|---|---|---|
| | Prisma Access (Cloud-verwaltet) | Prisma Access (Panorama-verwaltet)* | AIOps for NGFW | Prisma SASE Mehrmandanten-Plattform | | |
| | • Dokumente für Prisma Access (Managed by Strata Cloud Manager) und Prisma Access (Managed by Panorama) | | • Dokumente für AIOps for NGFW | • Dokumente für Prisma SASE-Mehrmandanten-Plattform | | |
| SASE-Zustand | Ja | Ja | Ja | | • ADEM-Beobachtbarkeit<br>• KI-gestütztes ADEM | |
| Best Practices | Ja | Nein | PAN-OS-Versionen: 10.0 oder höher | Ja | [Nur für AIOps for NGFW] Aktivierung der Telemetriefreigabe auf Geräten | • Prisma Access (Manage pro Mandant<br>• AIOps for NGFW: pro mit AIOps for NGFW-Instanz verbundener NGFW / verbundenem Panorama |
| Zusammenfassung der Konformität | Nein | Nein | Ja | Nein | [Nur für AIOps für NGFW] Aktivierung der Telemetriefreigabe auf Geräten | AIOps für NGFW: pro mit „AIOps für NGFW“-Instanz verbundener NGFW / verbundenem Panorama |

| Merkmal | Unterstützt in | | | | Lizenzen und andere Anforderungen | Umfang der aggregierten Daten |
|---|---|---|---|---|---|---|
| | Prisma Access (Cloud-verwaltet) | Prisma Access (Panorama-verwaltet)* | AIOps for NGFW | Prisma SASE Mehrmandanten-Plattform | | |
| On-Demand-BPA | Nein | Nein | Ja | Nein | TSF | AIOps für NGFW: pro mit „AIOps für NGFW“-Instanz verbundener NGFW / verbundenem Panorama |
| Zusammenfassung | Ja | Ja | Ja | Ja | • Strata Logging Service-Lizenz<br>• Bedrohungsabwehr-Lizenz<br>• URL-Filter-Lizenz<br>• WildFire-Lizenz<br>• Enterprise DLP-Lizenz | Pro Strata Logging Service-Mandant |
| WildFire | Ja | Nein | Ja | Ja** | WildFire-Lizenz | Pro Mandanten-Dienstgruppe (TSG) |
| DNS Security | Ja | Ja | Ja | Ja** | DNS Security-Lizenz | Pro Mandanten-Dienstgruppe (TSG) |
| Protokoll-Viewer | Ja | Ja | Ja | Ja | Strata Logging Service-Lizenz | Pro Strata Logging Service-Mandant |
| IOC-Suche | Ja | Nein | Ja | Ja** | Voraussetzungen zum Anzeigen | |

| Merkmal | Unterstützt in | | | | Lizenzen und andere Anforderungen | Umfang der aggregierten Daten |
|---|---|---|---|---|---|---|
| | Prisma Access (Cloud-verwaltet) | Prisma Access (Panorama-verwaltet)* | AIOps for NGFW | Prisma SASE Mehrmandanten-Plattform | | |
| | | | | | des Trenddiagramms in der Suche:<br>• DNS-Lizenz<br>• WildFire-Lizenz<br>• Strata Logging Service-Lizenz<br>• URL-Filterung | |
| Herunterladen/ Freigeben/ Planen | Ja | Ja | Ja | Ja | | Siehe jeweilige Merkmalsspalte in dieser Tabelle. |
| SaaS-Sicherheit | Ja | Nein | Nein | Nein | • SaaS-Sicherheitslizenz<br>• Strata Logging Service | Pro Prisma Access-Mandant |
| DLP-Vorfälle | Ja | Nein | Nein | Nein | Enterprise DLP-Lizenz | Pro Prisma Access-Mandant |
| Gerätezustand | Nein | Nein | Ja | Nein | • [Nur für AIOps for NGFW] Aktivierung der Telemetriefreigabe auf Geräten | AIOps for NGFW: pro mit AIOps for NGFW-Instanz verbundener NGFW / verbundenem Panorama |

| Merkmal | Unterstützt in | | | | Lizenzen und andere Anforderungen | Umfang der aggregierten Daten |
|---|---|---|---|---|---|---|
| | Prisma Access (Cloud-verwaltet) | Prisma Access (Panorama-verwaltet)* | AIOps for NGFW | Prisma SASE Mehrmandanten-Plattform | | |
| Einblicke in den Sicherheitsstatus | Nein | Nein | Ja | Nein | | AIOps for NGFW: pro mit AIOps for NGFW-Instanz verbundener NGFW / verbundenem Panorama |
| Fortschrittliche Bedrohungsabwehr | Nein | Nein | Ja | Nein | • Lizenz für Bedrohungsabwehr oder fortschrittliche Bedrohungsabwehr<br>• Strata Logging Service | Pro Strata Logging Service-Mandant |
| IoT Security | Ja | Ja | Ja | Nein | IoT Security-Lizenz | Pro IoT Security-Mandant |
| Prisma SD-WAN | Nein | Nein | Nein | Ja | Prisma SD-WAN-Lizenz | Pro Prisma SD-WAN-Mandant |
| PAN-OS-CVEs | Nein | Ja | Ja | | [Nur für AIOps für NGFW] Aktivierung der Telemetriefreigabe auf Geräten | • AIOps für NGFW: pro mit „AIOps für NGFW“-Instanz verbundener NGFW / verbundenem Panorama<br>• PSIRT-CVE-Datenbank mit API-Zugriff |

| Merkmal | Unterstützt in | | | | Lizenzen und andere Anforderungen | Umfang der aggregierten Daten |
|---|---|---|---|---|---|---|
| | Prisma Access (Cloud-verwaltet) | Prisma Access (Panorama-verwaltet)* | AIOps for NGFW | Prisma SASE Mehrmandanten-Plattform | | |
| Einführung von CDSS | Ja | Ja | Ja | | [Nur für AIOps für NGFW] Aktivierung der Telemetriefreigabe auf Geräten | AIOps für NGFW: pro mit „AIOps für NGFW“-Instanz verbundener NGFW / verbundenem Panorama |
| Funktionsannahme | Nein | Ja | Ja | | [Nur für AIOps für NGFW] Aktivierung der Telemetriefreigabe auf Geräten | AIOps für NGFW: pro mit „AIOps für NGFW“-Instanz verbundener NGFW / verbundenem Panorama |

**Prisma Access (Panorama-verwaltet)*** –

- Für Benutzer von Prisma Access (Panorama-verwaltet), bei denen Strata Logging Service in einer Region außerhalb Amerikas gehostet wird, müssen Sie die Zustimmung erteilen, damit Prisma Access Daten vom Strata Logging Service in der Region außerhalb Amerikas lesen und verarbeiten darf. Lesen und akzeptieren Sie den Datenschutzhinweis auf der Dashboard-Startseite, um Ihr Einverständnis zu erteilen und weitere Dashboards und Protokolle anzuzeigen. Nur App-, Instanz- und Kontoadministratoren können die Datenschutzerklärung sehen und akzeptieren.
- Dashboards werden in der Mehrmandanten-Umgebung von Prisma Access (Panorama-verwaltet) nicht unterstützt.

**Ja*** – Ja bedeutet, dass alle Versionen von Prisma Access und PAN-OS unterstützt werden.

**Ja**** – Auf der Mehrmandanten-Plattform werden Mandanten als Mandanten-Dienstgruppen (TSGs) identifiziert und ihnen wird eine TSG-ID zugewiesen. Pro Kunden-Support-Portal (CSP) können ein oder mehrere Mandanten zugeordnet werden. Die im Dashboard angezeigten Daten hängen von den folgenden Szenarien ab:

- Ihre App, über die Sie auf das Dashboard zugreifen, muss TSG-unterstützt sein und der Zugriff muss über die SASE-Plattform oder die Mandantenansicht im Hub erfolgen.
- Sie haben Ihrem Mandanten mithilfe von allgemeinen Diensten im Hub Geräte zugeordnet.

- Überprüfen Sie, ob Ihre Mandanten über eine 1:1- oder eine n:1-Zuordnung mit dem CSP verfügen.
  - Wenn Ihre Mandanten über eine 1:1-Zuordnung mit dem CSP verfügen, können Sie Dashboard-Daten aus allen Quellen anzeigen (im WildFire-Dashboard werden beispielsweise Daten aus Palo Alto Networks-Firewalls, Prisma Access, Traps, Cortex XDR, Prisma SaaS, Proofpoint und manuellen Uploads angezeigt).
  - Wenn pro CSP mehrere Mandanten zugeordnet sind, zeigt das Dashboard nur Daten von Prisma Access, Palo Alto Networks-Firewalls und Panorama-Geräten an, die bestimmten Mandanten zugeordnet sind, und nicht Daten aus anderen Quellen.

**AIOps for NGFW*** – Welche Dashboards in AIOps for NGFW verfügbar sind, hängt davon ab, ob Sie die Lizenzstufe „Free“ oder „Premium“ nutzen.

# Dashboard: Erstellen eines benutzerdefinierten Dashboards

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden<br>• Prisma SD-WAN | Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>❑ Prisma Access<br>❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>❑ Strata Cloud Manager Essentials<br>❑ Strata Cloud Manager Pro<br>❑ Prisma SD-WAN<br>Weitere für Sichtbarkeit erforderliche Lizenzen und Voraussetzungen:<br>❑ Lizenzen zum Freischalten bestimmter Widgets im Dashboard<br>❑ eine Rolle mit der Berechtigung zum Anzeigen des Dashboards<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Abgesehen von den Standard-Dashboards können Sie benutzerdefinierte Dashboards erstellen, um mithilfe von Widgets Einblick in die Bereiche Ihres Netzwerks zu erhalten, die für Sie von Interesse sind. Widgets sind Komponenten, die zum Erstellen eines Dashboards verwendet werden. Widgets werden kategorisiert und in der Widget-Bibliothek gespeichert. Klicken Sie auf **Dashboards** > **+** und wählen Sie eine Kategorie aus der Dropdown-Liste aus, um die Widgets anzuzeigen. Die in der Widget-Bibliothek verfügbaren Widgets hängen von Ihren Abonnements für Sicherheitsdienste ab. Wenn Sie beispielsweise AIOps for NGFW Premium- und Advanced WildFire-Lizenzen haben, können Sie alle Widgets in der WildFire-Kategorie anzeigen und verwenden, um ein Dashboard zu erstellen.

Dies sind die Widget-Kategorien, die zum Erstellen eines Dashboards verfügbar sind. Über die nachstehenden Links erfahren Sie mehr über die Lizenzanforderungen für den Zugriff auf Widgets in diesen Kategorien.

- Dashboard: Fortschrittliche Bedrohungsabwehr
- Dashboard: DNS Security
- Dashboard: WildFire

# Erstellen eines Dashboards

Sie können bis zu 10 Widgets in einem benutzerdefinierten Dashboard hinzufügen und 10 benutzerdefinierte Dashboards pro Benutzer erstellen. Das Dashboard und die Widgets können jederzeit angepasst werden. Sie können die Widget-Kachel und -Beschreibung anpassen, Filter ein- oder ausblenden, Dashboard-Einstellungen wie Layout, Dashboard-Name und Beschreibungen festlegen und auch Filter in das Dashboard einbinden.

**STEP 1 |** Klicken Sie auf **Dashboards** > **+**.


**STEP 2 |** Geben Sie einen Namen für das Dashboard ein.

**STEP 3 |** Wählen Sie eine Widget-Kategorie aus der Dropdown-Liste „Widget-Bibliothek“ aus.

**STEP 4 |** Fügen Sie das Widget zum Dashboard hinzu – Bewegen Sie den Mauszeiger über das Widget, um mehr über das Widget zu erfahren. Ziehen Sie das Widget per Drag-and-Drop auf die Dashboard-Arbeitsfläche.

Sie können der Dashboard-Arbeitsfläche weitere Widgets desselben oder eines anderen Typs aus einer anderen Widget-Kategorie hinzufügen.

**STEP 5 |** Wechseln Sie zwischen der Ansicht **Beispieldaten** und **Echte Daten**, um zu sehen, wie Ihr Dashboard-Widget aussieht. Anhand von Beispieldaten können Sie sich besser vorstellen, wie Ihr Dashboard aussehen wird und welche Art von Informationen Sie sehen können. Verwenden Sie die Option **Echte Daten**, um die tatsächlichen Daten für Ihre Bereitstellung anzuzeigen.

**STEP 6 |** (Optional) Sie können das Dashboard in der Editor-Ansicht anpassen:

- Ordnen Sie die Widgets im Dashboard neu an – Wählen Sie dazu das Widget aus und ziehen Sie es per Drag-and-Drop an die gewünschte Stelle auf der Arbeitsfläche.
- Bearbeiten Sie ein Widget – Verwenden Sie das Bearbeitungssymbol in der oberen rechten Ecke jedes Widgets, um die jeweiligen Widget-Einstellungen zu bearbeiten. Die verfügbaren Einstellungen hängen vom Widget ab und sind nicht bei allen Widgets gleich. Sie können beispielsweise den Widget-Namen, die Widget -Beschreibung und die Widget-Optionen bearbeiten, um die Daten im Widget zu filtern und zu sortieren, etwa nach Urteil oder Aktion.

  *Sie können die Widget-Einstellungen in der Editor-Ansicht oder nach dem Speichern des Dashboards bearbeiten.*

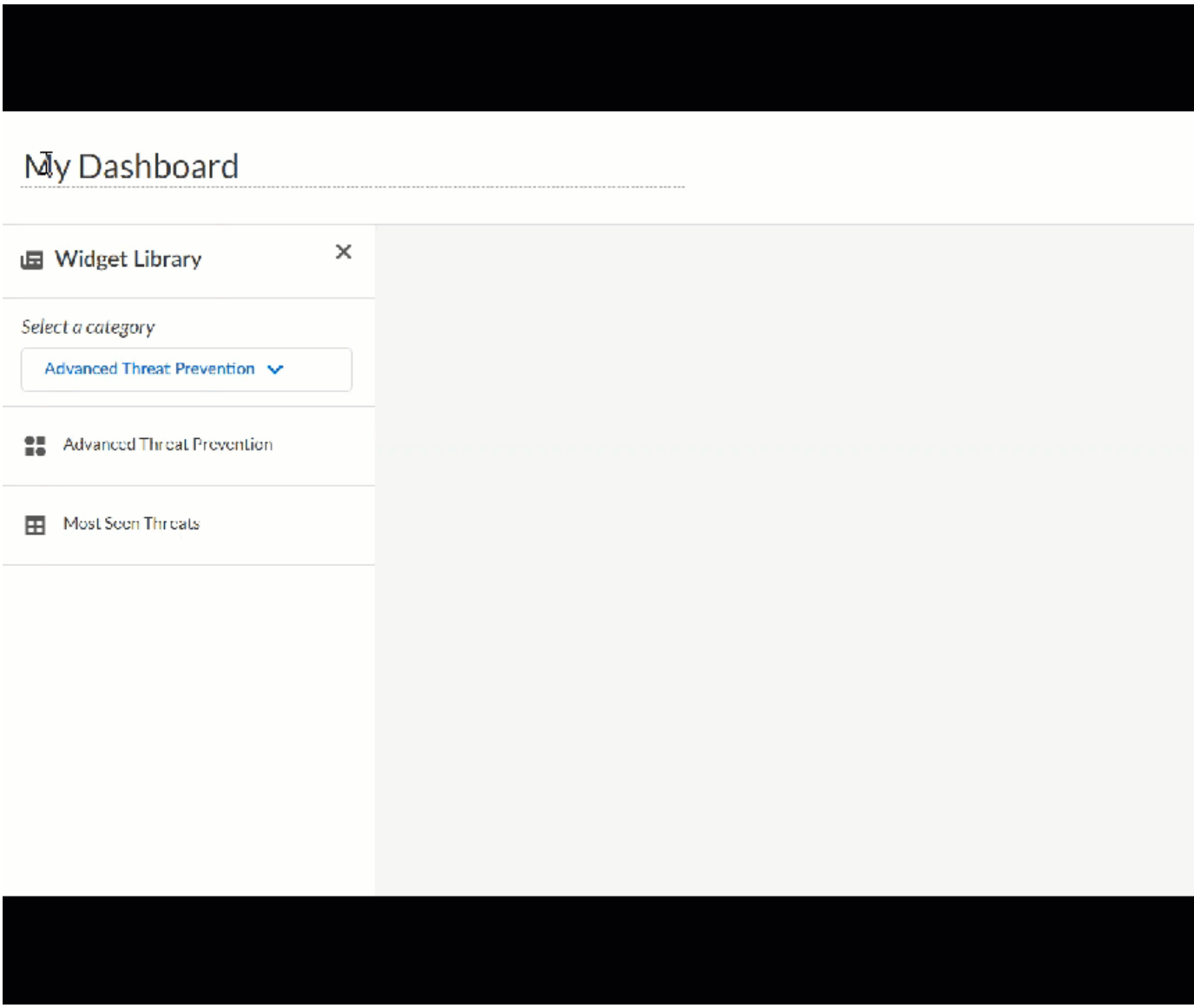
**STEP 7 |** Speichern Sie das Dashboard und klicken Sie oben auf der Seite auf **Gehen Sie zum Dashboard**, um das Dashboard zu öffnen.

**STEP 8 |** (Optional) Nachdem Sie das Dashboard gespeichert haben, haben Sie folgende Möglichkeiten:

- Ändern Sie den Zeitbereich, für den Sie die Dashboard-Daten anzeigen möchten.

  *Sie können die Zeit erst ändern, nachdem Sie das Dashboard gespeichert haben. In der Editor-Ansicht beträgt der Zeitbereich standardmäßig 24 Stunden.*

- Verwenden Sie das Symbol „Bearbeiten“ oder „Löschen“, um das benutzerdefinierte Dashboard zu ändern oder zu löschen.



# Dashboard: Gerätezustand

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | ❑ Strata Cloud Manager Essentials<br>❑ AIOps for NGFW Premium oder Strata Cloud Manager Pro<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

- Klicken Sie auf **Dashboards** > **Gerätezustand**, um zu beginnen.


## Was sehen Sie in diesem Dashboard?

*Das Dashboard zeigt die aggregierten Daten für alle Firewalls, die in Ihre Mandanten eingebunden sind, und sendet auch Telemetriedaten.*

Das Dashboard „Gerätezustand“ zeigt Ihnen den kumulativen Integritätsstatus und die Leistung Ihrer Bereitstellung basierend auf den Zustandsscores der integrierten NGFWs an. Der Gerätezustand wird durch den Schweregrad des Zustandsscores (0–100) und die entsprechende Zustandsnote (gut, angemessen, schlecht, kritisch) bestimmt. Der Zustandsscore wird anhand von Priorität, Anzahl, Art und Status der offenen Benachrichtigungen berechnet.

# Wie können Sie die Daten aus dem Dashboard nutzen?

Dieses Dashboard unterstützt Sie dabei, ...

- die Bereitstellungsverbesserungen, die Sie über einen bestimmten Zeitraum hinweg vorgenommen haben, anhand der Verlaufsdaten zum Zustandsscore zu verstehen.
- die Geräte in Ihrer Bereitstellung, die Aufmerksamkeit erfordern, einzugrenzen und Prioritäten für die Fehlerbehebung festzulegen.

*Die Berichtsfunktion (Bericht herunterladen, freigeben und planen) wird für dieses Dashboard nicht unterstützt.*

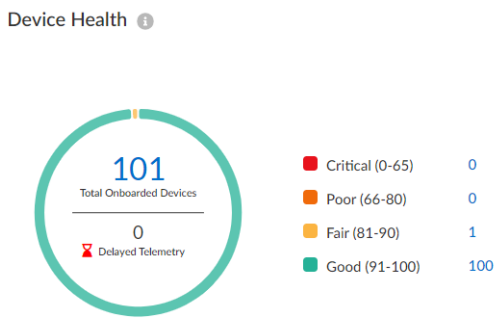
# Dashboard „Gerätezustand“: Gerätezustandsscores

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | ❑ Strata Cloud Manager Essentials<br>❑ AIOps for NGFW Premium oder Strata Cloud Manager Pro<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

- Klicken Sie auf **Dashboards** > **Gerätezustand**, um das Dashboard anzuzeigen.

Das Dashboard-Widget zeigt Folgendes:

- die Gesamtzahl der eingebundenen NGFWs
- die Anzahl der Geräte, die seit über 12 Stunden keine Telemetriedaten gesendet haben
- den Schweregrad des Zustandsscores für die integrierten Geräte in Ihrer Bereitstellung Klicken Sie auf die verlinkte Zahl, um Gerätedetails, Statistiken zum Gerätezustand sowie Benachrichtigungen zum Gerät anzuzeigen, die Ihre Aufmerksamkeit erfordern.

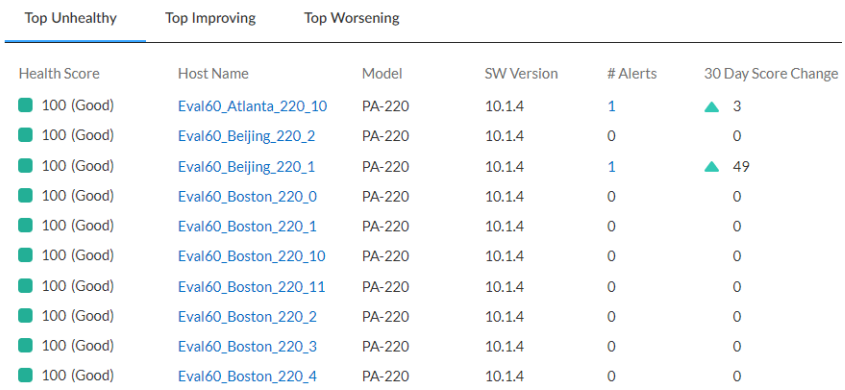


# Dashboard „Gerätezustand“: Gerätestatistik

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | ❑ Strata Cloud Manager Essentials<br>❑ AIOps for NGFW Premium oder Strata Cloud Manager Pro<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

- Klicken Sie auf **Dashboards** > **Gerätezustand**, um das Dashboard anzuzeigen.




**Top – schlechter Zustand**

Dies sind die Geräte mit den meisten Integritäts- und Leistungsproblemen in Ihrer Bereitstellung. Sie können auch ins Detail gehen, um die Geräteinformationen und Benachrichtigungen zu dem Gerät anzuzeigen. Beheben Sie die kritischen Benachrichtigungen, um den Zustandsscore und die Bereitstellungsintegrität zu verbessern.

**Top – Verbesserung**

Zeigen Sie die Top-10-Geräte in einem 30-Tages-Zeitraum mit verbesserten Zustandsscores im Vergleich zu den aktuellen Gerätezustandsscores an.

**Top – Verschlechterung**

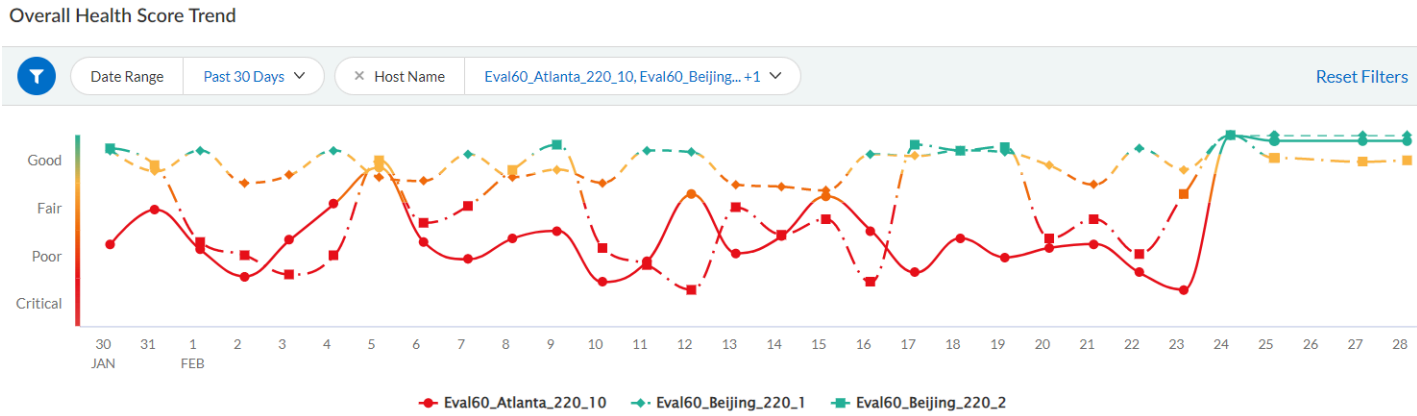
Überprüfen Sie den Gerätezustand über einen 30-Tages-Zeitraum. Dies sind die Top 10 der Geräte mit verschlechterten Zustandsscores im Vergleich zu den aktuellen Gerätezustandsscores.

# Dashboard „Gerätezustand“: Scoretrend

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | ❑ Strata Cloud Manager Essentials<br>❑ AIOps for NGFW Premium oder Strata Cloud Manager Pro |

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| | → Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

- Klicken Sie auf **Dashboards** > **Gerätezustand**, um das Dashboard anzuzeigen.




Das Diagramm zeigt den Zustandstrend Ihrer Bereitstellung für den ausgewählten Zeitraum. Fahren Sie mit dem Mauszeiger über den Auslösepunkt, um die Geräte anzuzeigen, die den Schweregrad des Zustandsscores beeinflussen. Sie können Trends für ein oder mehrere Geräte anzeigen, die nach Hostname, Modell oder Softwareversion gefiltert werden.

# Dashboard: Zusammenfassung

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden<br>• Prisma SD-WAN | Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>☐ Prisma Access<br>☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>☐ Strata Cloud Manager Essentials<br>☐ Strata Cloud Manager Pro<br>☐ Prisma SD-WAN<br>Weitere für Sichtbarkeit erforderliche Lizenzen und Voraussetzungen:<br>☐ Lizenzen zum Freischalten bestimmter Widgets im Dashboard<br>☐ eine Rolle mit der Berechtigung zum Anzeigen des Dashboards<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

- Klicken Sie auf **Strata Cloud Manager** > **Dashboards** > **Mehr Dashboards** > **Zusammenfassung**, um loszulegen.

## Was sehen Sie in diesem Dashboard?

*Das Dashboard zeigt aggregierte Daten pro Strata Logging Service-Mandant an.*

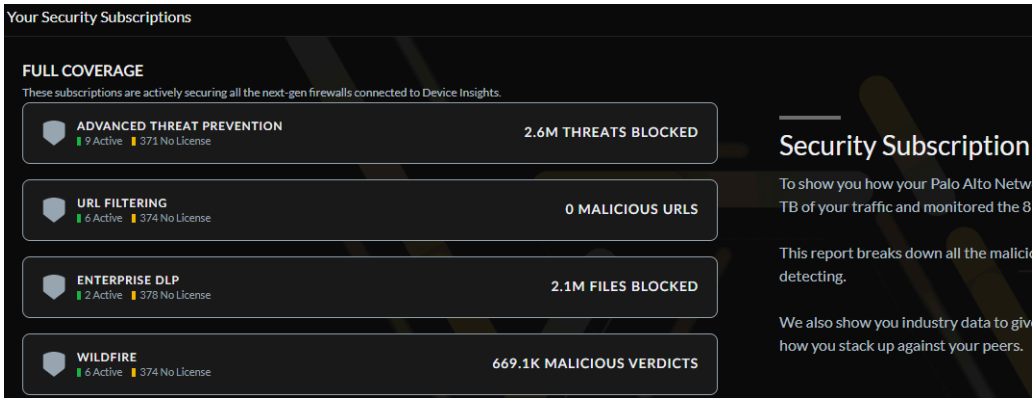
Das Dashboard „Zusammenfassung“ zeigt Ihnen, wie Ihre Palo Alto Networks-Sicherheitsabonnements Sie schützen. Dieser Bericht analysiert die böswilligen Aktivitäten in Ihrem Netzwerk, die von diesen Abonnements erkannt werden: **WildFire**, **Fortschrittliche Bedrohungsabwehr**, **Erweiterte URL-Filterung** und **Enterprise DLP**. Das Dashboard zeigt Daten für jeden dieser Dienste, einschließlich Links zu Sicherheitsdienst-Dashboards, um tiefer einzutauchen und weitere Untersuchungen durchzuführen.

Dieses Dashboard unterstützt Berichte. Diese Symbole  oben rechts im Dashboard weisen darauf hin, dass Berichte für dieses Dashboard unterstützt werden. Sie können Berichte, die die in diesem Dashboard angezeigten Daten behandeln, herunterladen, teilen und planen.

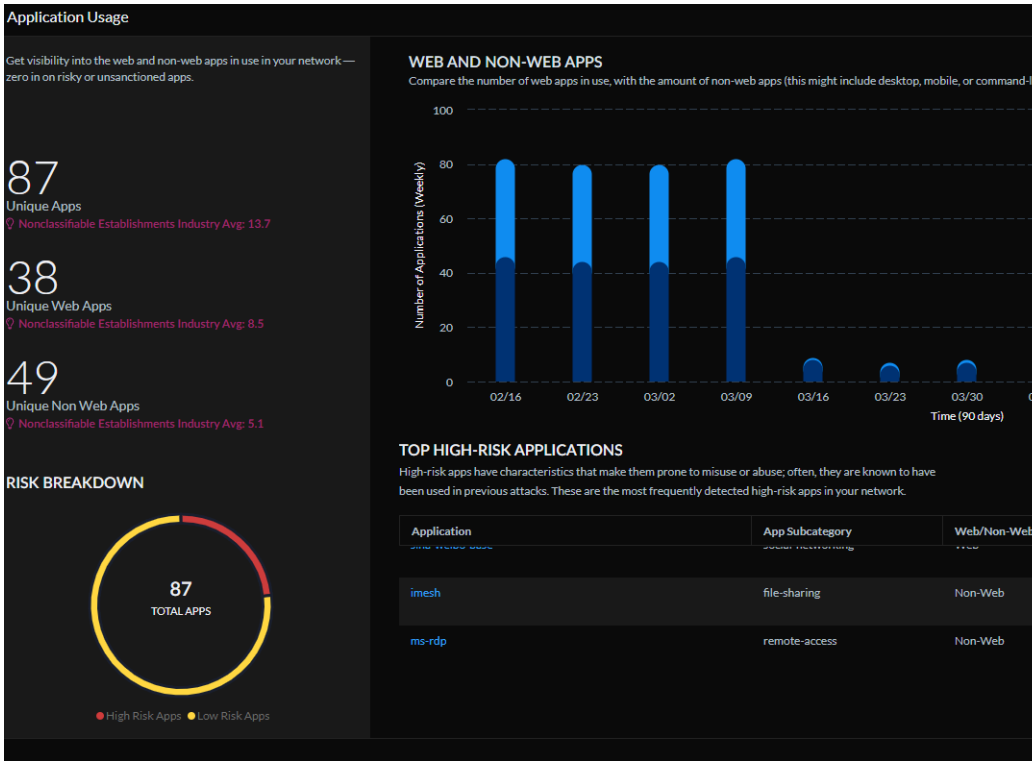
# Wie können Sie die Daten aus dem Dashboard nutzen?

- Überprüfen Sie alle bösartigen Aktivitäten, die von den aktiven Abonnements von Palo Alto Networks erkannt werden. Prüfen Sie, ob Sie die Abonnementeinstellungen oder Sicherheitsregeleinstellungen optimieren müssen, um etwaige Sicherheitslücken zu schließen.
- Zeigt Ihnen Branchendaten, um Ihnen einen Überblick über die Bedrohungslandschaft zu geben, mit der Sie konfrontiert sind, und um zu vermitteln, wie Sie im Vergleich zu Ihren Mitbewerbern dastehen.

Das Dashboard stellt die folgenden Daten bereit.

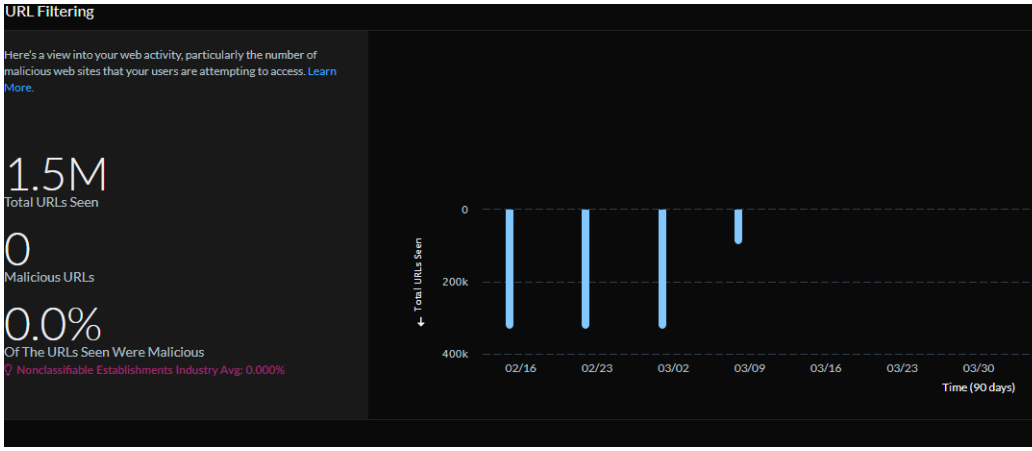
| | |
|---|---|
| **Dashboard „Zusammenfassung“: Ihre Sicherheitsabonnements** | Dieser Bericht liefert Ihnen Zahlen zu den bösartigen Aktivitäten, die Ihre Abonnements erkennen und verhindern:<br>• Anwendungen mit hohem Risiko<br>• Schwerwiegende Bedrohungen (Exploits, Malware und C2)<br>• Bösartige Webaktivitäten<br>• Dateibasierte Bedrohungen (einschließlich noch nie dagewesener Bedrohungen)<br>• Datenverlust<br>  |
| **Dashboard „Zusammenfassung“: Anwendungsnutzung** | Überprüfen Sie die Datenverkehrsprotokolle für Anwendungen mit hohem Risiko und finden Sie heraus, |

| | |
|---|---|
| | wie Sie den Sicherheitsstatus verbessern können.<br>  |
| **Dashboard „Zusammenfassung“: Fortschrittliche Bedrohungsabwehr**<br><br>*Erfordert eine Lizenz für fortschrittliche Bedrohungsabwehr.* | Untersuchen Sie die Sicherheitsrichtlinienregeln, die die meisten Bedrohungen zulassen. Überprüfen Sie diese Regeln, um herauszufinden, wo Sie eine strengere Regeldurchsetzung festlegen können. Erfahren Sie mehr. |
| **Dashboard „Zusammenfassung“: URL Filtering**<br><br>*Erfordert eine Lizenz für die erweiterte URL-Filterung.* | Überprüfen Sie die bösartigen Webaktivitäten in Ihrem Netzwerk, insbesondere die Anzahl der bösartigen |

Websites, auf die Ihre Benutzer zuzugreifen versuchen.

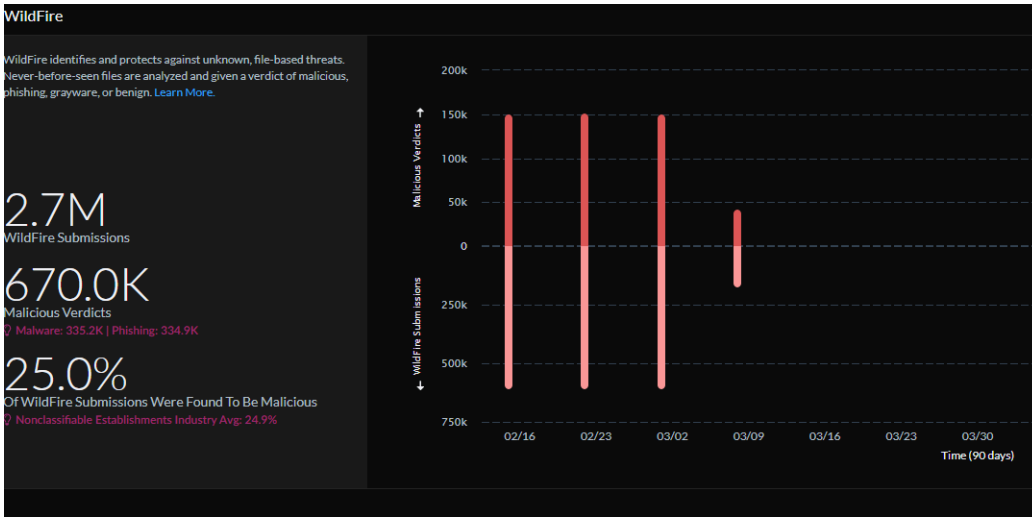



**Dashboard „Zusammenfassung“: WildFire**

*Erfordert eine Advanced WildFire-Lizenz.*

Die Peer-Daten in diesem Dashboard geben Ihnen Einblick in die Bedrohungslandschaft Ihrer Branche und zeigen Ihnen, wie Ihre Sicherheitsabdeckung im Vergleich zu ähnlichen Organisationen abschneidet. Diese Branchendaten werden auch für Abonnements angezeigt, die Sie nicht verwenden. Auf diese Weise können Sie erkennen, ob es Stellen gibt, an denen Sie die Abdeckung erhöhen können, um Sicherheitslücken zu schließen.

Hier sehen Sie einen Screenshot der Datentypen, die dieses Dashboard bereitstellt. Hier können Sie sehen, welche Arbeit WildFire leistet, um Ihr Netzwerk und Ihre Branche zu schützen. Erfahren Sie mehr. #



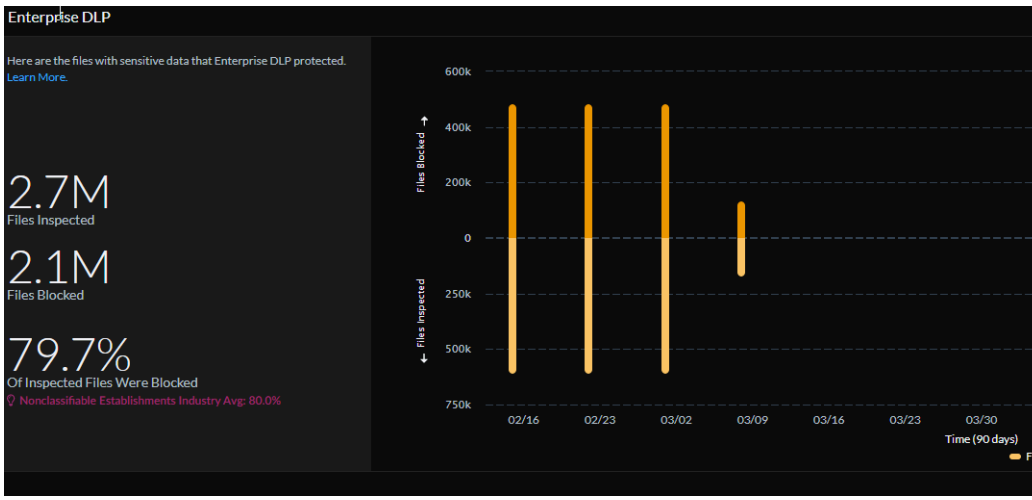

**Dashboard „Zusammenfassung“: Enterprise DLP**

Sehen Sie, wie Ihr Palo Alto Networks Enterprise DLP-Dienst Ihre Daten schützt, indem er Datensicherheitsstandards durchsetzt. Das Dashboard bietet Einblicke in die Anwendungen, bei denen die meisten Uploads durch DLP verhindert wurden, sowie die Gesamtzahl der durch DLP in Ihrem Netzwerk blockierten Dateien.

*Erfordert eine Enterprise DLP-Lizenz.*

Sie können diese Daten auch verwenden, um Vergleiche mit Branchenkollegen anzustellen und Ihre Sicherheitsstandards zu bewerten.

Überprüfen Sie die Anwendungen und Quellbenutzernamen, um besser zu verstehen, wo die DLP-Vorfälle ihren Ursprung haben, und um sie zu managen.

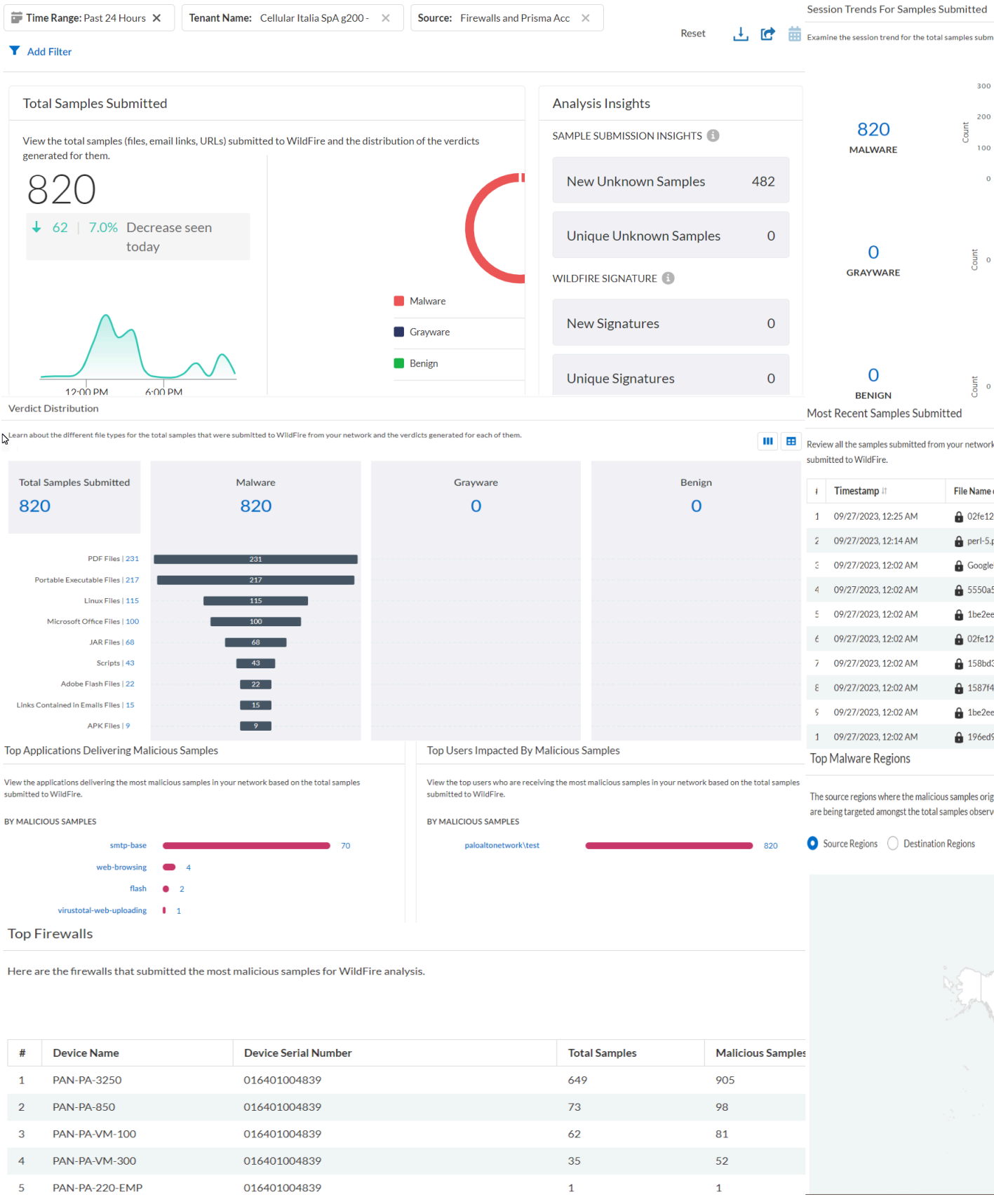


# Dashboard: WildFire

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>☐ Prisma Access<br>☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>☐ Strata Cloud Manager Essentials<br>☐ Strata Cloud Manager Pro<br>Weitere für Sichtbarkeit erforderliche Lizenzen und Voraussetzungen:<br>☐ eine Rolle mit der Berechtigung zum Anzeigen des Dashboards<br>☐ Advanced WildFire<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

- Klicken Sie auf **Strata Cloud Manager** > **Dashboards** > **Mehr Dashboards** > **WildFire**, um zu beginnen.




| # | Device Name | Device Serial Number | Total Samples | Malicious Samples |
|---|---|---|---|---|
| 1 | PAN-PA-3250 | 016401004839 | 649 | 905 |
| 2 | PAN-PA-850 | 016401004839 | 73 | 98 |
| 3 | PAN-PA-VM-100 | 016401004839 | 62 | 81 |
| 4 | PAN-PA-VM-300 | 016401004839 | 35 | 52 |
| 5 | PAN-PA-220-EMP | 016401004839 | 1 | 1 |

## Was sehen Sie in diesem Dashboard?

*Das Dashboard zeigt aggregierte Daten pro Mandanten-Dienstgruppe (TSG) an. Das Dashboard zeigt Daten aus Prisma Access, Palo Alto Networks-Firewalls und Panorama-Geräten an, die Ihrem Mandanten zugeordnet sind – vorausgesetzt, Ihre Mandanten verfügen über eine 1:1-Zuordnung zu Ihrem CSP-Konto (Customer Support Portal, Kunden-Support-Portal). Das Dashboard zeigt keine Daten aus anderen Quellen an, wenn pro Kunden-Support-Portal mehrere Mandanten verknüpft sind.*

Das WildFire-Dashboard zeigt Ihnen, wie WildFire Ihre Umgebung vor neuer Malware schützt, die in Dateien und Programmen versteckt ist. Dieses Dashboard unterstützt Berichte. Diese Symbole  oben rechts im Dashboard weisen darauf hin, dass Berichte für dieses Dashboard unterstützt werden. Sie können Berichte, die die in diesem Dashboard angezeigten Daten behandeln, herunterladen, teilen und planen.

## Wie können Sie die Daten aus dem Dashboard nutzen?

Verwenden Sie dieses Dashboard, um …

- (erfordert AIOps for NGFW Premium-Lizenz) WildFire-Übermittlungen zu überwachen und Details zu WildFire-Stichproben zu erhalten, die zur Analyse an die WildFire-Cloud übermittelt wurden
- Details zu den Zielbenutzern, den Anwendungen, die die Dateien bereitgestellt haben, den Firewalls, die die Stichproben zur Analyse übermittelt haben, sowie zu allen URLs anzuzeigen, die an der Command-and-Control-Aktivität der Dateien beteiligt sind
- (erfordert AIOps for NGFW Premium-Lizenz) WildFire-Protokolle und Analyseberichte anzuzeigen und basierend auf dem Bericht die WildFire-Einstellungen für Ihre Bereitstellung zu optimieren

## WildFire-Dashboard: Filter

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>❑ Prisma Access<br>❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>❑ Strata Cloud Manager Essentials<br>❑ Strata Cloud Manager Pro<br>Weitere für Sichtbarkeit erforderliche Lizenzen und Voraussetzungen:<br>❑ eine Rolle mit der Berechtigung zum Anzeigen des Dashboards<br>❑ Advanced WildFire |

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| | → Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Das WildFire-Dashboard bietet die folgenden Filteroptionen, um die Suche auf bestimmte Daten im Dashboard einzugrenzen.

- **Zeitbereich** – Wählen Sie zwischen **Letzte 24 Stunden**, **Vergangene 7 Tage**, **Vergangene 30 Tage** oder einem **benutzerdefinierten Zeitbereich**, um Daten für einen bestimmten Zeitrahmen anzuzeigen.
- **Mandantenname** – der Mandant, für den die Dashboard-Daten angezeigt werden.
- **Quelle** – Der Umfang der Dashboard-Daten stammt von den Firewalls von Prisma Access und von Palo Alto Networks.
- **Stichproben** – Wählen Sie die Option **Öffentlich** oder **Privat**, um die Daten anzuzeigen, die aus der Public- oder Private-Cloud-Umgebung von WildFire übermittelt wurden.
- **Urteil** – Zeigen Sie die Stichproben an, die in der WildFire-Analyse als **harmlos**, **Malware** oder **Grayware** identifiziert wurden.
- **Aktion** – Wählen Sie die Option **Zulassen** oder **Blockieren** aus, um die WildFire-Stichproben anzuzeigen, die von Ihrer Richtlinienregel zugelassen oder blockiert wurden.
- **Dateityp** – Zeigen Sie Daten basierend auf dem Dateityp der von WildFire analysierten Stichprobe an. Erfahren Sie mehr über die unterstützten Dateitypen für die WildFire-Analyse.
- **Datei-Hash** – Zeigen Sie die Daten für einen von WildFire analysierten Datei-Hash an. Nachfolgend sind die Hash-Versionen aufgeführt, die WildFire für jede analysierte Datei generiert:
  - **SHA-1** – zeigt den SHA-1-Wert für die Datei an.
  - **SHA-256** – zeigt den SHA-256-Wert für die Datei an.
  - **MD5** – zeigt die MD5-Informationen für die Datei an.
- **App-Name** – Filtern Sie Daten basierend auf den von einer Anwendung bereitgestellten Stichproben.
- **Quellregion** – Filtern Sie die Ansicht, um die Stichproben anzuzeigen, die von einem bestimmten Standort gesendet wurden.
- **Zielregion** – Filtern Sie die Ansicht, um die Stichproben anzuzeigen, die an einem bestimmten Standort empfangen wurden.
- **Benutzername** – Geben Sie den Benutzernamen ein, um die Daten für den Benutzer anzuzeigen, der die Stichprobe in Ihrem Netzwerk bereitstellen soll.
- **Seriennummer des Geräts** – Filtern Sie die Ansicht, um Daten für das Gerät anzuzeigen, das die Stichprobe zur WildFire-Analyse übermittelt hat.

# WildFire-Dashboard: Übermittelte Stichproben insgesamt

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>☐ Prisma Access<br>☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>☐ Strata Cloud Manager Essentials<br>☐ Strata Cloud Manager Pro<br>Weitere für Sichtbarkeit erforderliche Lizenzen und Voraussetzungen:<br>☐ eine Rolle mit der Berechtigung zum Anzeigen des Dashboards<br>☐ Advanced WildFire<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

- Klicken Sie auf **Dashboards** > **Mehr Dashboards** > **WildFire**, um das Dashboard anzuzeigen.

Die Gesamtzahl der während des ausgewählten Zeitraums zur WildFire-Analyse übermittelten Stichproben. Das Widget zeigt die Anzahl der von jeder Quelle übermittelten Stichproben und das für die Stichproben generierte Urteil an. Das Widget zeigt auch einen Anstieg der zur WildFire-Analyse übermittelten Stichproben an. Untersuchen Sie diese Spitzen bei den Malware-Stichproben und ergreifen Sie Maßnahmen, um die Auswirkungen von Bedrohungen auf Ihr Netzwerk einzudämmen.

# WildFire-Dashboard: Erkenntnisse aus der Analyse

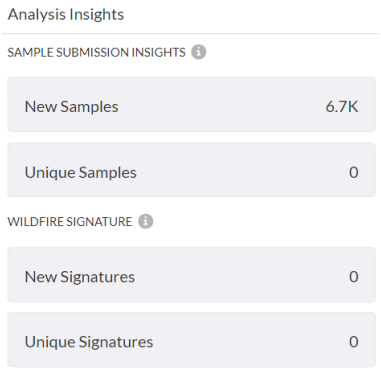
| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>☐ Prisma Access<br>☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>☐ Strata Cloud Manager Essentials<br>☐ Strata Cloud Manager Pro |

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| | Weitere für Sichtbarkeit erforderliche Lizenzen und Voraussetzungen:<br>☐ eine Rolle mit der Berechtigung zum Anzeigen des Dashboards<br>☐ Advanced WildFire<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

- Klicken Sie auf **Dashboards** > **Mehr Dashboards** > **WildFire**, um das Dashboard anzuzeigen.

Erhalten Sie Einblicke in die einzigartigen WildFire-Stichproben, die aus Ihrem Netzwerk übermittelt wurden, und in die generierten Signaturen. Verwenden Sie die Daten, um die neuen Bedrohungen zu verstehen, die im ausgewählten Zeitrahmen nur in Ihrem Netzwerk beobachtet wurden, und um zu erfahren, wie oft Ihr Netzwerk durch die generierten Signaturen geschützt wurde.

- **Einzigartige Stichproben** – Anzahl der von Ihrem Netzwerk an WildFire übermittelten Stichproben, die nur in Ihrem Netzwerk erkannt wurden, die WildFire bisher unbekannt waren und die in anderen öffentlichen oder privaten Feeds nicht verfügbar sind.
- **Neue unbekannte Stichproben** – Anzahl der neuen Stichproben, die aus Ihrem Netzwerk an WildFire übermittelt wurden und die WildFire bisher unbekannt waren (mit eindeutigem SHA256).
- **Eindeutige Signaturen** – Anzahl der Signaturen, die aus Stichproben generiert wurden, die in Ihrer Umgebung einzigartig sind.
- **Neue Signaturen** – Anzahl der von WildFire aus all Ihren hochgeladenen Stichproben erstellten neuen Signaturen.



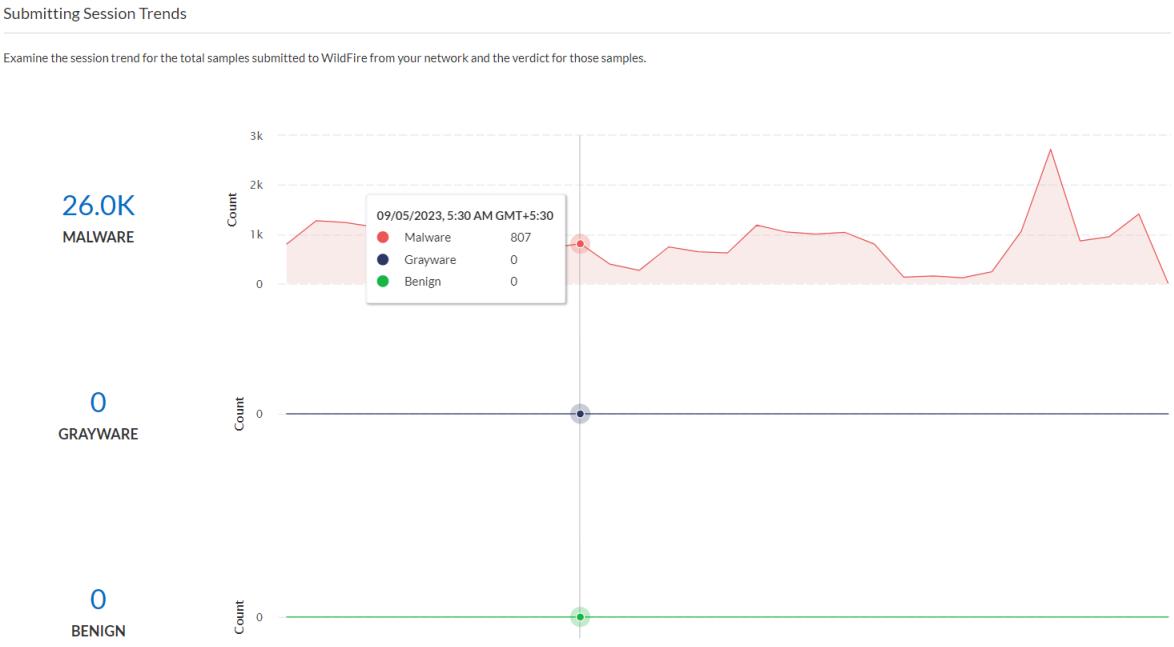

 

# WildFire-Dashboard: Sitzungstrends für übermittelte Stichproben

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>☐ Prisma Access<br>☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>☐ Strata Cloud Manager Essentials<br>☐ Strata Cloud Manager Pro<br>Weitere für Sichtbarkeit erforderliche Lizenzen und Voraussetzungen:<br>☐ eine Rolle mit der Berechtigung zum Anzeigen des Dashboards<br>☐ Advanced WildFire<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

- Klicken Sie auf **Dashboards** > **Mehr Dashboards** > **WildFire**, um das Dashboard anzuzeigen.

Untersuchen Sie die Trends für alle Stichproben, die aus Ihrem Netzwerk an WildFire übermittelt wurden, und die Urteile für diese Stichproben. Sie können eine IOC-Suche für diese Stichproben durchführen, um den Verlauf der Stichprobe in Ihrem Netzwerk und die globalen Analyseergebnisse der Stichprobe einzusehen.



# WildFire-Dashboard: Urteilsverteilung

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>☐ Prisma Access<br>☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>☐ Strata Cloud Manager Essentials<br>☐ Strata Cloud Manager Pro<br>Weitere für Sichtbarkeit erforderliche Lizenzen und Voraussetzungen:<br>☐ eine Rolle mit der Berechtigung zum Anzeigen des Dashboards<br>☐ Advanced WildFire<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

- Klicken Sie auf **Dashboards** > **Mehr Dashboards** > **WildFire**, um das Dashboard anzuzeigen.

Erfahren Sie mehr über die Urteile für neue Stichproben, die WildFire zum ersten Mal in Ihrem Netzwerk entdeckt hat. Konzentrieren Sie sich auf die Stichprobentypen, die am häufigsten Malware verbergen. Klicken Sie auf den Link, um mehr über die Stichprobe zu erfahren.

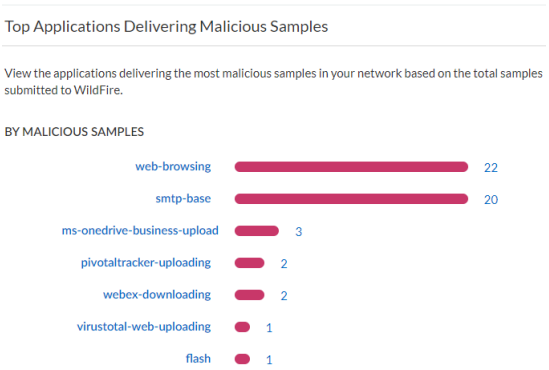

# WildFire-Dashboard: Top-Anwendungen, die bösartige Stichproben übertragen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>☐ Prisma Access<br>☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>☐ Strata Cloud Manager Essentials<br>☐ Strata Cloud Manager Pro<br>Weitere für Sichtbarkeit erforderliche Lizenzen und Voraussetzungen:<br>☐ eine Rolle mit der Berechtigung zum Anzeigen des Dashboards<br>☐ Advanced WildFire<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

- Klicken Sie auf **Dashboards** > **Mehr Dashboards** > **WildFire**, um das Dashboard anzuzeigen.

Überprüfen Sie die Details der Anwendungen, die die meisten bösartigen Stichproben in Ihr Netzwerk übertragen haben. Klicken Sie auf die Anzahl der bösartigen Stichproben, um mehr über die Stichproben zu erfahren.



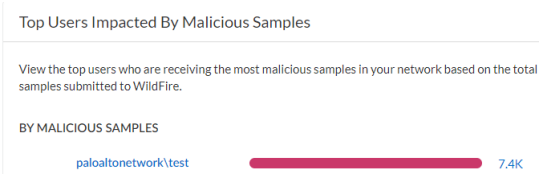

## WildFire-Dashboard: Top-Benutzer, die von bösartigen Stichproben betroffen sind

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>☐ Prisma Access<br>☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>☐ Strata Cloud Manager Essentials<br>☐ Strata Cloud Manager Pro<br>Weitere für Sichtbarkeit erforderliche Lizenzen und Voraussetzungen:<br>☐ eine Rolle mit der Berechtigung zum Anzeigen des Dashboards<br>☐ Advanced WildFire<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

- Klicken Sie auf **Dashboards** > **Mehr Dashboards** > **WildFire**, um das Dashboard anzuzeigen.

Hier werden die Benutzerkonten angezeigt, die am häufigsten verwendet werden, um bösartige Stichproben in Ihr Netzwerk zu übertragen. Klicken Sie auf den Benutzernamen, um die Benutzeraktivitätsmuster zu untersuchen.



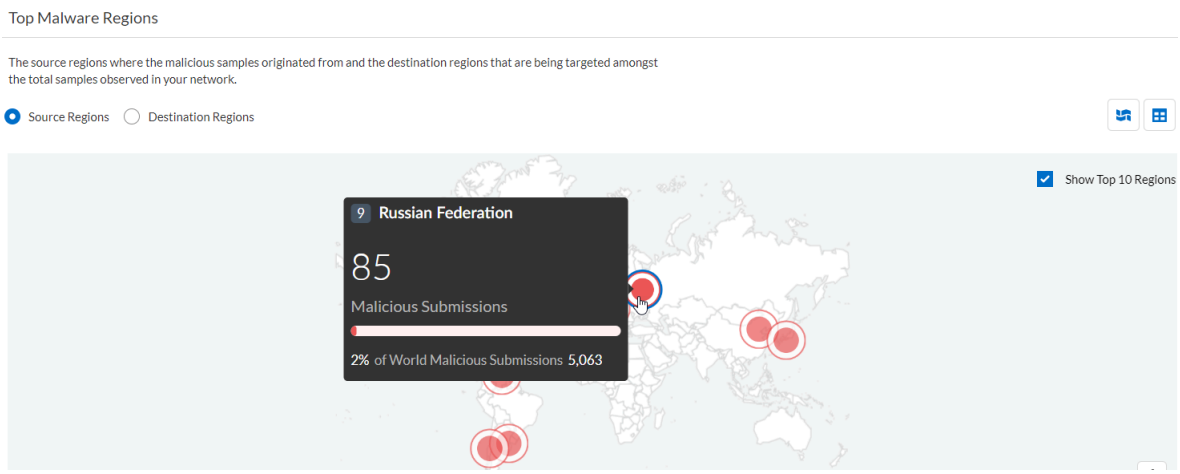

# WildFire-Dashboard: Top-Malware-Regionen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>☐ Prisma Access<br>☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>☐ Strata Cloud Manager Essentials<br>☐ Strata Cloud Manager Pro<br>Weitere für Sichtbarkeit erforderliche Lizenzen und Voraussetzungen:<br>☐ eine Rolle mit der Berechtigung zum Anzeigen des Dashboards<br>☐ Advanced WildFire<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

- Klicken Sie auf **Dashboards** > **Mehr Dashboards** > **WildFire**, um das Dashboard anzuzeigen.

Überprüfen Sie die Standorte in Ihrem Netzwerk, von denen die bösartigen Stichproben stammen oder an die sie übermittelt wurden. Sie können die Stichprobenanzahl für Quell- und Zielregionen in einem Karten- oder Tabellenformat anzeigen. Verwenden Sie diese Ansichten, um die von Malware angegriffenen Regionen zu ermitteln und die Angriffsart einzugrenzen.




# WildFire-Dashboard: Top-Firewalls

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>☐ Strata Cloud Manager Essentials<br>☐ Strata Cloud Manager Pro<br>Weitere für Sichtbarkeit erforderliche Lizenzen und Voraussetzungen:<br>☐ eine Rolle mit der Berechtigung zum Anzeigen des Dashboards<br>☐ Advanced WildFire<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

- Klicken Sie auf **Dashboards** > **Mehr Dashboards** > **WildFire**, um das Dashboard anzuzeigen.

Zeigen Sie die Firewalls an, die die bösartigsten Stichproben zur WildFire-Analyse übermitteln. Überprüfen Sie diese Firewalls, um die betroffenen Endpunkte aufzuspüren, und konfigurieren Sie die Richtlinienregeln neu, um die Bedrohungen zu reduzieren und die schädlichen Dateien an der Quelle einzudämmen.

Top Firewalls

Here are the firewalls that submitted the most malicious samples for WildFire analysis.

| # | Device Name | Device Serial Number | Total Samples | Malicious Samples |
|---|---|---|---|---|
| 1 | PAN-PA-3250 | 016401004839 | 4866 | 6947 |
| 2 | PAN-PA-5220-AC | 016401004839 | 1168 | 1715 |
| 3 | PAN-PA-VM-300 | 016401004839 | 619 | 1054 |
| 4 | PAN-PA-VM-100 | 016401004839 | 673 | 1017 |
| 5 | PAN-PA-850 | 016401004839 | 39 | 56 |
| 6 | PAN-PA-VM-500-E60 | 016401004839 | 5 | 6 |
| 7 | PAN-PA-220-EMP | 016401004839 | 3 | 5 |
| 8 | PAN-PA-5260-AC | 016401004839 | 1 | 1 |

# Dashboard: DNS Security

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>☐ Prisma Access<br>☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>☐ Strata Cloud Manager Essentials<br>☐ Strata Cloud Manager Pro<br>Weitere für Sichtbarkeit erforderliche Lizenzen und Voraussetzungen:<br>☐ eine Rolle mit der Berechtigung zum Anzeigen des Dashboards<br>☐ DNS Security oder Advanced DNS Security<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

- Klicken Sie auf **Strata Cloud Manager** > **Dashboards** > **Mehr Dashboards** > **DNS Security**, um loszulegen.

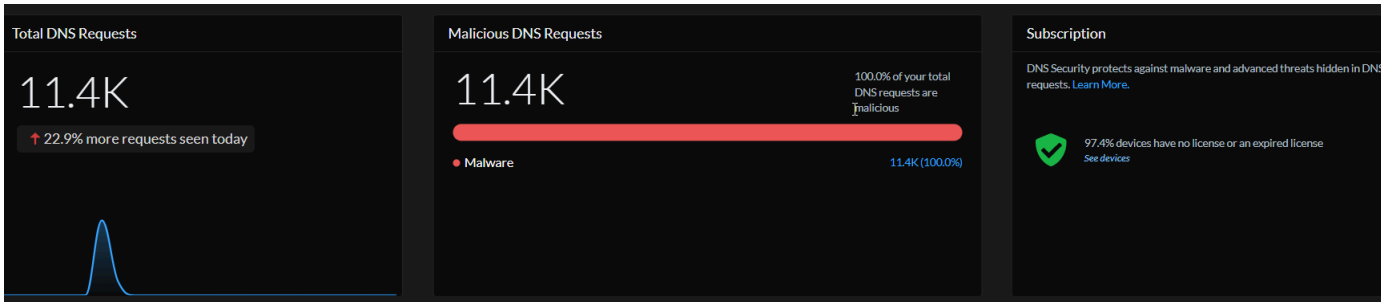
## Was sehen Sie in diesem Dashboard?

*Das Dashboard zeigt aggregierte Daten pro Mandanten-Dienstgruppe (TSG) an. Das Dashboard zeigt Daten von Prisma Access, Palo Alto Networks-Firewalls und Panorama-Geräten an, die Ihrem Mandanten zugeordnet sind.*

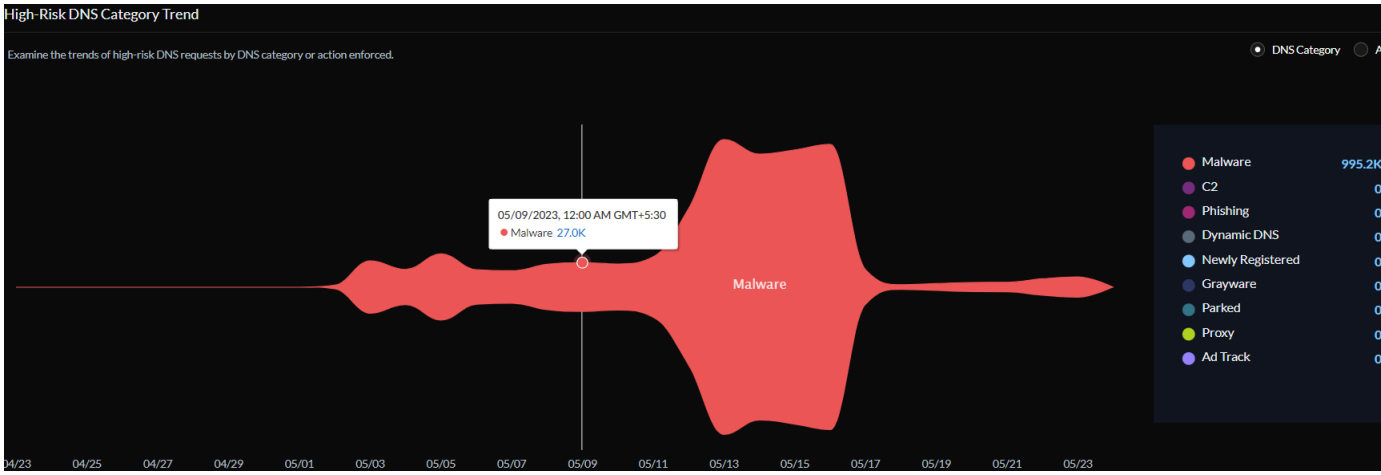
Das neue DNS Security-Dashboard zeigt Ihnen, wie Ihr DNS Security-Abonnement Sie vor erweiterten Bedrohungen und Malware schützt, die DNS verwenden. Sie können die im Dashboard angezeigten Informationen auch nach Zeitbereich, durchgeführter Aktion, Domäne, Auflöser-IP und DNS-Kategorie filtern. Die Quelle und der Mandantenname, für die die Daten im Dashboard angezeigt werden, werden in den Filtern „Mandantenname“ und „Quelle“ angezeigt. Sie können Folgendes anzeigen: DNS-Anfragestatistiken und -trends

- **Gesamtzahl der DNS-Anfragen** – zeigt die Gesamtzahl der DNS-Anfragen an, die von DNS Security verarbeitet werden. Das Liniendiagramm stellt die Anzahl der DNS-Anfragen basierend auf dem benutzerdefinierten Zeitbereich dar. Durch die Angabe eines benutzerdefinierten Zeitbereichs wird das Liniendiagramm entsprechend aktualisiert.

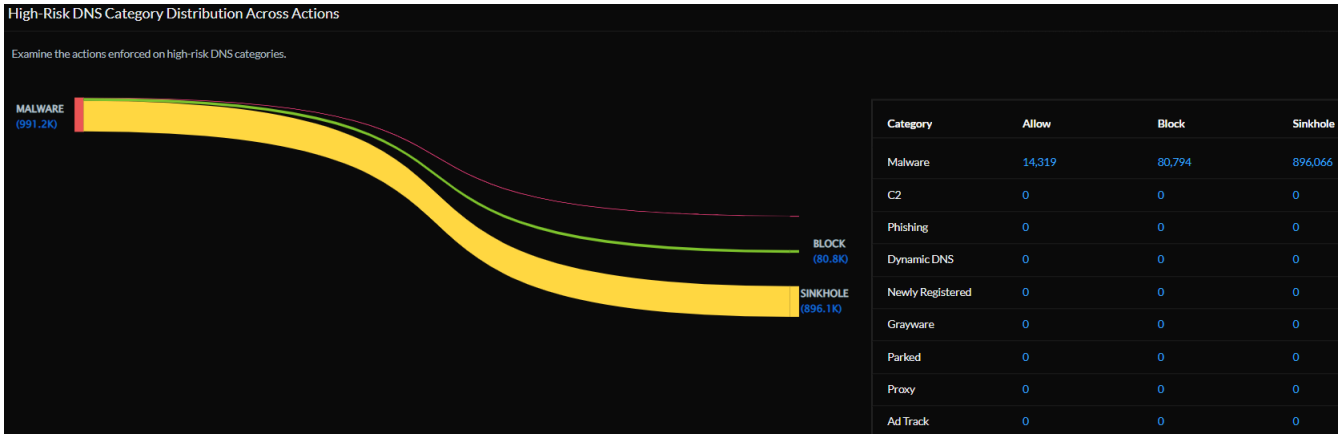
- **Bösartige DNS-Anfragen** – zeigt ein gestapeltes Balkendiagramm mit DNS-Anfragen an, die als bösartig eingestuft werden. Klicken Sie auf die verlinkte Zahl, um die Details der DNS-Anfragen anzuzeigen.
- **Abonnement** – zeigt die Anzahl der Geräte in Ihrem Netzwerk mit einem aktiven DNS Security-Abonnement an. Außerdem wird ein Prozentsatz der Geräte angezeigt, die nicht mit DNS Security ausgestattet sind oder deren Abonnement abgelaufen ist, einschließlich eines Links zu einer vollständigen Liste.




- **Trend hohes Risiko DNS-Kategorie** – Untersuchen Sie den Trend bei DNS-Anfragen mit hohem Risiko nach DNS-Kategorie oder nach den ergriffenen Maßnahmen. Bewegen Sie den Mauszeiger über einen bestimmten Ablauf, um ein Popup-Fenster zu öffnen, das die Anzahl der Anfragen oder die Art der erzwungenen Aktion anzeigt.

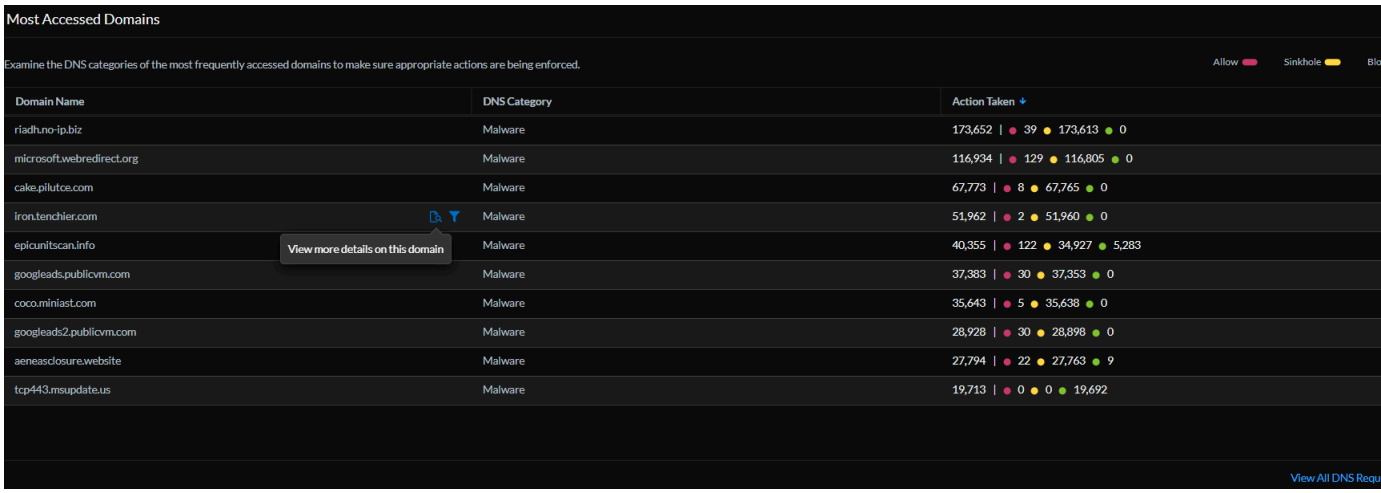



- **Hohes Risiko Verteilung DNS-Kategorie über Aktionen** – Untersuchen Sie die Maßnahmen, die die Firewall gegen bestimmte DNS-Kategorien mit hohem Risiko ergreift.

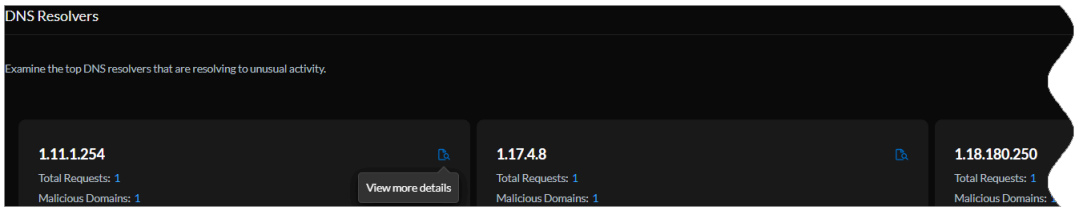


- **Am häufigsten aufgerufene Domänen** – bietet eine Liste der 10 am häufigsten aufgerufenen Domänen aus Ihrem Netzwerk, zusammen mit der DNS-Kategorie und der ausgeführten Aktion. Sie können Mehr Details anzeigen oder die relevanten Protokolle für eine Domäne einsehen. Wählen Sie **Alle DNS-Anfragen anzeigen**, um eine vollständige Liste der Domänen anzuzeigen, auf die zugegriffen wurde.




- **DNS-Auflöser** – Prüfen Sie auf bösartige und verdächtige DNS-Namensauflösungen in Ihrem Netzwerk. Zeigen Sie die besten DNS-Auflöser an, die bösartige Domänen auflösen, und die Auflöser, die verdächtig wenig DNS-Anfragen auflösen. Klicken Sie auf das Suchsymbol, um mehr Details zum Artefakt (IP-Adresse) anzuzeigen. Sie können den Verlauf des Artefakts in Ihrem Netzwerk und den globalen Analyseergebnissen anzeigen.




- **Benutzer, die bösartige Domänen besuchen** – Überprüfen Sie die Hosts in Ihrem Netzwerk, die versuchen, den Hostnamen oder die Domäne einer bösartigen URL aufzulösen.
- **(Erfordert eine Lizenz für Advanced DNS Security) Übernommene Domänen** – bietet eine Liste übernommener Domänen, die von Advanced DNS Security ermittelt wurden. Für jeden

Eintrag gibt es einen Kategorisierungsgrund und eine Anzahl der Verkehrstreffer basierend auf der Quell-IP.

Hijacked Domains

| Hijacked | Hits |
|---|---|
| xyz.test-ipv4-wildcard.hijacking.testpanw.com | 117 |
| www.test-ipv4-wildcard.hijacking.testpanw.com | 118 |
| www.test-cname-rrname-sub-wc.hijacking.testpanw.com | 353 |
| test.test-ipv4-wildcard.hijacking.testpanw.com | 118 |
| test-ipv6.hijacking.testpanw.com | 469 |
| test-ipv4.hijacking.testpanw.com | 472 |
| test-cname-rrname.hijacking.testpanw.com | 234 |
| test-cname-rrname-wc.hijacking.testpanw.com | 117 |
| qpwc.test-ipv4-wildcard.hijacking.testpanw.com | 118 |

- **(Erfordert eine Lizenz für Advanced DNS Security) Fehlkonfigurierte Domänen** – bietet eine Liste nicht auflösbarer Domänen, die mit den vom Benutzer angegebenen, öffentlich zugänglichen übergeordneten Domänen verknüpft sind. Für jeden Eintrag gibt es einen Grund für die Fehlkonfiguration und eine Anzahl von Verkehrstreffern basierend auf der Quell-IP.

Misconfigured Domains

| Misconfigured Domains | Misconfigured Reasons | Hits |
|---|---|---|
| demo.test-dnsmisconfig-zone-dangling.testpanw.com | test-dnsmisconfig-zone-dangling.testpanw.com:A:1.2.3.4 the IP 1.2.3.4 is allocatable | 117 |
| adns-demo.test-dnsmisconfig-zone-dangling.testpanw... | test-dnsmisconfig-zone-dangling.testpanw.com:A:1.2.3.4 the IP 1.2.3.4 is allocatable | 117 |
| abc.test-dnsmisconfig-zone-dangling.testpanw.com | test-dnsmisconfig-zone-dangling.testpanw.com:A:1.2.3.4 the IP 1.2.3.4 is allocatable | 589 |
| 123demo.test-dnsmisconfig-zone-dangling.testpanw.c... | test-dnsmisconfig-zone-dangling.testpanw.com:A:1.2.3.4 the IP 1.2.3.4 is allocatable | 0 |
| 123.test-dnsmisconfig-zone-dangling.testpanw.com | test-dnsmisconfig-zone-dangling.testpanw.com:A:1.2.3.4 the IP 1.2.3.4 is allocatable | 471 |

Dieses Dashboard unterstützt Berichte. Diese Symbole  oben rechts im Dashboard weisen darauf hin, dass Berichte für dieses Dashboard unterstützt werden. Sie können Berichte, die die in diesem Dashboard angezeigten Daten behandeln, herunterladen, teilen und planen.

## Wie können Sie die Daten aus dem Dashboard nutzen?

Mithilfe dieses Dashboards können Sie ...

- untersuchen, wie DNS-Anfragen verarbeitet und kategorisiert werden
- Einblicke in DNS-basierte Bedrohungen erhalten
- DNS-Anfragen übernommener und fehlkonfigurierter Domänen mit Advanced DNS Security erkennen

# Dashboard: KI-Laufzeitsicherheit

Das Dashboard „Strata Cloud Manager (SCM) Command Center“ bietet eine konsolidierte Ansicht der in Clustern und VMs bereitgestellten Cloud-Workloads, wie etwa der Pods, Modelle, Apps, VMs und Namespaces.

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • KI-Laufzeitsicherheit | ☐ Aktivieren Ihrer Lizenz für KI-Laufzeitsicherheit<br>☐ Voraussetzungen für die Einrichtung der KI-Laufzeitsicherheit<br>☐ Integrieren und Aktivieren eines Cloud-Kontos in SCM |

## Erkennen von Cloud-Ressourcen

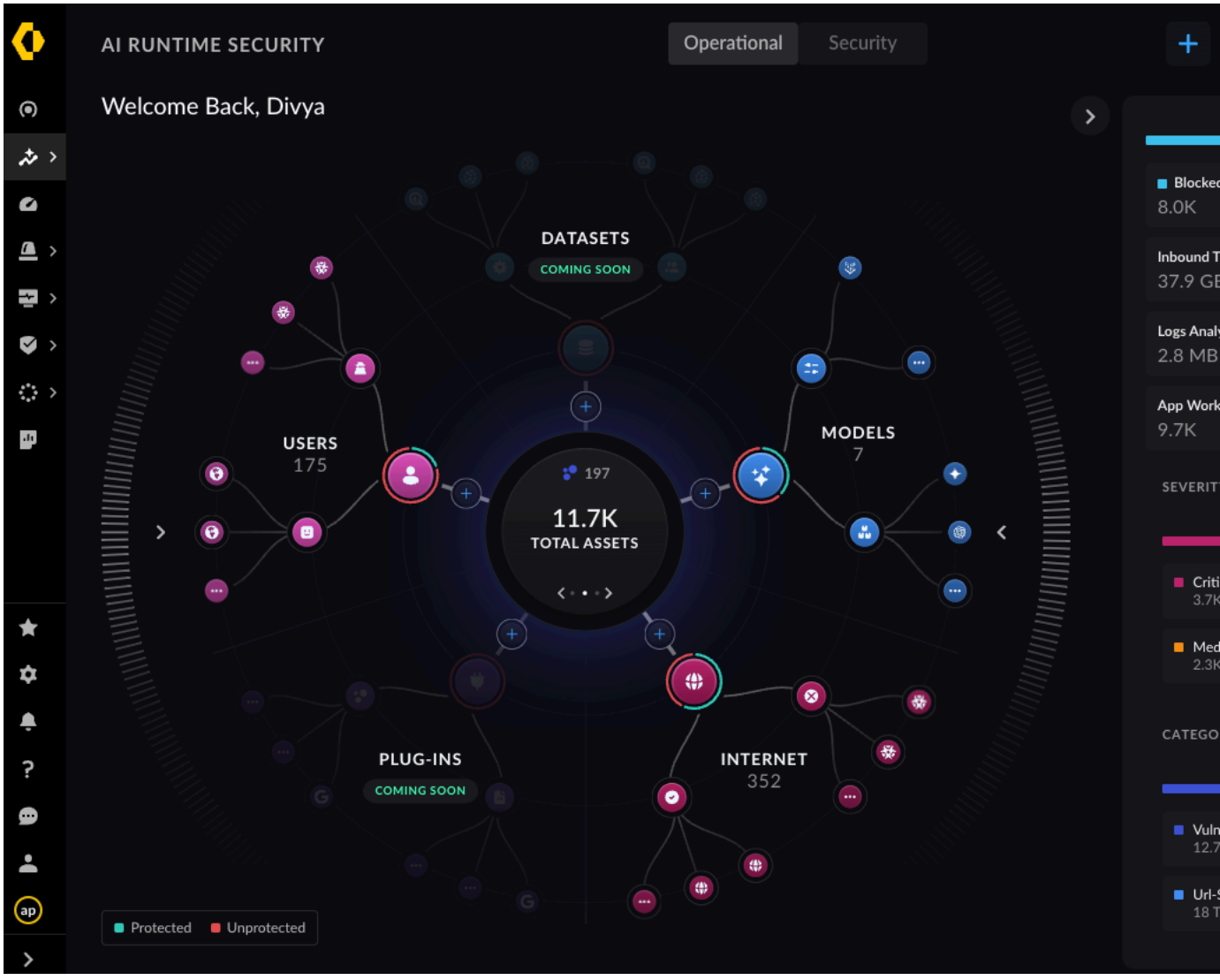
Nach dem erfolgreichen Onboarding Ihres Cloud-Kontos in SCM und der Aktivierung Ihres Servicekontos bietet das SCM-Dashboard eine einheitliche Echtzeit-Asset-Erkennung Ihrer Cloud-Workloads.

Das **Cloud Application Command Center** in SCM unter **Insights → KI-Laufzeitsicherheit** bietet aussagekräftige Einblicke in die Erkennung sämtlicher Cloud-Assets in Ihrem integrierten Cloud-Konto.

Die Asset-Erkennung im SCM-Dashboard ist in die Betriebs- und die Sicherheitsansicht unterteilt.

Die Erkennung zeigt eine Aufschlüsselung der Bedrohungen basierend auf der Dringlichkeit der Bedrohung und den Risikokategorien, darunter Sicherheitslückenerkennung, URL-Sicherheit und Prompt Injection.

1. Die **Betriebsansicht** ist eine aggregierte Ansicht, die Folgendes enthält:
    1. eine Gesamtanzahl und Aufschlüsselung der in Ihren integrierten Cloud-Umgebungen entdeckten Assets
    2. Datenverkehrsflüsse – durch die KI-Laufzeitsicherheitsinstanz geschützt bzw. ungeschützt
    3. Anwendungsworkloads (Container, Serverless-Funktionen und VMs)
    4. abgefragte KI-Modelle
    5. Benutzeranwendungen, die auf Internetziele zugreifen
    6. Benutzeranwendungen, auf die von externen Anwendungen aus zugegriffen wird
    7. Statistiken zum eingehenden und ausgehenden Datenverkehr



2. In der **Sicherheitsansicht** haben Sie folgende Möglichkeiten:
   1. Sie können eine KI-Laufzeitsicherheitsinstanz hinzufügen (Symbol „+“), um den ungeschützten Netzwerkverkehr zu schützen, wie in der Betriebsansicht angegeben.
   2. Wenn der Schutz der KI-Laufzeitsicherheitsinstanz bereits vorhanden ist, leiten Sie den ungeschützten Datenverkehr über die verfügbare KI-Laufzeitsicherheitsinstanz um.

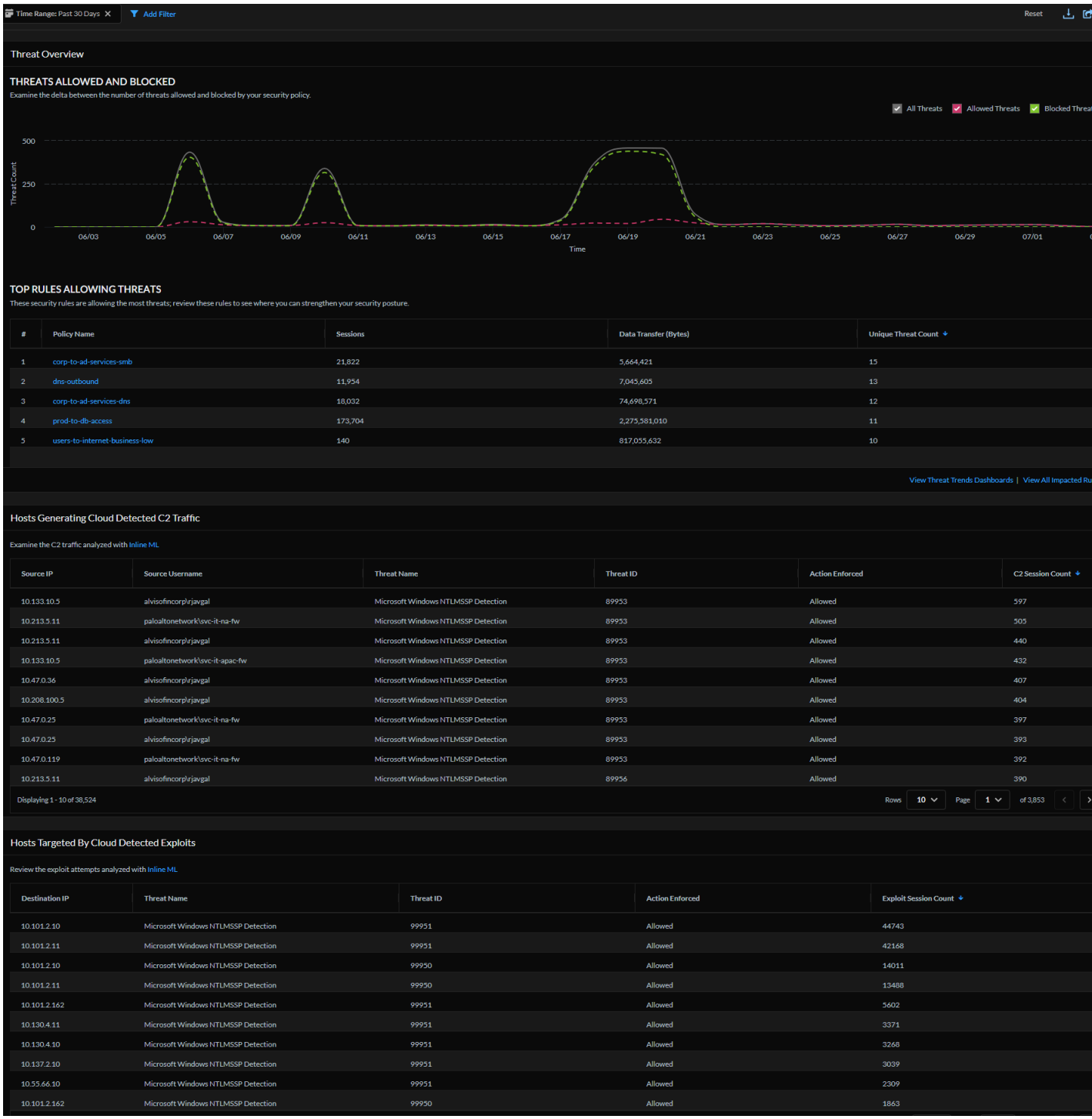

Erkennen Sie als Nächstes die riskanten Netzwerkflusspfade zwischen den Benutzer-Apps, KI-Modellen und dem Internet. Sehen Sie sich die Risikoanalyse des KI-Netzwerkverkehrs an und stellen Sie eine KI-Laufzeitsicherheitsinstanz bereit, um Ihre Cloud-Netzwerkarchitektur zu überwachen und zu schützen.

# Dashboard: Fortschrittliche Bedrohungsabwehr

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>☐ Prisma Access<br>☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>☐ Strata Cloud Manager Essentials<br>☐ Strata Cloud Manager Pro<br>Weitere für Sichtbarkeit erforderliche Lizenzen und Voraussetzungen:<br>☐ eine Rolle mit der Berechtigung, das Dashboard anzuzeigen<br>☐ Bedrohungsabwehr oder fortschrittliche Bedrohungsabwehr<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

- Klicken Sie auf **Strata Cloud Manager** > **Dashboards** > **Mehr Dashboards** > **Fortschrittliche Bedrohungsabwehr**, um loszulegen.




# Was sehen Sie in diesem Dashboard?

*Das Dashboard zeigt aggregierte Daten pro Strata Logging Service-Mandant an.*

Das Dashboard „Fortschrittliche Bedrohungsabwehr“ bietet einen Einblick in die in Ihrem Netzwerk erkannten Bedrohungen und identifiziert Möglichkeiten zur Verbesserung Ihres

Sicherheitsstatus. Bedrohungen werden mithilfe von Inline-Cloud-Analyse-Modellen und Bedrohungssignaturen erkannt, die aus bösartigen Verkehrsdaten generiert werden, die von verschiedenen Palo Alto Networks-Diensten gesammelt wurden. Dieses Dashboard bietet eine Zeitleistenansicht der erlaubten und blockierten Bedrohungen sowie eine Liste der Hosts, die von der Cloud erkannten C2-Verkehr generieren, sowie von Hosts, die durch von der Cloud erkannte Exploits angegriffen werden.

Dieses Dashboard unterstützt Berichte. Diese Symbole  oben rechts im Dashboard weisen darauf hin, dass Berichte für dieses Dashboard unterstützt werden. Sie können Berichte, die die in diesem Dashboard angezeigten Daten behandeln, herunterladen, teilen und planen.

## Wie können Sie die Daten aus dem Dashboard nutzen?

Verwenden Sie dieses Dashboard, um ...

- Bedrohungstransparenz in Ihrem Netzwerkverkehr zu erhalten
- Bedrohungssitzungen zu analysieren, um die Genauigkeit Ihrer Richtlinienregeln zu verbessern
- Einblicke in die durch Inline-Cloud-Analysen erkannten Bedrohungen in Echtzeit zu erhalten
- den Kontext der Bedrohung anhand von Protokollen und Cloud-Berichten zu ermitteln und diese Daten zur Verbesserung Ihres Reaktionsprozesses auf Vorfälle zu verwenden

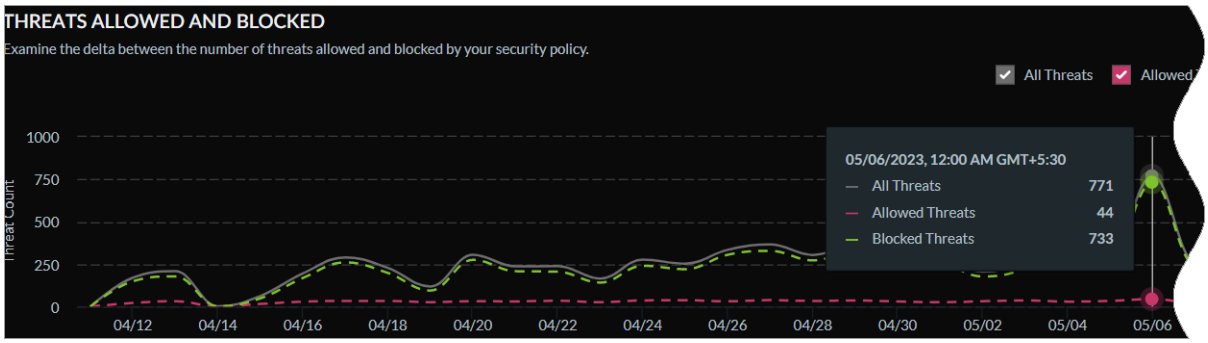
## Dashboard der fortschrittlichen Bedrohungsabwehr: Bedrohungsübersicht

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>❑ Prisma Access<br>❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>❑ Strata Cloud Manager Essentials<br>❑ Strata Cloud Manager Pro<br>Weitere für Sichtbarkeit erforderliche Lizenzen und Voraussetzungen:<br>❑ eine Rolle mit der Berechtigung, das Dashboard anzuzeigen<br>❑ Bedrohungsabwehr oder fortschrittliche Bedrohungsabwehr<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

- Klicken Sie auf **Strata Cloud Manager** > **Dashboards** > **Mehr Dashboards** > **Fortschrittliche Bedrohungsabwehr**, um das Dashboard anzuzeigen.

Vergleichen Sie das Verhältnis zwischen von Sicherheitsregeln erlaubten und blockierten Bedrohungen.



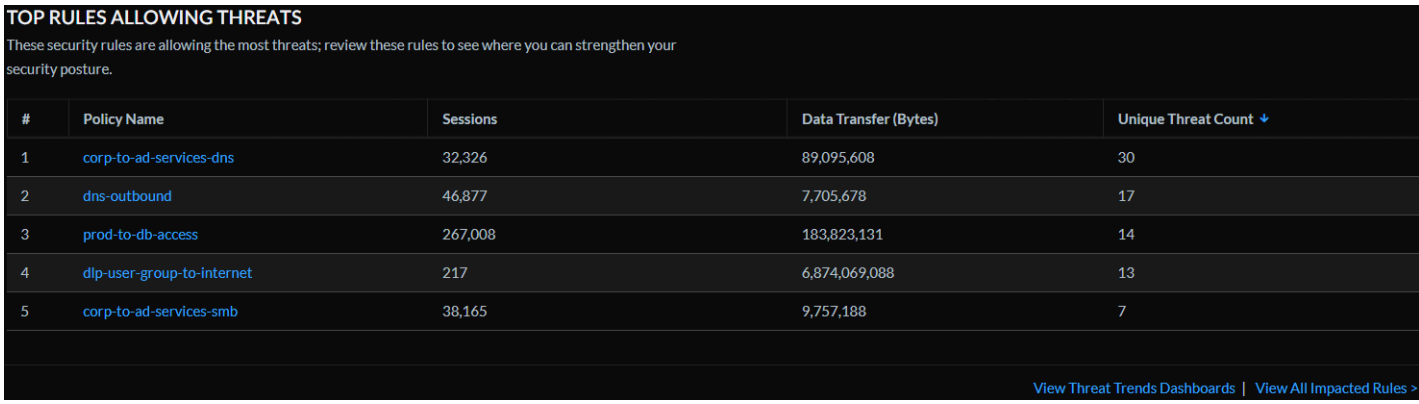

## Dashboard der fortschrittlichen Bedrohungsabwehr: Top-Regeln, die Bedrohungen erlauben

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>☐ Prisma Access<br>☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>☐ Strata Cloud Manager Essentials<br>☐ Strata Cloud Manager Pro<br>Weitere für Sichtbarkeit erforderliche Lizenzen und Voraussetzungen:<br>☐ eine Rolle mit der Berechtigung, das Dashboard anzuzeigen<br>☐ Bedrohungsabwehr oder fortschrittliche Bedrohungsabwehr<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

- Klicken Sie auf **Strata Cloud Manager** > **Dashboards** > **Mehr Dashboards** > **Fortschrittliche Bedrohungsabwehr**, um das Dashboard anzuzeigen.

Untersuchen Sie die Bedrohungssitzungen, die der Sicherheitsrichtlinienregel entsprechen, und finden Sie heraus, ob Sie die Richtlinienregel ändern müssen, um Ihre Sicherheit zu stärken. In Activity Insights können Sie die Bedrohungen und Abgleichsregeln weiter analysieren.




| Säule | Beschreibung |
|---|---|
| **Richtlinienname** | Die Sicherheitsrichtlinienregel, die die entsprechenden Bedrohungen zulässt. |
| **Sitzungen** | Die Anzahl der Bedrohungssitzungen, die der Sicherheitsrichtlinienregel entsprachen. |
| **Datenübertragung (Bytes)** | Die Menge an Daten, die Bedrohungssitzungen durchlaufen haben, die der Sicherheitsrichtlinienregel entsprachen. |
| **Anzahl einzigartiger Bedrohungen** | Die Anzahl der Bedrohungen, die der Sicherheitsrichtlinienregel entsprachen. |

## Dashboard der fortschrittlichen Bedrohungsabwehr: Hosts generieren in der Cloud erkannten C2-Datenverkehr

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>❑ Prisma Access<br>❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>❑ Strata Cloud Manager Essentials<br>❑ Strata Cloud Manager Pro<br>Weitere für Sichtbarkeit erforderliche Lizenzen und Voraussetzungen:<br>❑ eine Rolle mit der Berechtigung, das Dashboard anzuzeigen |

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| | ❑ Bedrohungsabwehr oder fortschrittliche Bedrohungsabwehr<br><br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

- Klicken Sie auf **Strata Cloud Manager** > **Dashboards** > **Mehr Dashboards** > **Fortschrittliche Bedrohungsabwehr**, um das Dashboard anzuzeigen.

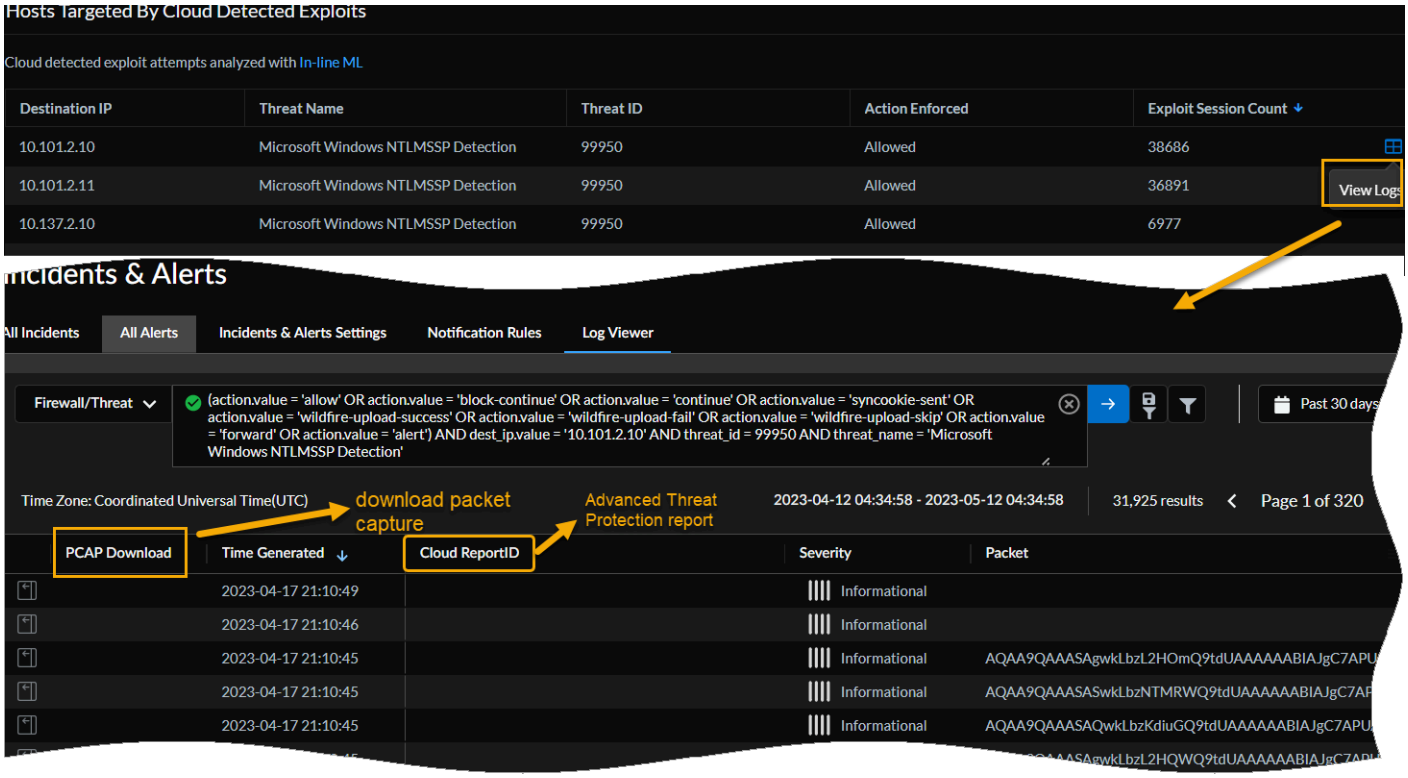
Untersuchen Sie die Quell-IPs und Benutzer, die für die Generierung von Command-and-Control-Datenverkehr (C2) verantwortlich sind. Die fortschrittliche Bedrohungsabwehr verwendet cloudbasierte Engines und Inline-Cloud-Analysen, um den Datenverkehr auf unbekannte C2-Angriffe und Sicherheitslücken zu scannen und zu analysieren. Klicken Sie auf das Suchsymbol neben der Quell-IP, um die mit der Quell-IP verbundenen Nutzungsmuster zu überprüfen. Ein Link zum Protokoll-Viewer hilft bei der Analyse der Bedrohungssitzungen, beim Herunterladen der Paketerfassung und des Cloud-Berichts, um zusätzlichen Kontext zu erhalten, bei der Nutzung der Bedrohungsanalysedaten von Palo Alto Networks sowie bei der Verbesserung Ihrer Vorfallreaktionsprozesse.

## Dashboard der fortschrittlichen Bedrohungsabwehr: Hosts im Visier von in der Cloud erkannten Exploits

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br><br>❑ Prisma Access<br>❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>❑ Strata Cloud Manager Essentials<br>❑ Strata Cloud Manager Pro<br><br>Weitere für Sichtbarkeit erforderliche Lizenzen und Voraussetzungen:<br><br>❑ eine Rolle mit der Berechtigung, das Dashboard anzuzeigen<br>❑ Bedrohungsabwehr oder fortschrittliche Bedrohungsabwehr<br><br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

- Klicken Sie auf **Strata Cloud Manager** > **Dashboards** > **Mehr Dashboards** > **Fortschrittliche Bedrohungsabwehr**, um das Dashboard anzuzeigen.

Dies sind die IPs, auf die Sicherheitslücken-Exploits abzielen. Die fortschrittliche Bedrohungsabwehr verwendet cloudbasierte Engines und Inline-Cloud-Analysen, um diesen Datenverkehr zu erkennen und zu analysieren. Bewegen Sie den Mauszeiger über die Ziel-IP-Adresse und klicken Sie auf das Suchsymbol, um die Nutzungsmuster im Zusammenhang mit der Ziel-IP zu überprüfen. Sehen Sie sich Protokolle an, um Kontext rund um die Bedrohung zu erhalten. Laden Sie den Cloud-Bericht und die Paketerfassung aus den Protokollen herunter, um zusätzlichen Kontext zu erhalten, und nutzen Sie die Bedrohungsanalysedaten und Bedrohungsdaten von Palo Alto Networks, um Ihre Vorfallreaktionsprozesse zu verbessern.

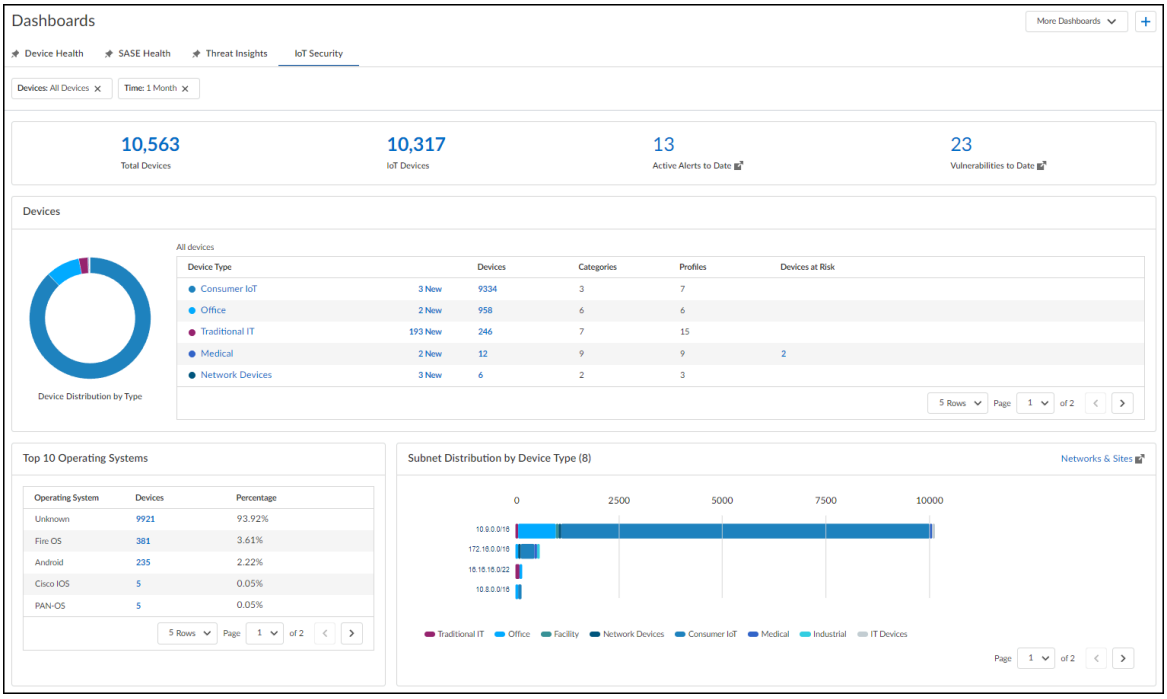


# Dashboard: IoT Security

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>☐ Prisma Access<br>☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>☐ Strata Cloud Manager Essentials<br>☐ Strata Cloud Manager Pro<br>Weitere für Sichtbarkeit erforderliche Lizenzen und Voraussetzungen:<br>☐ eine Rolle mit der Berechtigung zum Anzeigen des Dashboards<br>☐ IoT Security<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Wählen Sie zunächst **Dashboards** > **Mehr Dashboards** > **IoT-Sicherheit** aus.



## Was sehen Sie in diesem Dashboard?

Das IoT Security-Dashboard bietet Informationen zu den Geräten im Netzwerk, ihren Geräteprofilen und Ihren Betriebssystemen sowie dazu, wie sie auf die Subnetze verteilt sind (nach Gerätetyp). Für fortgeschrittene IoT-Sicherheitsprodukte (Enterprise IoT Security Plus, Industrial IoT Security oder Medical IoT Security) zeigt das IoT Security-Dashboard zusätzlich die Gesamtzahl der bis heute aktiven Benachrichtigungen und Sicherheitslücken an.

Blau formatierter Text ist interaktiv. Folgendes passiert, wenn Sie darauf klicken:

- Zusammenfassung (oben) – **Gesamtzahl Geräte** und **IoT-Geräte** verlinken zur Seite **Überwachen** > **Assets** mit angewendeten Filtern, um den Bestand für alle Geräte oder alle IoT-Geräte anzuzeigen. Der blaue Text für „Aktive Benachrichtigungen“ und „Aktive Sicherheitslücken“ öffnet die entsprechenden Seiten in Ihrem IoT Security-Portal. (Wenn keine Benachrichtigungen oder Sicherheitslücken vorliegen, lautet die Zahl 0 und es gibt keinen Link.)
- Geräte – Klicken Sie auf einen Abschnitt im Diagramm oder auf einen Eintrag in der Spalte „Gerätetyp“, um die Anzeige zu vergrößern und die Gerätekategorien innerhalb eines ausgewählten Typs anzuzeigen. Von dort aus können Sie auch die Geräteprofile innerhalb einer ausgewählten Kategorie aufrufen. Wenn Sie im Diagramm **Zurück** auswählen oder über der Tabelle auf eine Brotkrumennavigation klicken, wird wieder auf eine breitere Ebene der Geräteklassifizierung herausgezoomt.

  Die Zahlen in den Spalten „Geräte“ und „Gefährdete Geräte“ verweisen auf die Seite **Überwachen** > **Assets**. Strata Cloud Manager wendet automatisch einen Filter an, um Geräte anzuzeigen, die der ausgewählten Spalte und Zeile entsprechen. Je nach der angezeigten Ebene kann es sich dabei um den Gerätetyp, den Kategorienamen oder den Profilnamen handeln.

  *Manchmal sehen Sie die Anzahl neuer Geräte, die IoT Security im Netzwerk erkennt. Diese Zahlen werden links neben den Zahlen in der Spalte „Geräte“ angezeigt. IoT Security betrachtet Geräte als „Neu“, wenn sie innerhalb des oben im Dashboard festgelegten Zeitfilters erstmals im Netzwerk erkannt werden.*
- Top-10-Betriebssysteme – Die Zahlen in der Spalte „Geräte“ verlinken zur Seite **Überwachen** > **Assets** mit einem angewendeten Filter, der nur Geräte mit dem ausgewählten Betriebssystem anzeigt.
- Subnetzverteilung nach Gerätetyp – Bewegen Sie den Mauszeiger über die Leiste für ein Subnetz, um die Anzahl der nach Gerätetyp gruppierten Geräte im Subnetz anzuzeigen. Mithilfe dieser Informationen können Sie feststellen, ob zu viele nicht verwandte Gerätetypen im selben Subnetz vermischt sind. Wenn Sie beispielsweise Gebäude-, Industrie- und Verbraucher-IoT-Geräte in einem Subnetz sehen, sollten Sie möglicherweise die Geräte jedes Typs in eigene, separate Subnetze segmentieren. Wenn Sie auf **Netzwerke und Standorte** klicken, wird ein neues Browserfenster geöffnet, wo **Netzwerke** > **Netzwerke und Standorte** > **Netzwerke** im IoT-Sicherheitsportal angezeigt wird.

## Wie können Sie die Daten aus diesem Dashboard nutzen?

Verwenden Sie die Daten in diesem Dashboard, um mehr über die Geräte in Ihrem Netzwerk zu erfahren:

**Filter** (oben auf der Seite)

- Filtern Sie die im Dashboard angezeigten Daten nach Gerätetyp und Zeitraum (letztes Jahr, letzter Monat, letzte Woche, letzter Tag oder letzte Stunde), um Daten zu den Geräten anzuzeigen, die Sie interessieren.

**Zusammenfassung** (oben im Dashboard)

- Sehen Sie sich die Gesamtzahl der Geräte an, die in Ihrem Netzwerk aktiv waren, bestimmt durch Gerätetyp und Zeitfilter.
- Sehen Sie, wie viele der insgesamt aktiven Geräte IoT-Geräte sind.
- Entwickeln Sie ein Gespür für die Sicherheitslandschaft, in der die Geräte arbeiten, indem Sie sich die Anzahl der aktiven Benachrichtigungen und bisher erkannten Sicherheitslücken ansehen.

**Geräte**

- Informieren Sie sich über die Anzahl der Geräte verschiedener Gerätetypen und erfahren Sie im Detail, wie viele Geräte es in den verschiedenen Gerätekategorien und -profilen gibt. Informieren Sie sich über die Anzahl der Geräte mit kritischem Risiko auf den einzelnen präzisen Ebenen der Geräteklassifizierung und finden Sie heraus, um welche Art von Geräten es sich handelt.

**Top-10-Betriebssysteme**

- Von allen Geräten, deren Betriebssystem IoT Security erkannt hat, sehen Sie die zehn gängigsten Betriebssysteme, die Anzahl der Geräte, auf denen sie ausgeführt werden, sowie den Prozentsatz aller Geräte.

**Subnetzverteilung nach Gerätetyp**

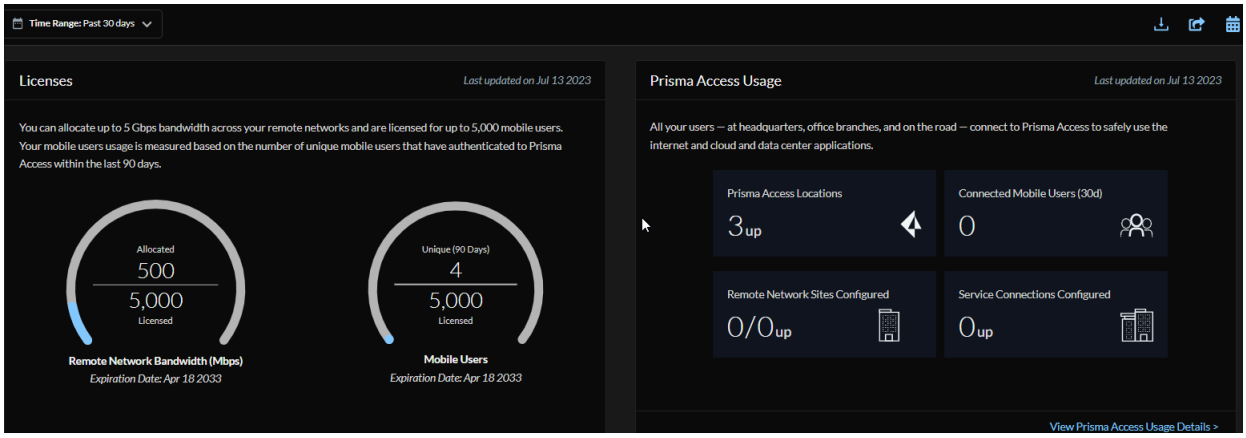
- Sehen Sie, wie verschiedene Gerätetypen auf Subnetze im gesamten Netzwerk verteilt sind. Wenn Sie einen umfangreichen Mix unterschiedlicher Gerätetypen im selben Subnetz feststellen, sollten Sie eine Segmentierung in eigene, separate Subnetze in Erwägung ziehen.

# Dashboard: Prisma Access

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager) | Eine der folgenden Komponenten:<br>☐ Prisma Access-Lizenz<br>☐ Strata Cloud Manager Pro<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

- Klicken Sie auf **Strata Cloud Manager** > **Dashboards** > **Mehr Dashboards** > **Prisma Access**, um zu beginnen.




## Was sehen Sie in diesem Dashboard?

Erfahren Sie, wie Sie die im Rahmen Ihrer Lizenz verfügbare Funktionalität nutzen können, und verschaffen Sie sich einen Überblick über den Zustand und die Leistung Ihrer Prisma Access-Umgebung.

Prisma Access-Nutzungsdaten umfassen:

- eine Übersicht über Ihre Prisma Access-Nutzung – Ihre Lizenzen, Prisma Access-Standorte und Kapazität mobiler Benutzer und/oder Bandbreitennutzung
- Top-Prisma Access-Standorte für mobile Benutzer und Remote-Netzwerke
- den gesamten Bandbreitenverbrauch für Remote-Netzwerk- und Dienstverbindungsstandorte sowie die verbrauchsstärksten Remote-Netzwerk- und Service-Verbindungsstandorte
- Trends zur Tunnelunterbrechung, einschließlich der am stärksten betroffenen Tunnel

*Das Dashboard zeigt die aggregierten Daten pro Prisma Access-Mandanten.*

Dieses Dashboard unterstützt Berichte. Diese Symbole  oben rechts im Dashboard weisen darauf hin, dass Berichte für dieses Dashboard unterstützt werden. Sie können Berichte, die die in diesem Dashboard angezeigten Daten behandeln, herunterladen, teilen und planen.

## Wie können Sie die Daten aus dem Dashboard nutzen?

Dieses Dashboard hilft Ihnen, Einblick in die Prisma Access-Nutzung in Ihrem Netzwerk zu gewinnen und Ihre Konfigurationseinstellungen basierend auf den Dashboard-Daten anzupassen.

# Dashboard: Anwendungserfahrung

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)* | ❑ Prisma Access-Lizenz<br>❑ ADEM Observability-Lizenz zum Anzeigen der Daten für überwachte Anwendungen<br>❑ Lizenz für Remote-Netzwerke<br>*(erforderlich, um die Daten zu „Erfahrung für Remote-Standort“ anzuzeigen)* |

- Klicken Sie auf **Strata Cloud Manager** > **Dashboards** > **Mehr Dashboards** > **Anwendungserfahrung**, um loszulegen.

## Was sehen Sie in diesem Dashboard?

Die in diesem Dashboard angezeigten Daten ändern sich und entsprechen der Karte, die Sie auswählen: „Erfahrung der mobilen Benutzer“ oder „Erfahrung für Remote-Standort“. Wenn Sie neu bei AI-Powered ADEM sind, können Sie damit beginnen, die Anwendungen zu untersuchen, die in Ihrer Organisation verwendet werden. Mit diesen Informationen können Sie dann ermitteln, für welche Anwendungen Sie Anwendungstests erstellen möchten. Wenn Benutzer oder Remote-Standorte Anwendungsprobleme melden, ist dieses Dashboard ein guter Ort, um mit der Eingrenzung des Problems zu beginnen. Die Anwendungsnutzungsdaten werden aus dem tatsächlichen Benutzerdatenverkehr abgerufen, der Prisma Access durchläuft. Dazu gehört auch der Datenverkehr von mobilen Benutzern und Remote-Standorten.

Sie können einen Filter hinzufügen, um die Ergebnisse einzugrenzen, sodass nur Daten für bestimmte Anwendungen, Bereitstellungstypen, Erfahrungsscores, mobile Benutzer, Gruppen oder Prisma Access-Standorte angezeigt werden. Zeigen Sie den individuellen Erfahrungsscore für die Anwendung sowie die Anzahl der Benutzer und Remote-Standorte an, die von bestehenden Leistungsproblemen betroffen sind.

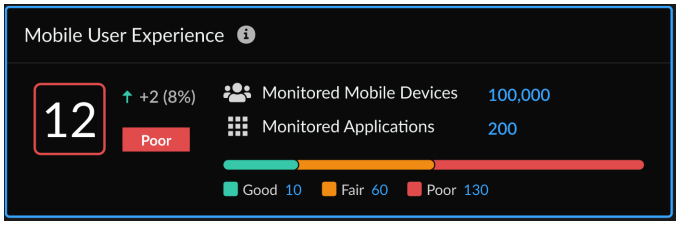
## Wie können Sie die Daten aus dem Dashboard nutzen?

Nachdem Sie die Anwendungen überprüft haben, die in Ihrem Netzwerk ausgeführt werden, und bestimmt haben, welche Anwendungen Sie überwachen möchten, können Sie einen Anwendungstest erstellen. Beachten Sie beim Erstellen von Anwendungstests, dass Sie zwar Anwendungstests erstellen können, die auf mehrere Benutzer oder Standorte ausgerichtet sind, die Anzahl der Tests jedoch auf der Anzahl der Anwendungstests basiert, die jeder einzelne Benutzer oder jedes ION-Gerät ausführt (wenn Sie z. B. einen Anwendungstest für Slack haben und ihn für 1000 Benutzer durchführen, wird dies als 1000 Tests auf Ihre Lizenz angerechnet).

# Dashboard „Anwendungserfahrung“: Karte zur Erfahrung mobiler Benutzer

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)* | ❑ Prisma Access-Lizenz<br>❑ ADEM Observability-Lizenz zum Anzeigen der Daten für **überwachte Anwendungen** |

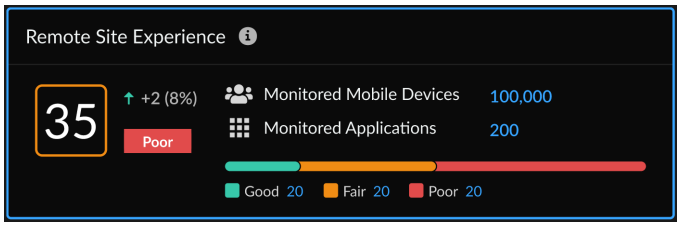
Dieses Widget zeigt den durchschnittlichen Anwendungssegmentscore für alle mobilen Benutzer aller überwachten Anwendungen. Außerdem wird Ihnen eine Aufschlüsselung der guten, angemessenen und schlechten Erfahrungen nach Anzahl der Benutzergeräte angezeigt. Sie können Details zu Benutzern mit angemessener oder schlechter Leistung anzeigen, um mit der Untersuchung zu beginnen. Der Erfahrungsscore auf dieser Karte gibt Ihnen einen Hinweis auf die allgemeine digitale Erfahrung des Benutzers. Für jede Anwendung, die für mobile Benutzer überwacht wird, berechnet ADEM einen Score basierend auf fünf kritischen Metriken: Anwendungsverfügbarkeit, DNS-Auflösungszeit, TCP-Verbindungszeit, SSL-Verbindungszeit und HTTP-Latenz. Wenn die Anwendung den Verfügbarkeitstest nicht besteht (Anwendung ist nicht verfügbar), beträgt der Erfahrungsscore 0. Erst wenn die Anwendung erreichbar ist, werden die verbleibenden vier Metriken berechnet. Jede der oben genannten Metriken (mit Ausnahme der Anwendungsverfügbarkeit) hat eine andere Gewichtung und verfügt über untere und obere Baseline-Schwellenwerte. Ihre kombinierte Gewichtung ergibt 100. Die Summe dieser einzelnen Metrikwerte ergibt den Anwendungserfahrungsscore für einen Benutzer. Der Erfahrungsscore eines Benutzers wird durch den Durchschnitt aller Testprobenergebnisse für jede Anwendung ermittelt.




# Dashboard „Anwendungserfahrung“: Karte zur Erfahrung an Remote-Standorten

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)* | ❑ Prisma Access-Lizenz<br>❑ ADEM Observability-Lizenz zum Anzeigen der Daten für **überwachte Anwendungen**<br>❑ Lizenz für Remote-Netzwerke |

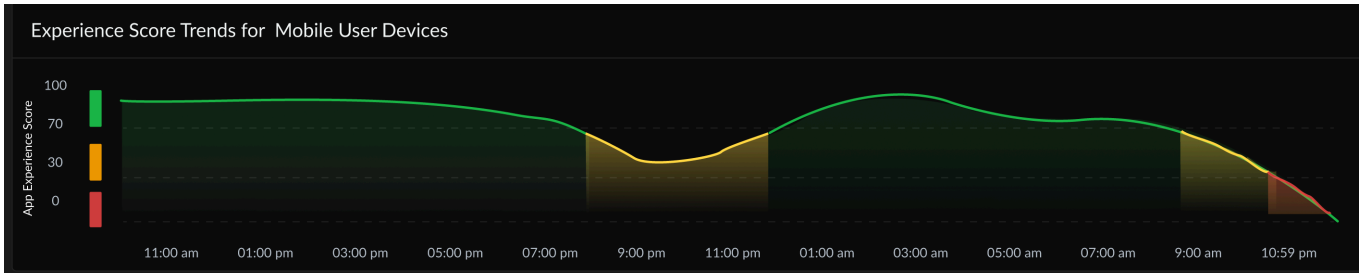
Der Erfahrungsscore für Remote-Standorte ist ein Durchschnittswert aller überwachten Anwendungen auf allen aktiven WAN-Pfaden. Es handelt sich um einen Durchschnitt aller Testprobenergebnisse, die von den einzelnen für diesen Remote-Standort überwachten Anwendungen gesammelt werden. Dies ist der Gesamterfahrungsscore (umschlossen von einem farbcodierten Quadrat) des Remote-Standorts oder der Zweigstelle. Er ergibt sich aus einem Durchschnitt der Erfahrungsscores aller Testproben, die auf aktiven Pfaden aller für diesen Standort überwachten Anwendungen gesammelt wurden. Obwohl der Erfahrungsscore jedes Sicherungspfads individuell berechnet wird und für jeden Remote-Standort und jede Anwendung verfügbar ist, wird dieser Erfahrungsscore für Sicherungspfade bei der Berechnung des Erfahrungsscores eines Remote-Standorts nicht berücksichtigt. Sie können die Leistung von Standorten mit angemessener oder schlechter Leistung detailliert anzeigen, indem Sie auf die Zahl neben „Angemessen“ oder „Schlecht“ klicken.




## Dashboard „Anwendungserfahrung“: Erfahrungsscoretrends

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)* | ❑ Prisma Access-Lizenz<br>❑ ADEM Observability-Lizenz zum Anzeigen der Daten für **überwachte Anwendungen** |

Dieses Widget zeigt ein Zeitreihendiagramm der durchschnittlichen Erfahrung aller mobilen Benutzer an. Der Erfahrungsscore wird in festgelegten Intervallen während des ausgewählten Zeitbereichs berechnet und angezeigt. Die Y-Achse ist basierend auf dem Scorebereich farbcodiert, um Ihnen die Qualität Ihres Erfahrungsscores anzuzeigen (Rot = schlecht, Gelb = angemessen und Grün = gut). Bewegen Sie den Mauszeiger über die Trendlinie, um den Erfahrungsscore zu dem Zeitpunkt anzuzeigen, an dem sich der Mauszeiger befindet.

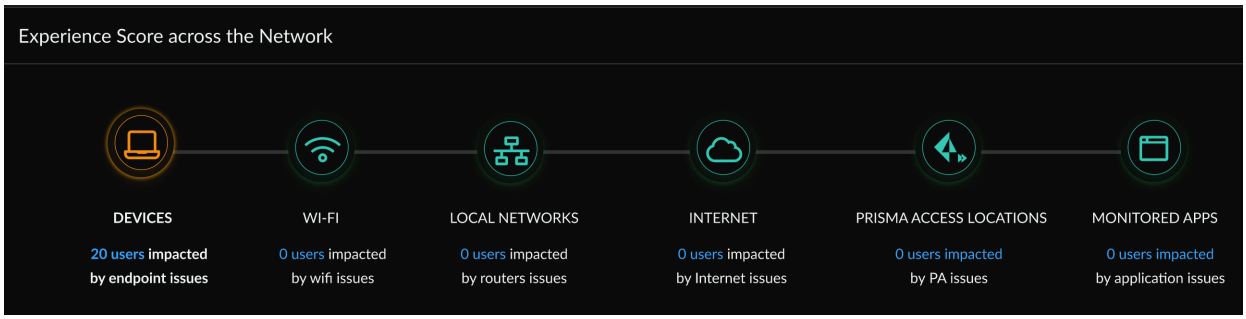


# Dashboard „Anwendungserfahrung“: Netzwerkübergreifender Erfahrungsscore

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)* | ❑ Prisma Access-Lizenz<br>❑ ADEM Observability-Lizenz zum Anzeigen der Daten für **überwachte Anwendungen** |

Identifizieren Sie das Netzwerksegment, das in Ihrer Organisation Probleme verursachen könnte – von den Endpunkten (für mobile Benutzer) oder Zweigstellen (Remote-Standorte) bis hin zu den Anwendungen. Sie können sehen, welches Netzwerksegment in Ihrer Organisation möglicherweise Probleme verursacht – von den Endpunkten und Prisma SD-WAN-Remote-Standorten bis hin zur Anwendung. Sie können sehen, welches Segment (beispielsweise der Ausfall eines Internetanbieters, eines Computerstandorts oder einer SaaS-Anwendung) die digitale Erfahrung in Ihrer Organisation beeinträchtigt, und auch die genaue Anzahl der Benutzer oder Standorte anzeigen, die davon betroffen sind. Die Symbole sind farbcodiert und basieren auf dem durchschnittlichen Segment-Zustandsscore aller mobilen Benutzer. Ein grünes Symbol steht für „Gut“ (Score >= 70), Gelb steht für „Angemessen“ (Score von 30–70) und Rot steht für „Schlecht“ (Score < 30).




**Geräte** – Gerätezustandsmetriken (CPU/Speicher/Festplattenspeicher/Festplattenwarteschlange/Akku)

**WLAN** – WLAN-Metriken (Signalqualität, Tx, Rx, SSID, BSSID, Kanal)

**Lokale Netzwerke** – Netzwerkleistungsmetriken (Latenz/Verlust/Jitter)

**Internet** – Netzwerkleistungsmetriken (Latenz/Verlust/Jitter); wenn ein Gerät nicht mit GlobalProtect, dem Internetsegment, verbunden ist, sind die Netzwerkleistungsmetriken dieselben wie beim für das Anwendungssegment ausgeführten TCP-PING-Test.

**Prisma Access-Standorte** – Netzwerkleistungsmetriken (Latenz/Verlust/Jitter); der Test für dieses Segment wird nicht ausgeführt, wenn das Gerät nicht mit GlobalProtect verbunden ist.

**Überprüfte Anwendungen** – Netzwerkleistungsmetriken (Latenz/Verlust/Jitter); Anwendungsleistungsmetriken (Verfügbarkeit, DNS-Suche, TCP-Verbindung, SSL-Verbindung, HTTP-Latenz, Zeit bis zum ersten Byte, Zeit bis zum letzten Byte, Datenübertragung)

# Dashboard „Anwendungserfahrung“: Globale Verteilung der Anwendungserfahrungsscores

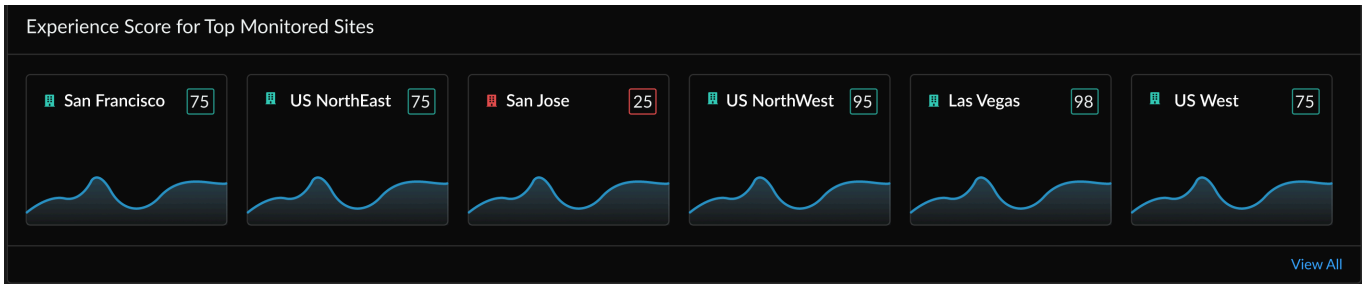
| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)* | ❑ Prisma Access-Lizenz<br>❑ ADEM Observability-Lizenz zum Anzeigen der Daten für **überwachte Anwendungen** |

Abhängig von der Karte, die Sie auswählen, zeigt Ihnen die Kartenansicht in diesem Widget die Erfahrung von Prisma Access-Standorten an, basierend auf der Gesamtzahl der überprüften mobilen Benutzer und Anwendungen oder der Gesamtzahl der Remote-Standorte und Anwendungen, die an einem bestimmten Prisma Access-Standort überwacht werden. Die Prisma Access-Standorte sind mit Kreisen markiert, die farbcodiert sind, um den Status der Anwendungssegmentscores aller überwachten mobilen Benutzer und Remote-Standorte anzuzeigen, die mit dem spezifischen, mit einem Kreis markierten Prisma Access-Standort verbunden sind. Bewegen Sie den Mauszeiger über einen Kreis, um die Erfahrungsscores für den Standort sowie die Gesamtzahl der überwachten mobilen Benutzergeräte oder Remote-Standorte und die Gesamtzahl der Anwendungen anzuzeigen, die für diesen Standort überwacht werden. Mehrere Orte, die geografisch sehr nahe beieinander liegen, werden durch einen Kreis mit einer Zahl darin dargestellt. Die Zahl gibt an, wie viele Standorte in diesem Gebiet gruppiert wurden. Um genau zu sehen, welche Standorte gruppiert wurden, zoomen Sie auf die Karte.

# Dashboard „Anwendungserfahrung“: Erfahrungsscore für überwachte Top-Standorte

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)* | ❑ Prisma Access-Lizenz<br>❑ ADEM Observability-Lizenz zum Anzeigen der Daten für **überwachte Anwendungen** |

Dieses Widget zeigt eine Karte pro Anwendung an und zeigt die Standorte mit den höchsten Scores an. Dieses Widget zeigt den Erfahrungsscoretrend der Remote-Standorte während des ausgewählten Zeitbereichs. Bewegen Sie den Mauszeiger über die Trendlinie, um den Erfahrungsscore für den jeweiligen Zeitpunkt anzuzeigen.

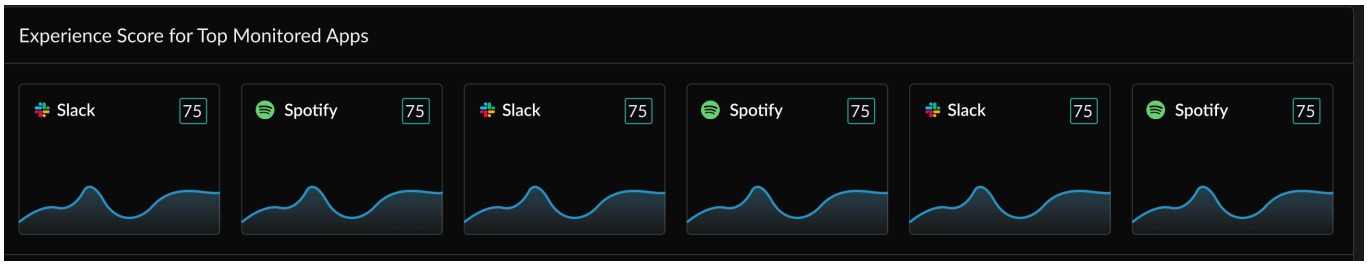



# Dashboard „Anwendungserfahrung“: Erfahrungsscore für Top überwachte Apps

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)* | ❑ Prisma Access-Lizenz<br>❑ ADEM Observability-Lizenz zum Anzeigen der Daten für **überwachte Anwendungen** |

Jede Anwendungskarte zeigt Ihnen die durchschnittliche Anwendungssegmentbewertung (die im Quadrat eingeschlossene Zahl) für alle überprüften mobilen Benutzer für diese bestimmte Anwendung am Remote-Standort. Der Erfahrungsscore wird als Durchschnitt der Anwendungserfahrungsscores aller überprüften Anwendungen berechnet. Der Erfahrungsscore stellt die End-to-End-Erfahrung für die aktiven Pfade der Anwendung dar. Es handelt sich um den Durchschnitt aller Testproben, die ausschließlich auf den aktiven Pfaden für diese spezielle Anwendung gesammelt wurden. Die Trendlinie zeigt Ihnen den Durchschnitt aller 5-minütigen APM-Datenproben für den ausgewählten Zeitrahmen.

Sie können sehen, wie viele Anwendungen Sie überwachen und wie viele aktive Pfade und Sicherungspfade überwacht werden. Auf jeder Anwendungskarte ist die Anzahl der betroffenen Pfade angegeben. Klicken Sie auf eine Anwendungskarte, um die Metriken für diese spezifische Anwendung anzuzeigen.



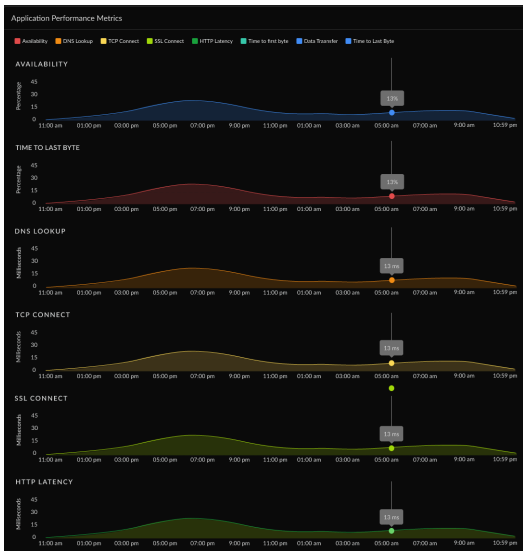

 

# Dashboard „Anwendungserfahrung“: Anwendungsleistungsmetriken

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)* | ❑ Prisma Access-Lizenz<br>❑ ADEM Observability-Lizenz zum Anzeigen der Daten für **überwachte Anwendungen** |

Autonomous DEM verwendet TCP-Ping und Curl, um die End-to-End-Anwendungsleistung zu bestimmen.

| Metrik | Beschreibung |
|---|---|
| Verfügbarkeit | Anwendungsverfügbarkeit (in Prozent) während des **Zeitbereichs**. |
| DNS-Lookup | DNS-Auflösungszeit. |
| TCP-Verbindung | Zeit, die zum Herstellen einer TCP-Verbindung benötigt wird. |
| SSL-Verbindung | Zeit, die zum Herstellen einer SSL-Verbindung benötigt wird. |
| HTTP-Latenz | Zeit, die zum Herstellen einer HTTP-Verbindung benötigt wird. |
| Zeit bis zum ersten Byte | Die Summe aus DNS-Lookup, TCP-Verbindung, SSL-Verbindung und HTTP-Latenz ergibt die Zeit bis zum ersten Byte. |
| Datenübertragung | Gesamtzeit, die für die Übertragung aller Daten benötigt wurde. |
| Zeit bis zum letzten Byte | Zeit bis zum ersten Byte + Datenübertragungsdauer. |



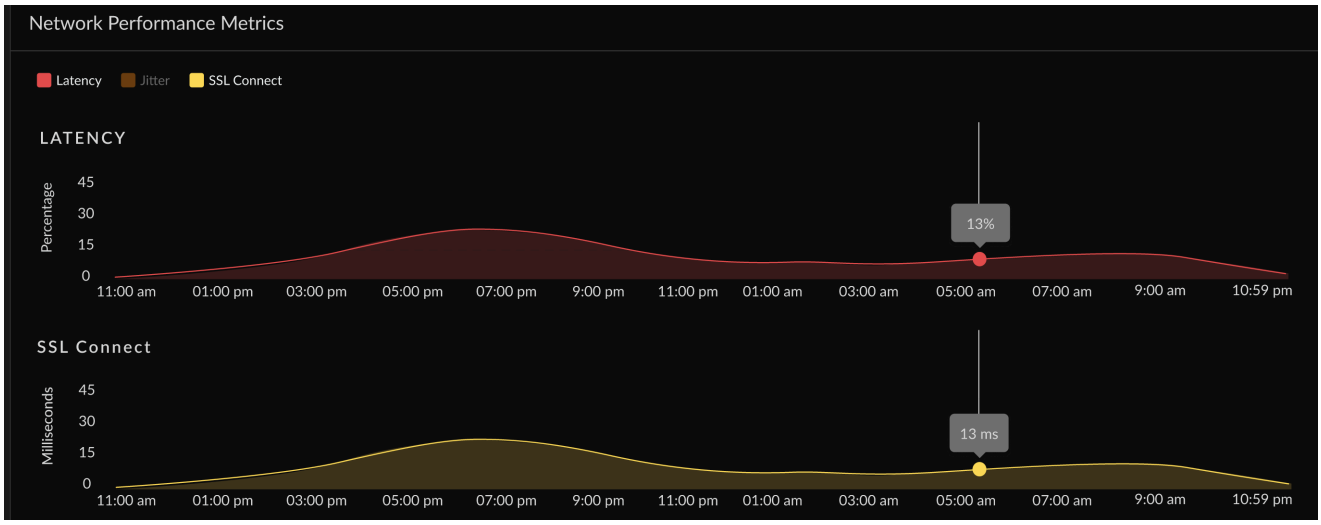

# Dashboard „Anwendungserfahrung“: Netzwerkleistungsmetriken

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)* | ❑ Prisma Access-Lizenz<br>❑ ADEM Observability-Lizenz zum Anzeigen der Daten für **überwachte Anwendungen** |

ADEM verwendet ICMP-Pings, um die Netzwerkleistung in jedem Segment zu bestimmen.

| Metrik | Beschreibung |
|---|---|
| Verfügbarkeit | Netzwerkverfügbarkeitsmetriken während des **Zeitbereichs**. |
| Netzwerklatenz | Zeit, die zum Übertragen der Daten über das Netzwerk benötigt wird. |
| Paketverlust | Verlust von Paketen während der Datenübertragung. |
| Jitter | Änderung der Latenz während des **Zeitbereichs**. |

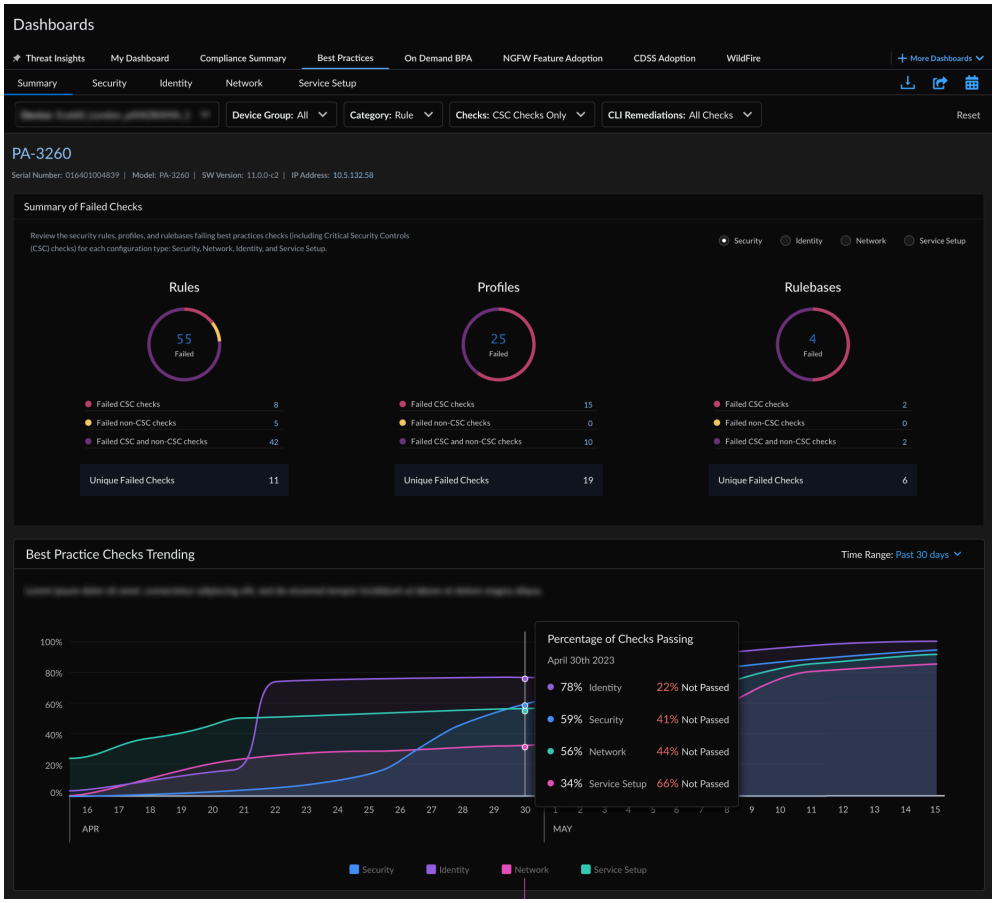


# Dashboard: Best Practices

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>☐ Prisma Access<br>☐ AIOps for NGFW Premium<br>☐ Strata Cloud Manager Essentials<br>☐ Strata Cloud Manager Pro<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

- Klicken Sie auf **Strata Cloud Manager** > **Dashboards** > **Mehr Dashboards** > **Best Practices**, um loszulegen.



# Was sehen Sie in diesem Dashboard?

*Das Dashboard zeigt aggregierte Daten pro Prisma Access und NGFW/Panorama, die Ihrem Mandanten zugeordnet sind.*

Das Best-Practice-Dashboard misst Ihren Sicherheitsstatus anhand der Best-Practice-Richtlinien von Palo Alto Networks. Vor allem umfasst die Best-Practice-Bewertung Prüfungen für die Critical Security Controls (CSC) des Center for Internet Security. CSC-Prüfungen werden getrennt von anderen Best-Practice-Überprüfungen durchgeführt, sodass Sie Updates, die Sie an die CSC-Compliance heranführen, einfach auswählen und priorisieren können.

Das Best-Practice-Dashboard ist in fünf Abschnitte unterteilt:

- **Zusammenfassung**

  Bietet Ihnen einen umfassenden Überblick über alle fehlgeschlagenen Überprüfungen für ein Gerät über die Konfigurationstypen (Sicherheit, Netzwerk, Identität und Diensteinrichtung), historische Trenddiagramme für BPA-Überprüfungen und die Bewertung Ihrer Best-Practice-Akzeptanzraten für wichtige Funktionsbereiche.
- **Sicherheit**

  Zeigt die Regeln, Regelsätze oder Profile an, bei denen Best Practice- und CSC-Prüfungen für das ausgewählte Gerät und den ausgewählten Standort fehlschlagen. Sofern verfügbar, können Sie mit CLI-Korrekturen Probleme mit Ihren Richtlinienregeln beheben. CLI-Korrekturen werden mithilfe von TSF-Daten generiert, die Sie beim Erstellen eines On-Demand-BPA hochladen.

  - **Regelsätze**

    Betrachtet, wie Ihre Richtlinie organisiert ist und ob Konfigurationseinstellungen, die für viele Regeln gelten, mit Best Practices (einschließlich CSC-Prüfungen) übereinstimmen.
  - **Regeln**

    Zeigt Ihnen die Regeln an, die Best Practice und CSC-Überprüfungen nicht bestanden haben. Erfahren Sie, wo Sie schnell Maßnahmen ergreifen können, um fehlgeschlagene Prüfungen zu beheben. Regeln werden nach Anzahl der Sitzungen sortiert, sodass Sie damit beginnen können, die Regeln zu überprüfen und zu aktualisieren, die sich auf den größten Teil des Datenverkehrs auswirken.
  - **Profile**

    Zeigt Ihnen, wie sich Ihre Profile mit Best Practices messen, einschließlich CSC-Überprüfungen. Profile führen eine erweiterte Überprüfung auf Datenverkehr durch, der einer Sicherheits- oder Entschlüsselungsregel entspricht.
- **Identität**

  Zeigt an, ob die Einstellungen für die Authentifizierungsdurchsetzung (Authentifizierungsregel, Authentifizierungsprofil und Authentifizierungsportal) für ein Gerät den Best Practices entsprechen und mit den CSC-Prüfungen konform sind.
- **Netzwerk**

  Überprüft, ob die Anwendungsüberschreibungsregeln und Netzwerkeinstellungen mit Best Practices und CSC-Prüfungen übereinstimmen.

- **Diensteinrichtung**

  Sehen Sie, wie die Abonnements, die Sie auf Ihren Geräten aktiviert haben, mit den Best Practices und CSC-Prüfungen übereinstimmen. Sie können hier die WildFire-Einrichtung sowie die Konfigurationen von GlobalProtect Portal und GlobalProtect Gateway überprüfen und die fehlgeschlagenen Prüfungen korrigieren.

Dieses Dashboard unterstützt Berichte. Diese Symbole  oben rechts im Dashboard weisen darauf hin, dass Berichte für dieses Dashboard unterstützt werden. Sie können Berichte, die die in diesem Dashboard angezeigten Daten behandeln, herunterladen, teilen und planen.

## Wie können Sie die Daten aus dem Dashboard nutzen?

Während Best-Practice-Leitfäden Ihnen helfen sollen, Ihren Sicherheitsstatus zu stärken, können Sie die Ergebnisse dieses Berichts auch dabei unterstützen, Bereiche zu bestimmen, in denen Sie Änderungen vornehmen können, um Ihre Umgebung effektiver zu verwalten.

# Dashboard: Zusammenfassung der Konformität

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | ❑ AIOps for NGFW Premium oder Strata Cloud Manager Pro<br><br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Sie können den Änderungsverlauf der Sicherheitsüberprüfungen anzeigen, die vor bis zu 12 Monaten vorgenommen wurden, zusammengefasst nach den CIS- (Center for Internet Security) und NIST-Frameworks (National Institute of Standards and Technology). Für jedes Framework wird eine Liste mit Kontrollen sowie der Prozentsatz der aktuellen und durchschnittlichen Konformitätsrate, die Gesamtzahl der Best-Practice-Überprüfungen sowie die Anzahl der fehlgeschlagenen Prüfungen für jede Kontrolle angezeigt.

Interagieren Sie mit dem Diagramm und der Liste, um den Zusammenhang zwischen Kontrollen und ihren Verlaufsstatistiken zu sehen. Zeigen Sie Details zu einzelnen Kontrollen und den zugehörigen Prüfungen an, und wählen Sie eine Best-Practice-Überprüfung aus, um die Firewallkonfiguration anzuzeigen, bei der die Prüfung fehlschlägt.

Das **Critical Security Controls-Framework von CIS** umfasst eine priorisierte Reihe von Handlungsempfehlungen und Best Practices, die dazu beitragen, Unternehmen und ihre Daten vor bekannten Cyberangriffsvektoren zu schützen. Sie können Prüfzusammenfassungen für 11 der 16 Basis- und grundlegenden CIS-Kontrollen anzeigen:

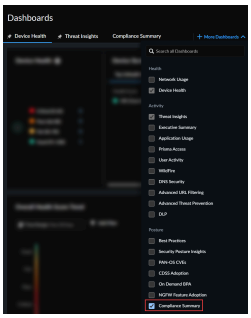
- CSC 3: Kontinuierliches Sicherheitsrisikomanagement
- CSC 4: Kontrollierte Nutzung von Administratorrechten
- CSC 6: Pflege, Überwachung und Analyse von Auditierungslogs
- CSC 7: E-Mail- und Webbrowser-Schutz
- CSC 8: Malware-Abwehr
- CSC 9: Beschränkung und Kontrolle von Netzwerkports, Protokollen und Diensten
- CSC 11: Sichere Konfiguration für Netzwerkgeräte wie Firewalls, Router und Switches
- CSC 12: Grenzverteidigung
- CSC 13: Datenschutz
- CSC 14: Kontrollierter Zugriff basierend auf dem Need-to-Know-Prinzip
- CSC 16: Kontoüberwachung und #kontrolle

Das **NIST Cybersecurity Framework SP 800-53 Controls** bietet Bundesbehörden und anderen Organisationen Leitlinien zur Implementierung und Aufrechterhaltung von Sicherheits- und Datenschutzkontrollen für ihre Informationssysteme. Sie können Prüfzusammenfassungen für acht Familien von NIST-Kontrollen anzeigen:

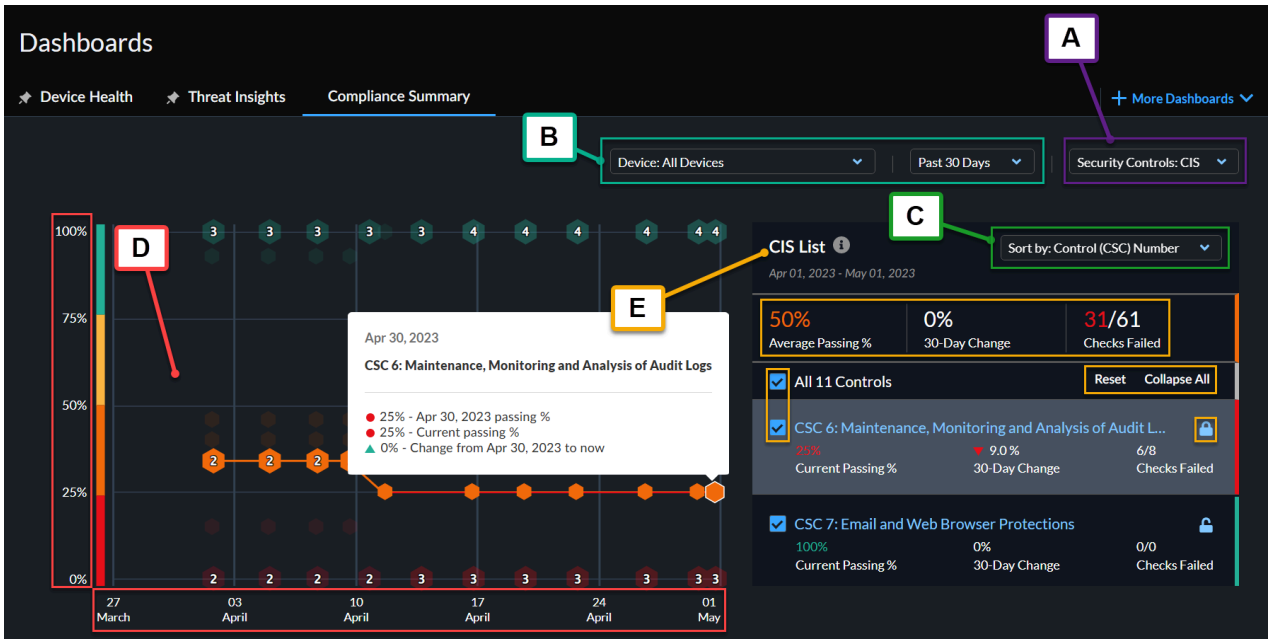
- SC: Zugriffssteuerung
- AU: Auditing und Rechenschaftspflicht
- CM: Verwaltung der Konfiguration
- CP: Notfallplanung
- IA: Identifizierung und Authentifizierung
- RA: Risikobewertung
- SC: System- und Kommunikationsschutz
- SI: System- und Informationsintegrität

Um zum Dashboard „Zusammenfassung der Konformität“ zu gelangen, gehen Sie zu **Dashboards** und wählen Sie dann die Registerkarte **Zusammenfassung der Konformität** aus.

*Wenn **Zusammenfassung der Konformität** nicht unter den Registerkartenoption angezeigt wird, wählen Sie **Mehr Dashboards** aus und aktivieren Sie dann das Kontrollkästchen bei **Zusammenfassung der Konformität** unter den Optionen für **Status**.*



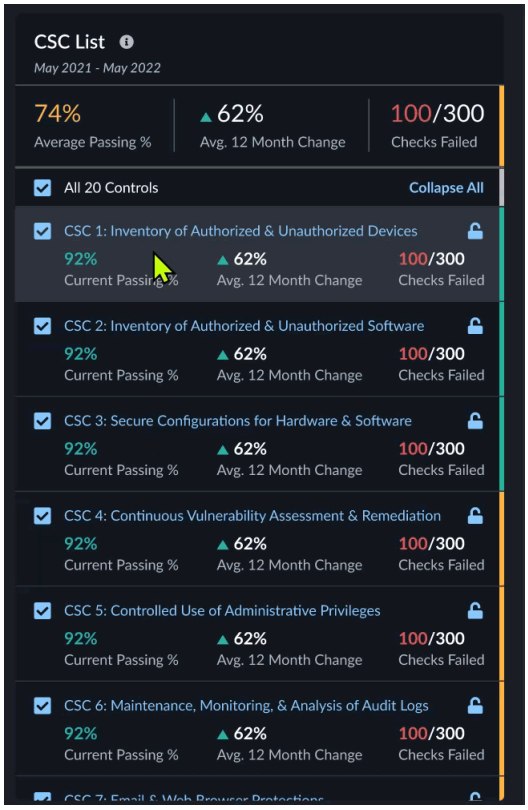



| | |
|---|---|
| **A) Auswahl kritischer Sicherheitskontrollen** | CIS- oder NIST-Kontrollen auswählen |
| **B) Filtern nach** | • Gerät<br>• Zeitrahmen<br>  • Vergangene 7 Tage<br>  • Letzte 30 Tage<br>  • Vergangene 90 Tage<br>  • Letzte 6 Monate<br>  • Letzte 12 Monate |
| **C) Sortieren nach** | • CSC-Kontrollnummer<br>• % aktuell bestanden<br>• % Änderung<br>• Anzahl fehlgeschlagener Überprüfungen |
| **D) Liniendiagramm** | • % bestanden – zeigt den Prozentsatz zum Bestehen eines bestimmten Prüfungstyps an.<br>• Zeitleiste – zeigt an, wann der Prozentsatz für einen bestimmten Prüfungstyp gemessen wurde. |

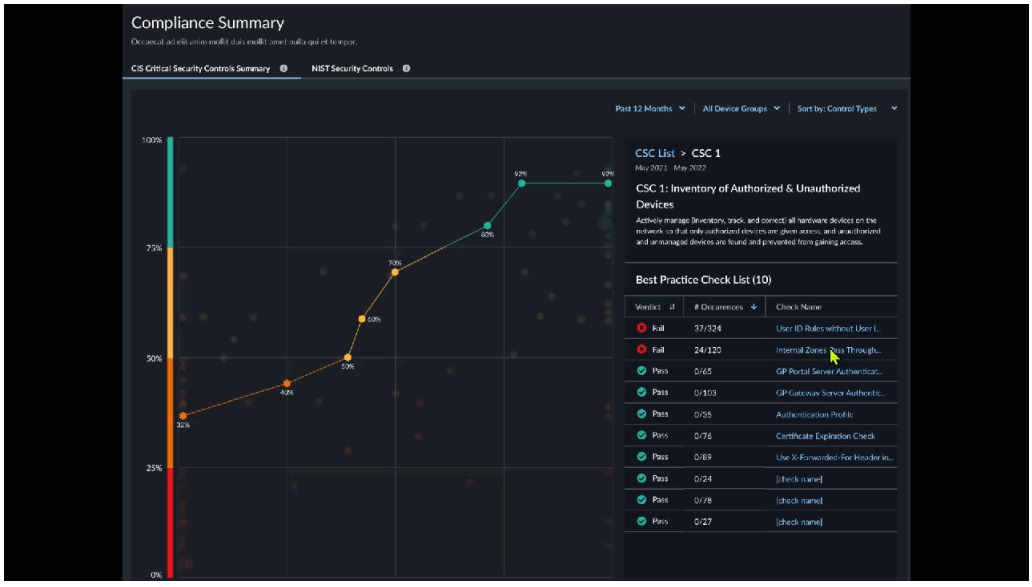
| | |
|---|---|
| **E) Checkliste** | • Statistiken<br>  • Durchschnittliche % bestanden – zeigt den durchschnittlichen Prozentsatz bestandener Prüfungen an.<br>  • 12-Monats-Änderung – zeigt Änderungen über einen Zeitraum von 12 Monaten an.<br>  • Fehlgeschlagene Überprüfungen – zeigt die Anzahl der fehlgeschlagenen Prüfungen an.<br>• Ausgewählte Kontrollen – Ein Häkchen sorgt dafür, dass die jeweilige Kontrolle auf dem Liniendiagramm angezeigt wird.<br>• Zurücksetzen – entfernt alle Sperren.<br>• Alle ein-/ausblenden – zeigt Statistiken in der Liste bzw. blendet sie aus.<br>• Liniendiagramm sperren – behält gesperrte Prüfungen im Liniendiagramm im Blick. |

- *Wählen Sie eine Kontrolle in der Liste aus, um die darin enthaltenen Best-Practice-Überprüfungen anzuzeigen.*




- *Wählen Sie eine Best-Practice-Überprüfung aus, um die Firewallkonfiguration anzuzeigen, bei der die Prüfung fehlschlägt.*

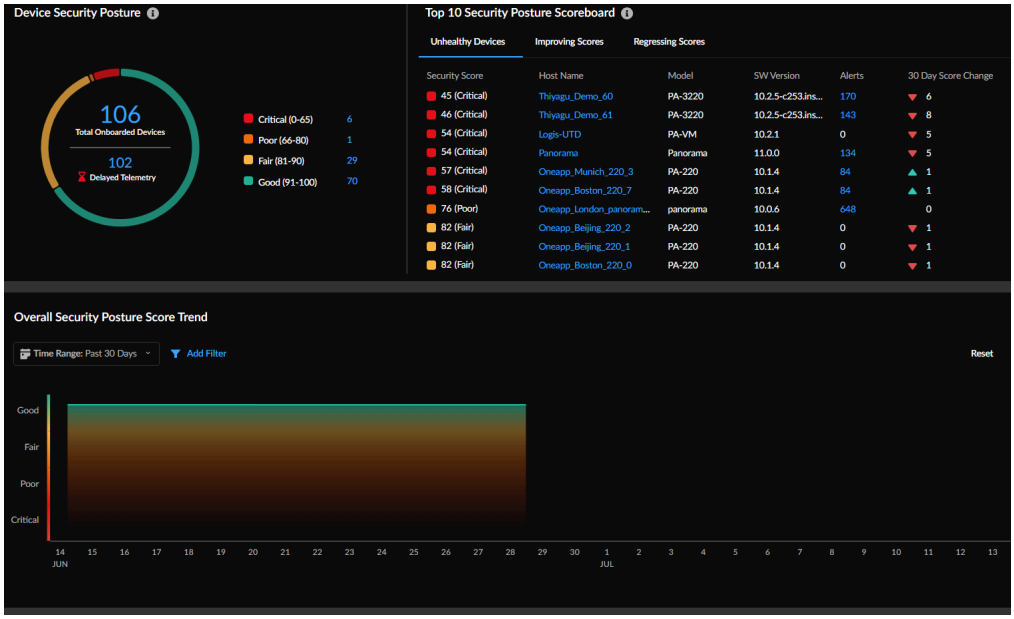


# Dashboard: Einblicke in den Sicherheitsstatus

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | ☐ Strata Cloud Manager Essentials<br>☐ AIOps for NGFW Premium oder Strata Cloud Manager Pro<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

- Klicken Sie auf **Strata Cloud Manager** > **Dashboards** > **Mehr Dashboards** > **Einblicke in den Sicherheitsstatus**, um zu beginnen.




## Was sehen Sie in diesem Dashboard?

*Das Dashboard zeigt aggregierte Daten für alle Firewalls, die Ihrem Mandanten zugeordnet sind, und sendet auch Telemetriedaten.*

Verschaffen Sie sich Einblick in den Sicherheitsstatus und -trend Ihrer Bereitstellung basierend auf dem Sicherheitsstatus der eingebundenen NGFW-Geräte. Der Schweregrad der Sicherheitsbewertung (0–100) und die entsprechende Sicherheitsstufe (gut, angemessen, schlecht, kritisch) bestimmen den Sicherheitsstatus eines Geräts. Der Sicherheitswert wird anhand von Priorität, Anzahl, Art und Status der offenen Benachrichtigungen berechnet.

# Wie können Sie die Daten aus dem Dashboard nutzen?

Verwenden Sie dieses Dashboard für Folgendes:

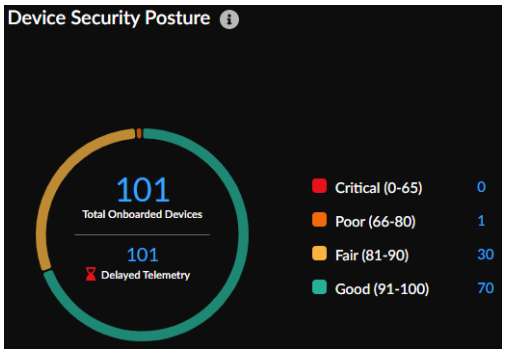
- Ermitteln Sie den Trend von Problemen, die den Sicherheitsstatus Ihrer Bereitstellung beeinflussen.
- Untersuchen Sie die Sicherheitsverbesserungen, die Sie in Ihrer Bereitstellung vorgenommen haben, indem Sie sich die vergangenen Sicherheitsbewertungsdaten ansehen.
- Grenzen Sie Geräte ein, bei denen die Möglichkeit besteht, den Sicherheitsstatus zu verbessern, und priorisieren Sie die Behebung dieser Probleme.

*Die Berichtsfunktion (Bericht herunterladen, freigeben und planen) wird für dieses Dashboard nicht unterstützt.*

# Dashboard „Einblicke in den Sicherheitsstatus“: Sicherheitsstatus des Geräts

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | ☐ Strata Cloud Manager Essentials<br>☐ AIOps for NGFW Premium oder Strata Cloud Manager Pro<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

- Klicken Sie auf **Strata Cloud Manager** > **Dashboards** > **Mehr Dashboards** > **Einblicke in den Sicherheitsstatus**, um das Dashboard anzuzeigen.




Das Dashboard-Widget zeigt Folgendes:

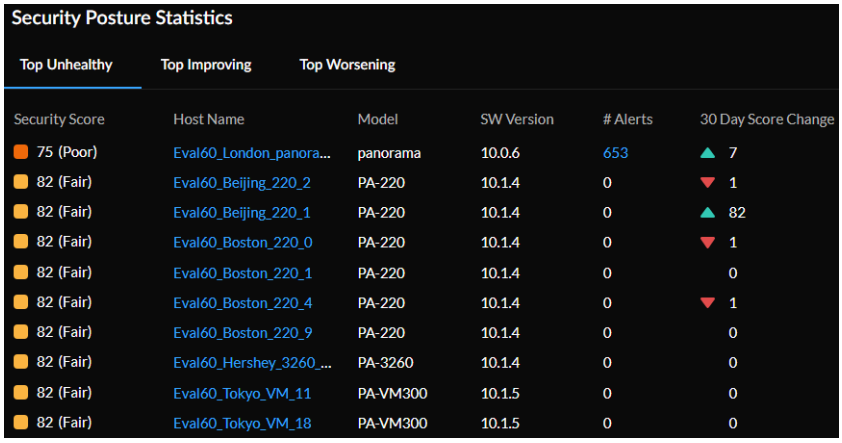
- Die Gesamtzahl der eingebundenen NGFWs.
- Die Anzahl der Geräte, die seit über 12 Stunden keine Telemetriedaten gesendet haben.
- Die Priorität des Sicherheitswerts für die eingebundenen Geräte in Ihrer Bereitstellung. Klicken Sie auf die verlinkte Zahl, um Gerätedetails und Sicherheitsstatistiken anzuzeigen.

# Dashboard „Einblicke in den Sicherheitsstatus“: Statistiken zum Sicherheitsstatus

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | ❑ Strata Cloud Manager Essentials<br>❑ AIOps for NGFW Premium oder Strata Cloud Manager Pro<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

- Klicken Sie auf **Strata Cloud Manager** > **Dashboards** > **Mehr Dashboards** > **Einblicke in den Sicherheitsstatus**, um das Dashboard anzuzeigen.




**Top – schlechter Zustand**

Dies sind die zehn Geräte, die sich am stärksten auf den Sicherheitsstatus Ihrer Bereitstellung auswirken. Gehen Sie ins Detail, um die Geräteinformationen und Benachrichtigungen zu dem Gerät anzuzeigen. Führen Sie die Schritte zur Behebung der kritischen Gerätebenachrichtigungen durch, um den Sicherheitsstatus zu verbessern.

**Top – Verbesserung**

Zeigen Sie die Top-10-Geräte mit verbesserten Sicherheitswerten in einem 30-Tages-Zeitraum an – verglichen mit den aktuellen Sicherheitswerten der Geräte.

**Top – Verschlechterung**

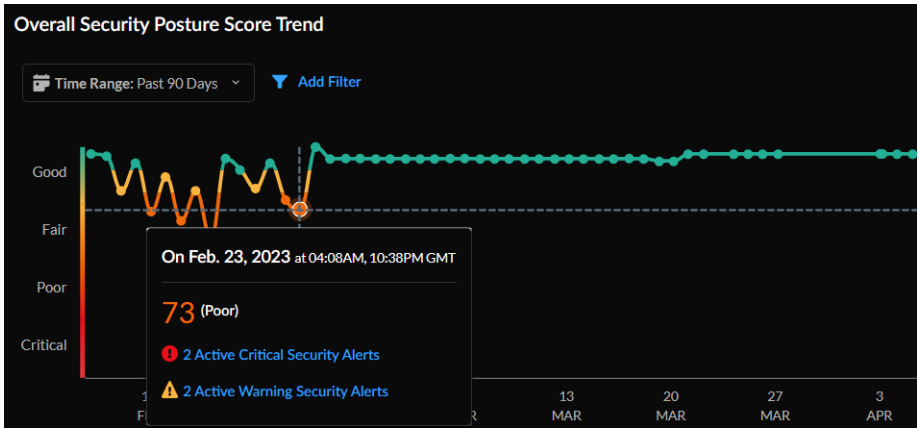
Dies sind die Geräte mit verschlechterten Sicherheitswerten im Vergleich zu den aktuellen Sicherheitswerten der Geräte. Prüfen Sie die Benachrichtigungen auf diesen Geräten und setzen Sie Prioritäten, um sie zu beheben.

# Dashboard „Einblicke in den Sicherheitsstatus“: Scoretrend

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | ❑ Strata Cloud Manager Essentials<br>❑ AIOps for NGFW Premium oder Strata Cloud Manager Pro<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

- Klicken Sie auf **Strata Cloud Manager** > **Dashboards** > **Mehr Dashboards** > **Einblicke in den Sicherheitsstatus**, um das Dashboard anzuzeigen.

Das Diagramm zeigt den Trend zum Sicherheitsstatus Ihrer Bereitstellung für den ausgewählten Zeitraum. Bewegen Sie den Mauszeiger über den Auslösepunkt, um die Geräte und aktiven Benachrichtigungen anzuzeigen, die den Trend zum Sicherheitsstatus beeinflussen. Sie können Trends für ein oder mehrere Geräte anzeigen, die nach Hostname, Modell oder Softwareversion gefiltert werden.

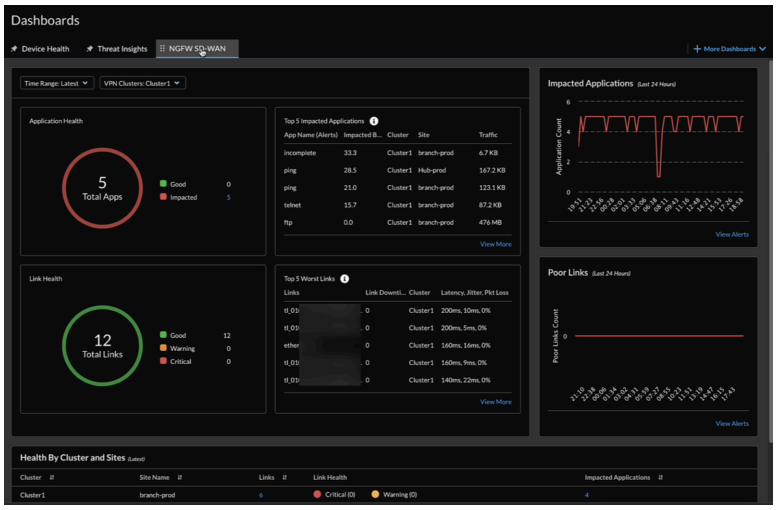


# Dashboard: NGFW SD-WAN

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | ☐ AIOps for NGFW Premium oder Strata Cloud Manager Pro<br><br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

- Klicken Sie auf **Dashboards > Mehr Dashboards > NGFW SD-WAN**, um zu beginnen.




Um dieses Dashboard zu nutzen, können Sie in Strata Cloud Manager ein softwaredefiniertes Wide Area Network (SD-WAN) für Ihre Palo Alto Networks-NGFWs einrichten.

## Was sehen Sie in diesem Dashboard?

Das **NGFW SD-WAN**-Dashboard zeigt Ihnen die Leistungsmetriken für Verbindungen und Anwendungsverkehr für Cloud-verwaltete Firewalls mit SD-WAN.

## Wie können Sie die Daten aus dem Dashboard nutzen?

Dieses Dashboard hilft Ihnen bei Folgendem:

- Einblick in die Leistungsmesswerte von Anwendungen und Verbindungen in Ihren VPN-Clustern, um Probleme anhand von Übersichtsinformationen aller VPN-Cluster zu beheben.
- Detaillierte Untersuchungen, um die Probleme auf die betroffenen Standorte, Anwendungen und Verbindungen einzugrenzen.
- Auslösen aussagekräftiger Benachrichtigungen zur Untersuchung und Behebung fehlerhafter Verbindungen und Anwendungen. Mit ML-gestützter Anomalieerkennung, Normalitätsband

und Prognosen basieren die aussagekräftigen Benachrichtigungen auf datengestützten Schwellenwerten. Darüber hinaus erhalten Sie Einblicke in Trends.

Hier ist ein Video, das zeigt, wie Sie das NGFW SD-WAN-Dashboard überwachen.

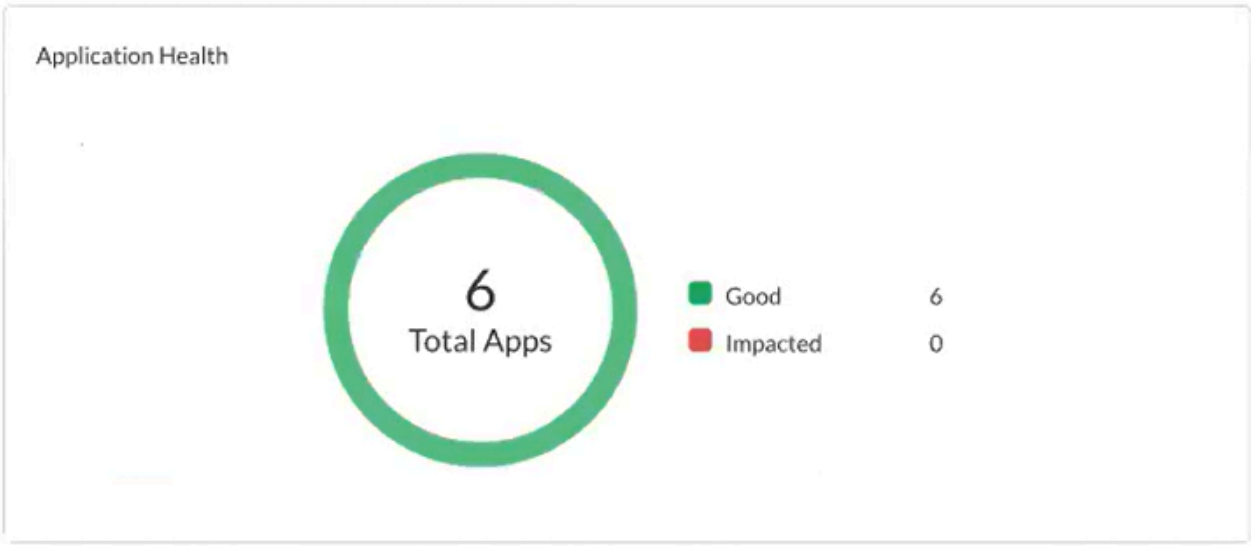
## NGFW SD-WAN Dashboard: Anwendungszustand

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | ❑ AIOps for NGFW Premium oder Strata Cloud Manager Pro<br><br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Das Dashboard zeigt Folgendes:

- Die Gesamtzahl der Anwendungen für die ausgewählte Zeitdauer und den VPN-Cluster.
- Die Anzahl der betroffenen Anwendungen, d. h. eine oder mehrere Anwendungen im VPN-Cluster, für die keiner der Pfade eine Jitter-, Latenz- oder Paketverlustleistung aufweist, die die angegebenen Schwellenwerte im Pfadqualitätsprofil in der Liste der Pfade erfüllt, aus denen die Firewall auswählen kann.
- Die Anzahl der Anwendungen, deren Zustand gut ist, d. h. Anwendungen im VPN-Cluster, bei denen keine Probleme mit der Jitter-, Latenz- oder Paketverlustleistung auftreten.

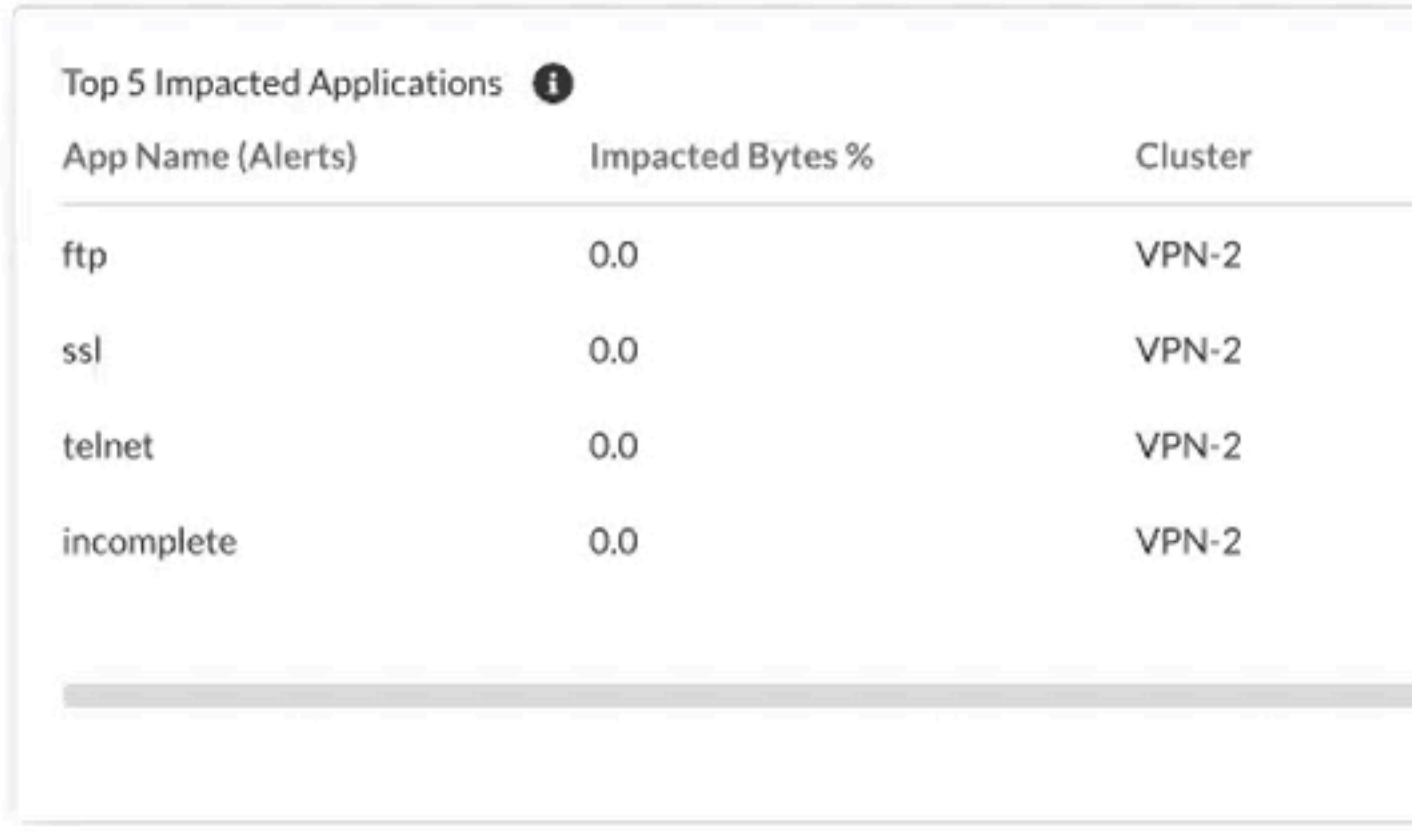
 




## NGFW SD-WAN Dashboard: Am stärksten betroffene Anwendungen

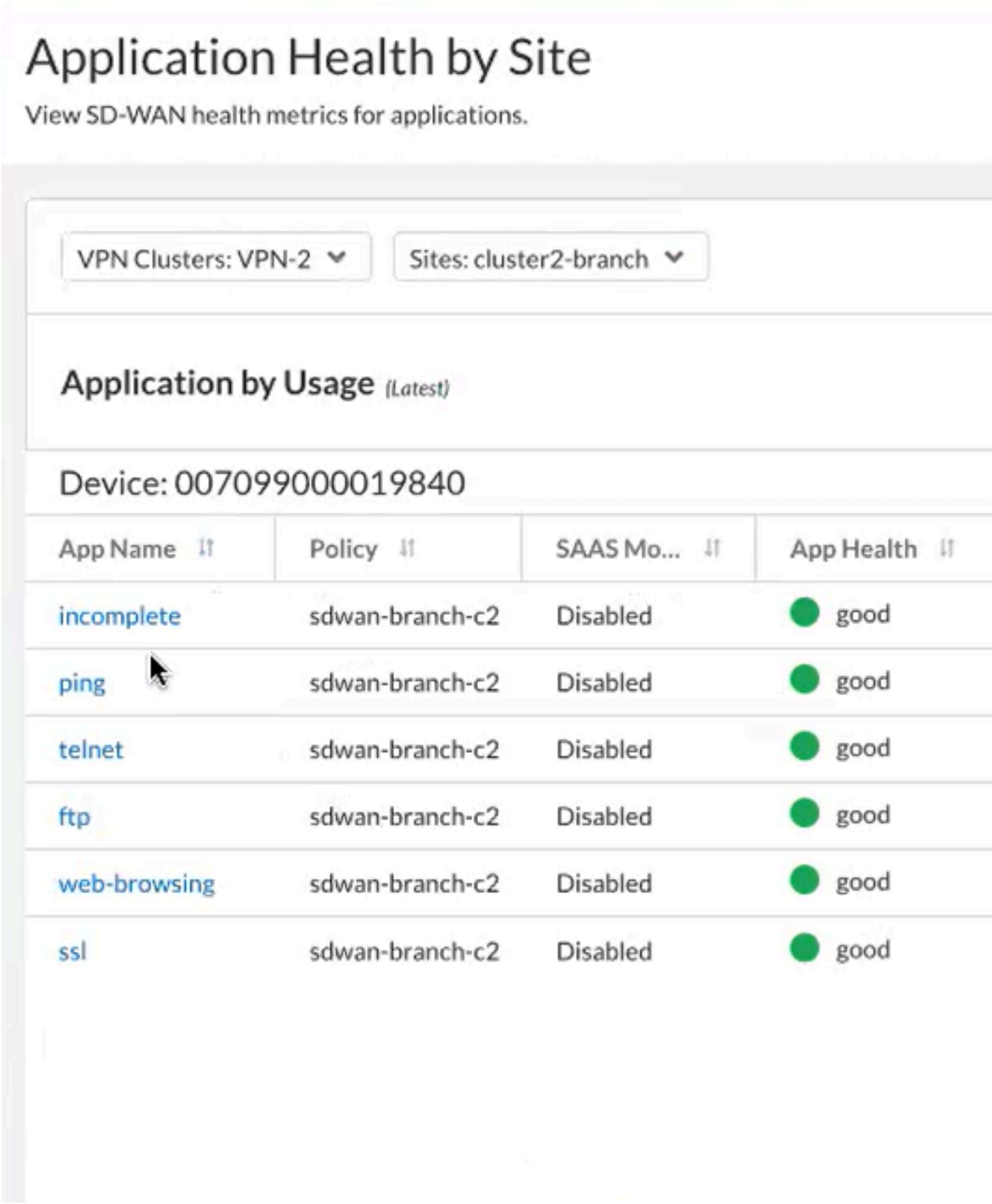
| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | ☐ AIOps for NGFW Premium oder Strata Cloud Manager Pro<br><br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Für die ausgewählte Zeitdauer und den ausgewählten VPN-Cluster zeigt Strata Cloud Manager Ihre fünf am stärksten betroffenen Anwendungen auf Grundlage ihres berechneten Prozentsatzes des betroffenen Datenverkehrs an den Gesamtbytes an. Ein höherer berechneter Prozentsatz weist auf eine größere Auswirkung auf die Anwendung hin.




Klicken Sie auf **Mehr anzeigen**, um alle betroffenen Anwendungen zu überprüfen.

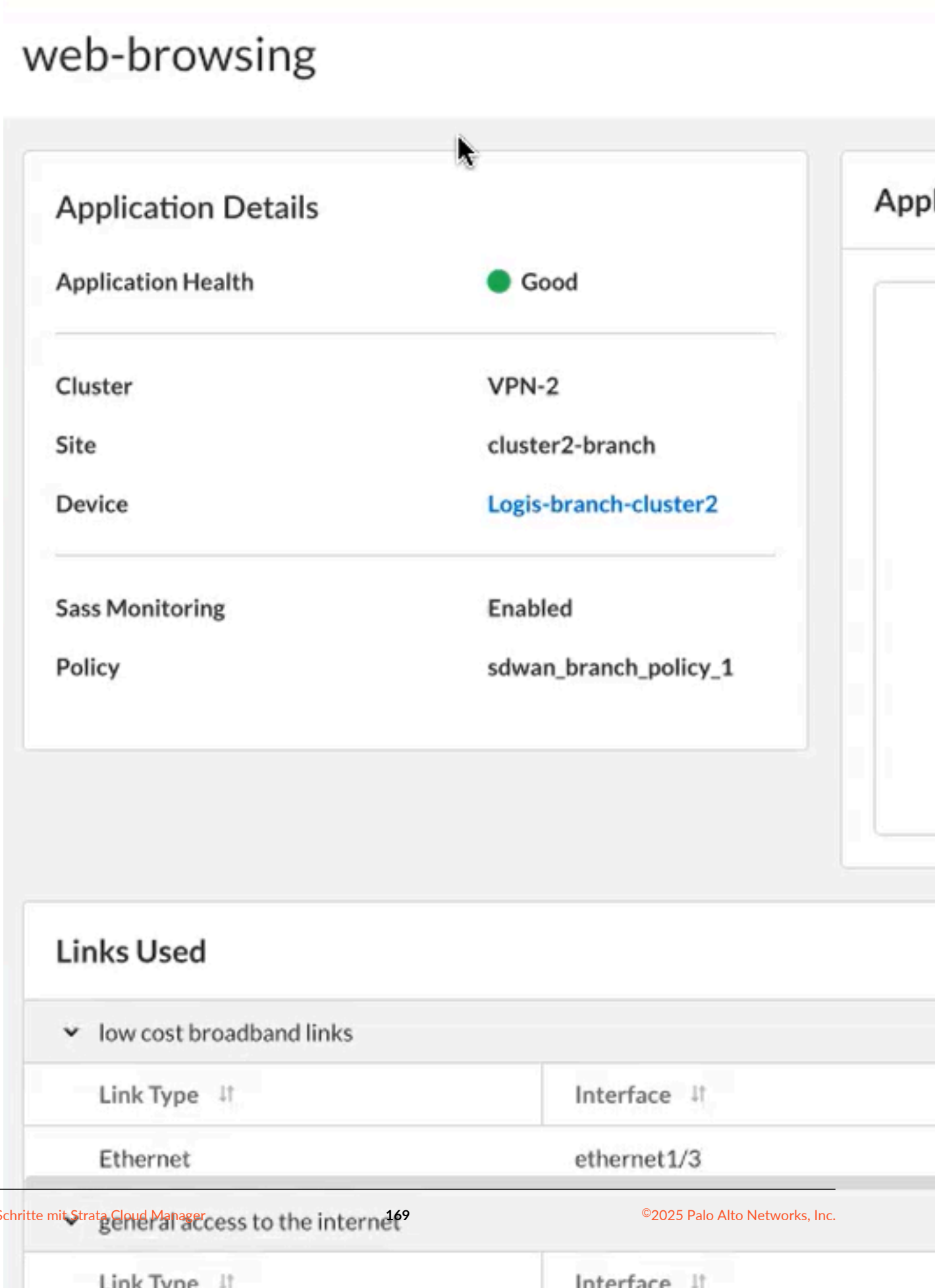
 



Klicken Sie auf eine Anwendung, um deren Details anzuzeigen, einschließlich des Datenverkehrs und der verwendeten Verbindung. Sie können auch auf eine verwendete Verbindung klicken, um ihre Details anzuzeigen.



# NGFW SD-WAN Dashboard: Betroffene Anwendungen

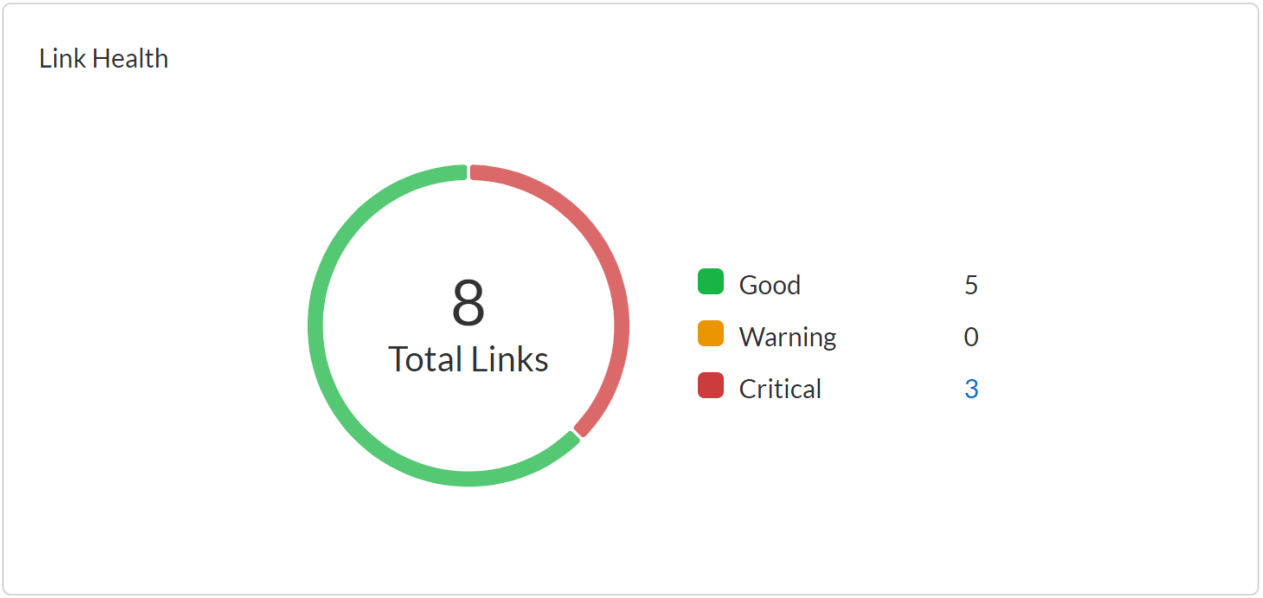
| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | ☐ AIOps for NGFW Premium oder Strata Cloud Manager Pro<br><br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

- Das Diagramm zeigt einen Trend der betroffenen Anwendungen in den letzten 24 Stunden. Bewegen Sie den Mauszeiger über die Trendlinie, um die betroffenen Anwendungen zu einem bestimmten Zeitpunkt anzuzeigen.
- Klicken Sie auf **Benachrichtigungen anzeigen**, um die zugehörigen Benachrichtigungen anzuzeigen, die aufgrund der betroffenen Anwendungen ausgelöst werden.

# NGFW SD-WAN Dashboard: Verbindungszustand

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | ☐ AIOps for NGFW Premium oder Strata Cloud Manager Pro<br><br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

- Die Gesamtzahl der Verbindungen für die ausgewählte Zeitdauer und den VPN-Cluster.
- Die Anzahl der Verbindungen, die als „Kritisch“, „Warnung“ und „Gut“ klassifiziert sind.
- Klicken Sie auf die verlinkte Zahl für **Kritisch**, um die aufgrund der SD-WAN-Verbindungsleistung ausgelösten Benachrichtigungen anzuzeigen.

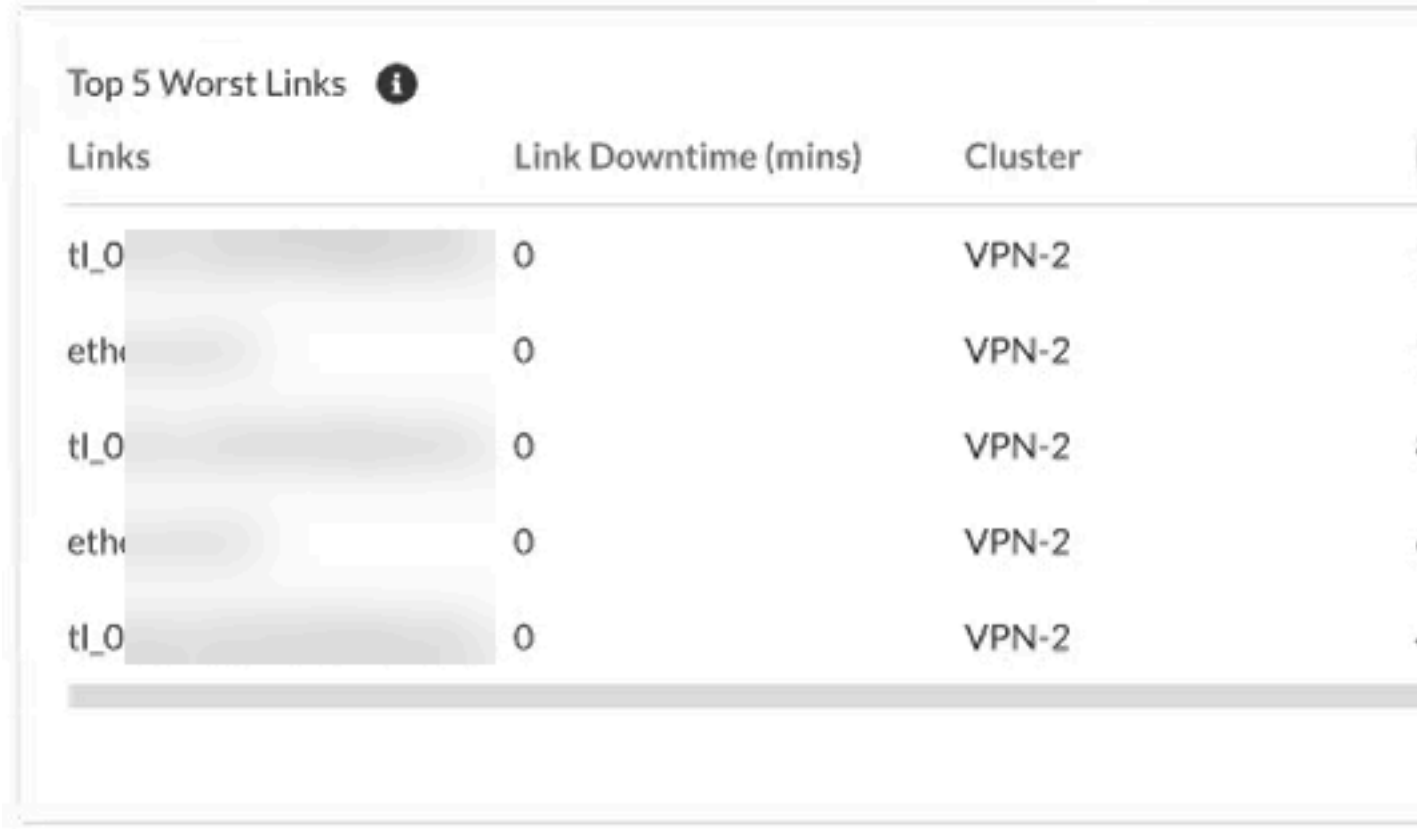


# NGFW SD-WAN Dashboard: Schlechteste Verbindungen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | ❑ AIOps for NGFW Premium oder Strata Cloud Manager Pro<br><br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

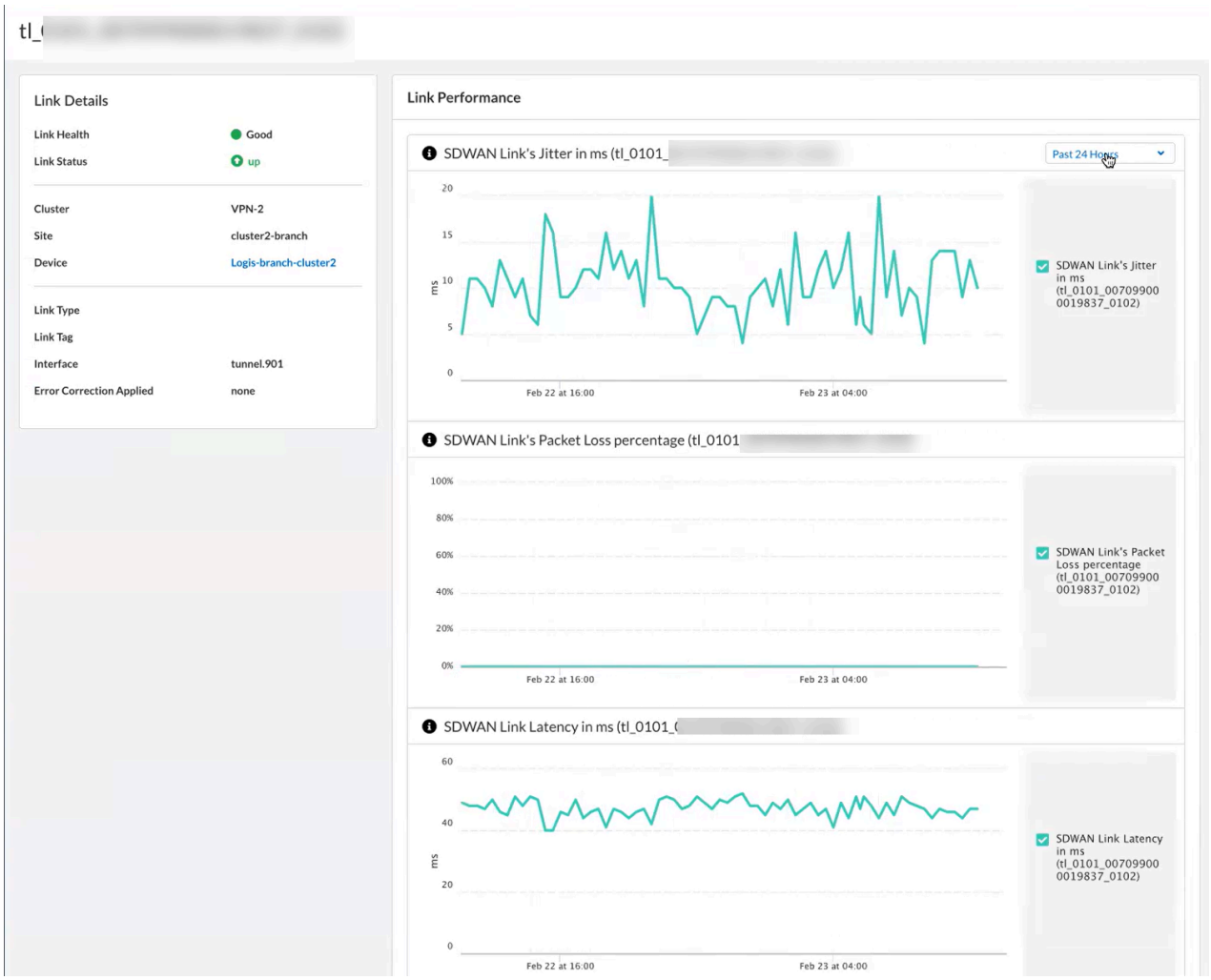
Für die ausgewählte Zeitdauer und den ausgewählten VPN-Cluster zeigt Strata Cloud Manager Ihre fünf schlechtesten Verbindung auf Grundlage des berechneten Durchschnitts der Schnittstellenmetriken (Tunnelausfallzeit, Latenz, Jitter und Paketverlust) an. Die Links werden nach der Priorität von Tunnelausfallzeiten, Latenz, Paketverlust und Jitter eingestuft. Ein höherer berechneter Durchschnitt weist auf die schlechte Qualität der Links hin.




Klicken Sie auf **Mehr anzeigen**, um alle betroffenen Verbindungen zu überprüfen.


Klicken Sie außerdem auf eine Verbindung, um ihre Details anzuzeigen, einschließlich Diagrammen, die auf der Verbindungsleistung basieren.

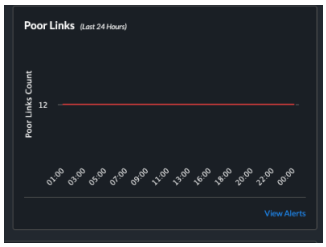


# NGFW SD-WAN Dashboard: Schlechte Links

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | ❑ AIOps for NGFW Premium oder Strata Cloud Manager Pro<br><br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

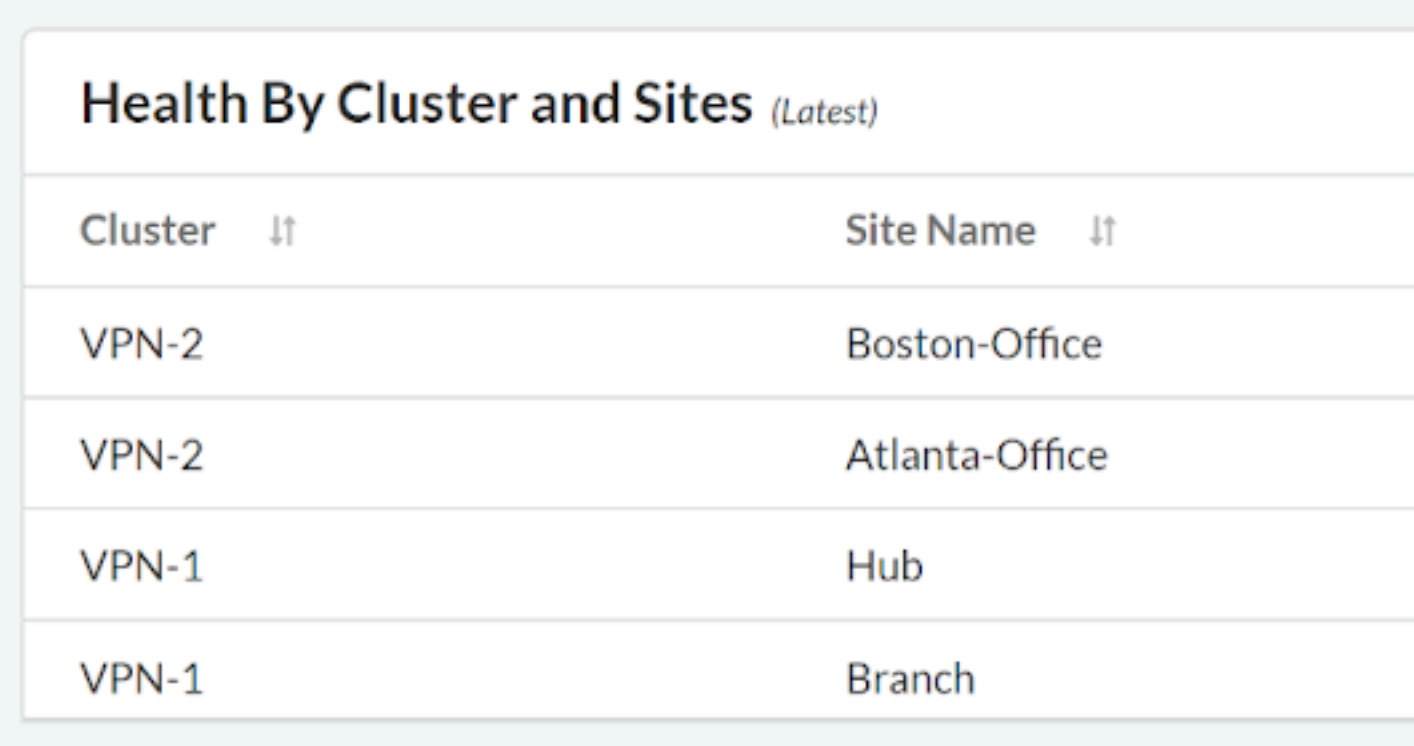
- Das Diagramm zeigt einen Trend, der schlechte Verbindungen zeigt, die in den letzten 24 Stunden entdeckt wurden. Bewegen Sie den Mauszeiger über die Trendlinie, um die schlechten Verbindungen zu einem bestimmten Zeitpunkt anzuzeigen.
- Klicken Sie auf **Benachrichtigungen anzeigen**, um die zugehörigen Benachrichtigungen anzuzeigen, die aufgrund der schlechten Verbindungen ausgelöst werden.




# NGFW SD-WAN Dashboard: Zustand nach Clustern und Standorten

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | ❑ AIOps for NGFW Premium oder Strata Cloud Manager Pro<br><br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Zeigen Sie für jede Standort die Anzahl der Verbindungen, ihren Zustand und die betroffenen Anwendungen an.




Klicken Sie auf die verlinkten Zahlen unter diesen Spalten, um Details dazu anzuzeigen.

# Dashboard: Prisma SD-WAN

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma SD-WAN | ❑ Prisma SD-WAN-Lizenz<br>Weitere für Sichtbarkeit erforderliche Lizenzen und Voraussetzungen:<br>❑ Lizenzen zum Freischalten bestimmter Widgets im Dashboard<br>❑ WAN Clarity für prädiktive Analysen<br>❑ eine Rolle mit der Berechtigung zum Anzeigen des Dashboards<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

## Was sehen Sie in diesem Dashboard?

Das Dashboard bietet Ihnen eine grafische Übersicht über die Netzwerk-, Geräte- und Anwendungsmetriken von Prisma SD-WAN. Darüber hinaus wird Ihnen Folgendes angezeigt:

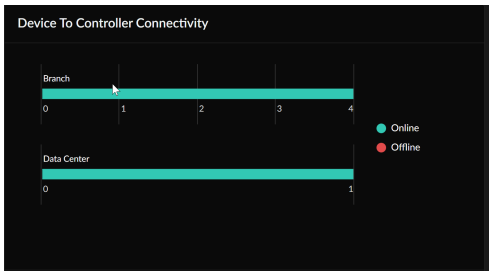
- der Verbindungsstatus zwischen Zweigstellen- und Rechenzentrumsgeräten und Controller
- die Anwendungsnutzungsdaten für Ihren ein- und ausgehenden Datenverkehr
- grundlegende Netzwerkeinblicke und -berichte für alle Zweigstellen eines Mandanten aus der letzten Woche
- Informationen zu den wichtigsten Zweigstellen und Rechenzentrumsstandorten nach der Anzahl der generierten Vorfälle
- die Verbindungsqualitätsmetriken für Ihre Standorte wie MOS-Score, Paketverlust, Jitter und Latenz
- Die prognostizierte Kapazitätsauslastung auf Standortebene basiert auf Informationen der letzten drei bis sechs Monate.

## Prisma SD-WAN-Dashboard: Konnektivität von Gerät zu Controller

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma SD-WAN | ❑ Prisma SD-WAN-Lizenz<br>Weitere für Sichtbarkeit erforderliche Lizenzen und Voraussetzungen: |

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| | ❑ Lizenzen zum Freischalten bestimmter Widgets im Dashboard<br>❑ WAN Clarity für prädiktive Analysen<br>❑ eine Rolle mit der Berechtigung zum Anzeigen des Dashboards<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Das Widget Konnektivität von Gerät zu Controller zeigt die Anzahl der Online- und Offline-ION-Geräte an, die mit dem Prisma SD-WAN-Controller für eine Zweigstelle und ein Rechenzentrum verbunden ist. Anhand dieser interaktiven Grafik können Sie den Online- oder Offline-Status eines beanspruchten Geräts für die entsprechende Zweigstelle und das entsprechende Rechenzentrum anzeigen.



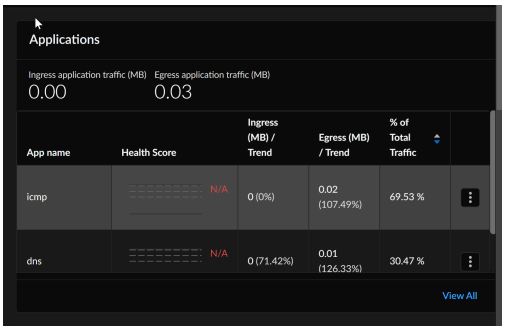

Wenn Sie entweder auf **Zweigstelle** oder **Rechenzentrum** in der interaktiven Grafik klicken, können Sie den Namen und den Status der beanspruchten und nicht beanspruchten Geräte, die installierte Softwareversion, die letzte Aktivität und den Redundanzstatus des Geräts anzeigen.

## Prisma SD-WAN-Dashboard: Anwendungen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma SD-WAN | ❑ Prisma SD-WAN-Lizenz<br>Weitere für Sichtbarkeit erforderliche Lizenzen und Voraussetzungen:<br>❑ Lizenzen zum Freischalten bestimmter Widgets im Dashboard<br>❑ WAN Clarity für prädiktive Analysen<br>❑ eine Rolle mit der Berechtigung zum Anzeigen des Dashboards<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung |

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| | stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Das Widget Anwendungen zeigt Informationen zur Anwendungsnutzung am Standort während des ausgewählten Zeitbereichs an. Der gesamte ein- und ausgehende Anwendungsverkehr für den Zeitbereich wird angezeigt. Die Top-10-Anwendungen nach Verkehrsaufkommen werden zusammen mit dem sonstigen Datenverkehr angezeigt. Klicken Sie auf **Alle anzeigen**, um die Anwendungszustandsverteilung, die TCP-Anwendungszustandsverteilung im Zeitverlauf, neue Flüsse, die Bandbreitenauslastung, die Transaktionsstatistiken für den ausgewählten Zeitbereich sowie die Top-Anwendungen anzuzeigen. Sie können im Dashboard detaillierte Informationen zur Leistung einer Anwendung sowie zu den Messdaten pro Standort für den ausgewählten Zeitbereich anzeigen.



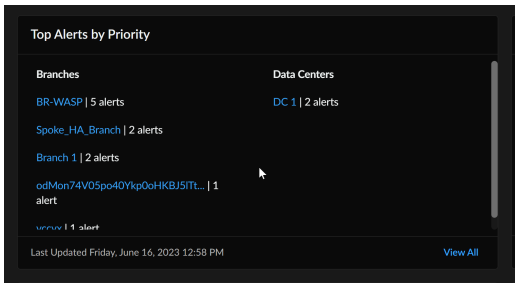

Zunächst werden die Metriken für alle TCP-Anwendungen angezeigt, Sie können jedoch auch eine der Top-10-TCP-Anwendungen auswählen, um sich noch stärker auf eine bestimmte Top-Anwendung zu konzentrieren.

## Prisma SD-WAN-Dashboard: Top-Benachrichtigungen nach Priorität

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma SD-WAN | ❑ Prisma SD-WAN-Lizenz<br>Weitere für Sichtbarkeit erforderliche Lizenzen und Voraussetzungen:<br>❑ Lizenzen zum Freischalten bestimmter Widgets im Dashboard<br>❑ WAN Clarity für prädiktive Analysen<br>❑ eine Rolle mit der Berechtigung zum Anzeigen des Dashboards<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Das Widget **Top-Benachrichtigungen nach Priorität** zeigt die fünf wichtigsten Benachrichtigungen nach Priorität an. Sie können Informationen zu den wichtigsten Zweigstellen- und Rechenzentrumsstandorten anhand der Anzahl der im ausgewählten Zeitbereich generierten Benachrichtigungen anzeigen. Sie können zur Detailansicht wechseln, um die Benachrichtigungsinformationen pro Standort für den ausgewählten Zeitbereich anzuzeigen.




Klicken Sie auf **Alle anzeigen**, um die folgenden Informationen zu den Benachrichtigungen anzuzeigen:

- wann der Alarm erstellt wurde
- Name des Vorfalls
- primäres betroffenes Objekt
- Schweregrad der Benachrichtigung
- Priorität der Benachrichtigung

Klicken Sie auf das Drei-Punkte-Symbol, um die Benachrichtigung zu beheben.

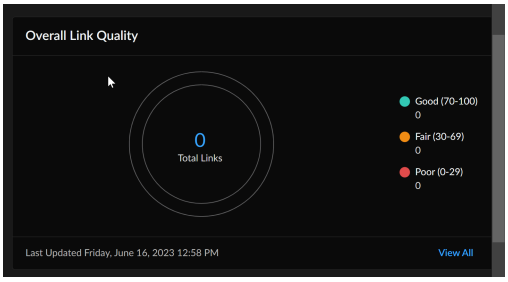
## Prisma SD-WAN-Dashboard: Allgemeine Verbindungsqualität

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma SD-WAN | ☐ Prisma SD-WAN-Lizenz<br><br>Weitere für Sichtbarkeit erforderliche Lizenzen und Voraussetzungen:<br><br>☐ Lizenzen zum Freischalten bestimmter Widgets im Dashboard<br>☐ WAN Clarity für prädiktive Analysen<br>☐ eine Rolle mit der Berechtigung zum Anzeigen des Dashboards<br><br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Das Widget **Allgemeine Verbindungsqualität** bietet eine Gesamtübersicht über den aktuellen Status der Verbindungen all Ihrer Standorte für den ausgewählten Zeitbereich. Sie können detaillierte Informationen zur Verbindungsleistung, zum Verbindungs-

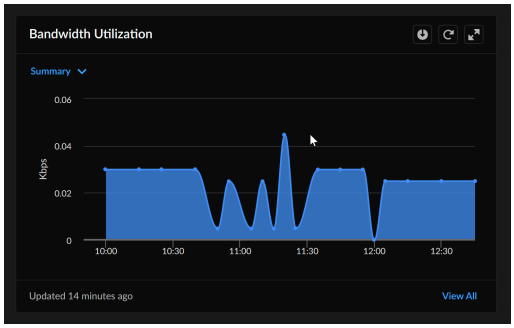
Paketverlust, zum Verbindungs-Jitter und zur Verbindungslatenz anzeigen und im Dashboard Verbindungsqualitätsmetriken die gewünschten Informationen genauer analysieren.




## Prisma SD-WAN-Dashboard: Bandbreitennutzung

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma SD-WAN | ❑ Prisma SD-WAN-Lizenz<br>Weitere für Sichtbarkeit erforderliche Lizenzen und Voraussetzungen:<br>❑ Lizenzen zum Freischalten bestimmter Widgets im Dashboard<br>❑ WAN Clarity für prädiktive Analysen<br>❑ eine Rolle mit der Berechtigung zum Anzeigen des Dashboards<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Das Widget Bandbreitennutzung zeigt die Menge der Bandbreite, die auf einem Pfad in einem Netzwerk verwendet wird. Es bietet eine visuelle Darstellung der Bandbreitenspitzen, der gesamten von einem bestimmten Standort verbrauchten Bandbreite sowie der Anwendung und gibt an, ob der Upload in Eingangs-, in Ausgangs- oder in beide Richtungen erfolgt.




Fahren Sie mit dem Mauszeiger über das Diagramm **Bandbreitennutzung**, um eine detailliertere Ansicht der Bandbreitenauslastung einer Anwendung oder eines bestimmten Zeitpunkts zu erhalten. Typischerweise werden die Anwendungen nach ihrer Bandbreitennutzung sortiert.

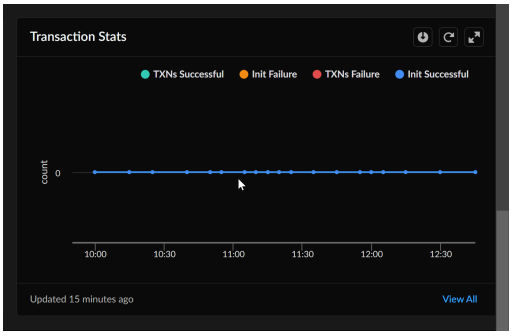
Das Diagramm zeigt die im Laufe der Zeit verbrauchte Bandbreite. Die 1H-Ansicht bietet detaillierte Daten im Minutentakt und das 1D-Bild zeigt alle fünf Minuten neue Daten an. Die 1D-Diagrammdaten umfassen für jede Probe durchschnittlich über fünf Minuten. Wenn die Auslastung länger als fünf Minuten anhält, können Sie in beiden Diagrammen die entsprechende Spitzenauslastung sehen.

Sie können die Download-Option des Widgets verwenden, um das Diagramm zur Bandbreitenauslastung in den Formaten PDF, CSV, XLS oder PNG herunterzuladen.

# Prisma SD-WAN-Dashboard: Transaktionsstatistiken

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma SD-WAN | ❑ Prisma SD-WAN-Lizenz<br><br>Weitere für Sichtbarkeit erforderliche Lizenzen und Voraussetzungen:<br><br>❑ Lizenzen zum Freischalten bestimmter Widgets im Dashboard<br><br>❑ WAN Clarity für prädiktive Analysen<br><br>❑ eine Rolle mit der Berechtigung zum Anzeigen des Dashboards<br><br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Das Widget Transaktionsstatistiken bietet Transaktionsstatistiken über TCP-Flüsse, einschließlich Initiierungs-/Transaktionserfolgen und -fehlschlägen für eine bestimmte Anwendung oder für alle Anwendungen, für einen bestimmten Pfad oder für alle Pfade sowie für alle Zustandsereignisse. Es misst die Leistung sowie die Verfügbarkeit von Netzwerken und Anwendungen, die auf Netzwerkpfaden ausgeführt werden. Für jede Anfrage auf einem bestimmten Pfad überwacht Prisma SD-WAN in Echtzeit die Transaktionsfehlerraten für Initiierungs- und Datenübertragungstransaktionen.




Zeigen Sie im Diagramm „Transaktionsstatistiken“ die Liste der Apps nach Bandbreitennutzung oder Pfad an. Sie können erfolgreiche Transaktionen herausfiltern, um eine detaillierte Ansicht

der Statistiken zu fehlgeschlagenen Transaktionen zu erhalten. Das Diagramm zeigt die Anzahl erfolgreicher oder fehlgeschlagener Transaktionen für die folgenden Kategorien an:

- **Initialisierung erfolgreich**: Erfolgreicher Abschluss des Drei-Wege-Handshakes.
- **Erfolgreiche TXNs**: Erfolgreiche Datenübertragung nach Abschluss des Drei-Wege-Handshakes.
- **Initialisierungsfehler**: Der Drei-Wege-Handshake konnte nicht abgeschlossen werden. Gründe für einen Fehler können eine falsch konfigurierte Firewall, ein Problem mit dem Anwendungsserver, eine falsch konfigurierte Netzwerk-Zugriffskontrollliste oder ein Problem mit dem WAN-Netzwerkanbieter sein.
- **TXNs-Fehler**: Nicht erfolgreiche Datenübertragung nach Abschluss des Drei-Wege-Handshakes. Gründe für einen Fehler können eine falsch konfigurierte Firewall, ein Problem mit dem Anwendungsserver, eine falsch konfigurierte Netzwerk-Zugriffskontrollliste oder ein Problem mit dem WAN-Netzwerkanbieter sein.

Sie können die Download-Option des Widgets verwenden, um das Diagramm zur Bandbreitenauslastung in den Formaten PDF, CSV, XLS oder PNG herunterzuladen.

## Prisma SD-WAN-Dashboard: Prädiktive Analysen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma SD-WAN | ☐ Prisma SD-WAN-Lizenz<br><br>Weitere für Sichtbarkeit erforderliche Lizenzen und Voraussetzungen:<br><br>☐ Lizenzen zum Freischalten bestimmter Widgets im Dashboard<br>☐ WAN Clarity für prädiktive Analysen<br>☐ eine Rolle mit der Berechtigung zum Anzeigen des Dashboards<br><br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Das Widget Prädiktive Analyse bietet Einblick in den Zustand von Standorten und Anwendungen sowie proaktive Überwachung, um kritische Probleme schneller zu erkennen und zu beheben und so die Servicelevel zu verbessern. Es identifiziert kritische Standorte, Verbindungen und Anwendungen und kategorisiert sie auf Mandantenebene basierend auf den KI-/ML-Zustandsscores als **gut**, **angemessen** und **schlecht**. Das Widget ermöglicht die Vorhersage der Kapazitätsauslastung auf Zweigstellenebene auf der Grundlage von Informationen der letzten drei bis sechs Monate.

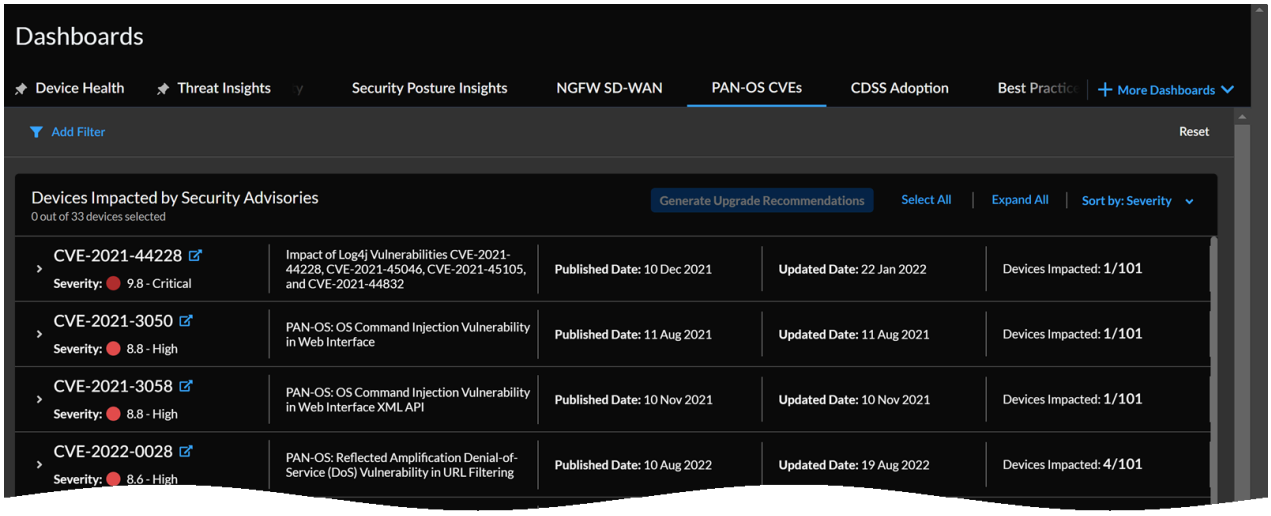

Der Standardzeitbereich zum Anzeigen der Metriken beträgt drei Stunden. Sie können ihn jedoch je nach gewünschtem Informationsumfang zu kürzeren oder längeren Zeiträumen ändern. Erhalten Sie Einblicke in die Top 10 der Standorte, deren Bandbreitenauslastung in den letzten 28 Tagen gestiegen ist. Sie können sich die 7-Tage-Vorhersage ansehen, wenn die 28-Tage-Vorhersage nicht verfügbar ist, und die zukünftige Kapazitätsauslastung der Zweigstelle vorhersagen.

Klicken Sie auf **Alle anzeigen**, um Einblicke in Zweigstellen, Anwendungen, Verbindungen, Netzwerkeinblicke, Top-Standorte mit gestiegenem Verkehrsaufkommen in den letzten 30 Tagen sowie in Standortkapazitätsprognosen und -anomalien zu erhalten.

# Dashboard: PAN-OS-CVEs

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | ☐ Strata Cloud Manager Essentials<br>☐ AIOps for NGFW Premium oder Strata Cloud Manager Pro<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

- Klicken Sie auf **Dashboards > Mehr Dashboards > PAN-OS-CVEs**, um zu beginnen.




## Was sehen Sie in diesem Dashboard?

*Das Dashboard zeigt die aggregierten Daten für alle Firewalls und Panorama-Bereitstellungen, die in Ihren Mandanten eingebunden sind, und sendet auch Telemetriedaten. Darüber hinaus werden die Telemetriedaten aus der CVE-Datenbank des NGFW PSIRT angezeigt.*

Das Dashboard **PAN-OS-CVEs** zeigt Ihnen abhängig von den auf den Geräten aktivierten Funktionen die Anzahl der von einer bestimmten Sicherheitslücke betroffenen Geräte an. Strata Cloud Manager analysiert die aktivierten Funktionen, um die vom CVE betroffenen Geräte zu bestimmen.

Nachdem Sie die Sicherheitslücken der betroffenen Geräte verstanden haben, können Sie Ihre Patches mithilfe der Funktion „Empfehlungen für Upgrade“ planen. Erweitern Sie die CVEs und wählen Sie Firewalls aus, die Sie aktualisieren möchten, um die Sicherheitslücken zu beheben, und klicken Sie auf **Upgrade-Empfehlungen generieren**. Sie werden zu NGFW – Upgrade-Empfehlungen weitergeleitet, um den generierten Bericht anzuzeigen.

Hier erfahren Sie, wie Sie Sicherheitslücken, die sich auf Geräte auswirken, bewerten und Upgrade-Empfehlungen zum Beheben der Sicherheitslücken erstellen.

## Wie können Sie die Daten aus dem Dashboard nutzen?

Dieses Dashboard unterstützt Sie bei Folgendem:

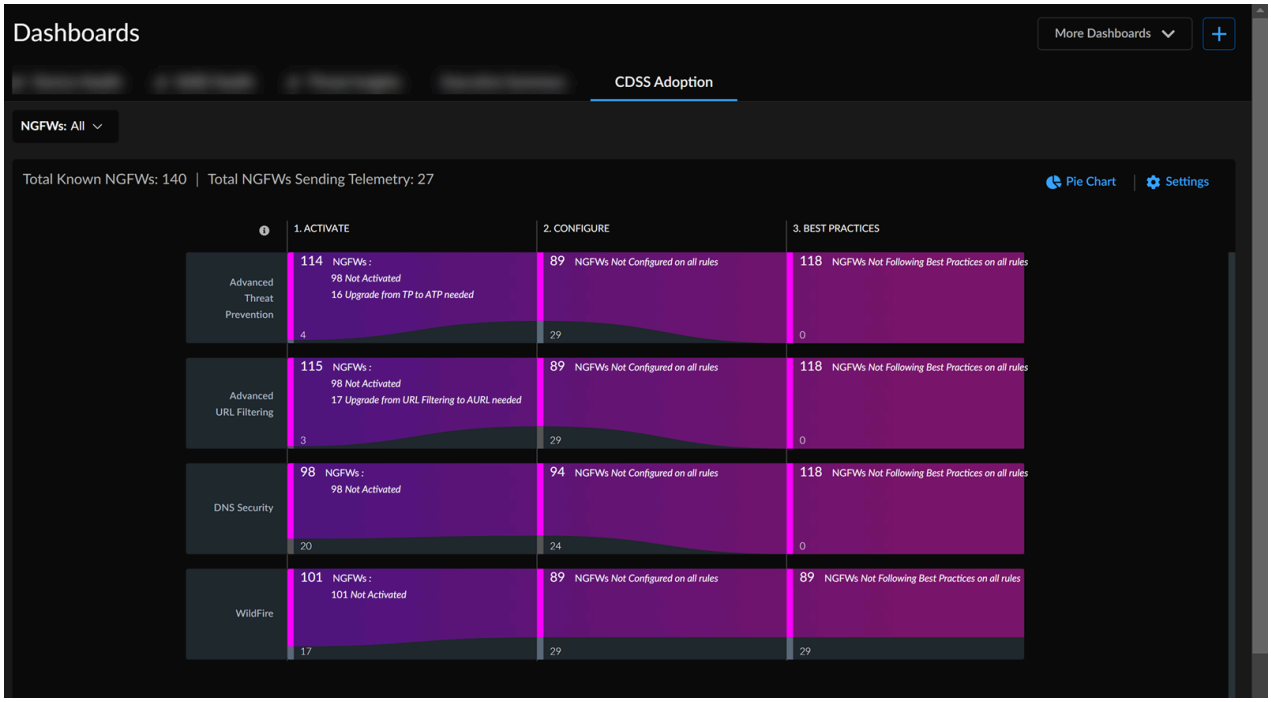
- Entscheiden Sie, welche Geräte aktualisiert werden sollen, um eine Sicherheitslücke zu schließen.
- Zeigen Sie Details zu einem betroffenen Gerät an, beispielsweise Hostname, Modell, Seriennummer, SW-Version und letztes Telemetrie-Update, indem Sie einen CVE erweitern.
- Filtern Sie CVEs und sortieren Sie sie weiter nach **Schweregrad** oder **betroffenen Geräten**.
- Klicken Sie auf die mit einer CVE verknüpfte Empfehlung, um sie anzuzeigen.

# Dashboard: Einführung von CDSS

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | ❑ Strata Cloud Manager Essentials<br>❑ AIOps for NGFW Premium oder Strata Cloud Manager Pro<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

- Klicken Sie auf **Dashboards** > **Status** > **Einführung von CDSS**, um loszulegen.




## Was sehen Sie in diesem Dashboard?

- *Das Dashboard zeigt die aggregierten Daten für alle Firewalls, die in Ihre Mandanten eingebunden sind, und sendet auch Telemetriedaten.*
- *Derzeit unterstützt dieses Dashboard nur vier Sicherheitsabonnements: „Fortschrittliche Bedrohungsabwehr“, „Erweiterte URL-Filterung“, „DNS Security“ und „WildFire“.*

Das Dashboard **Einführung von CDSS** zeigt die empfohlenen Abonnements für über die Cloud bereitgestellte Sicherheitsdienste (Cloud-Delivered Security Services, CDSS) und deren Verwendung auf Ihren Geräten. Dies hilft Ihnen, Sicherheitslücken zu bestimmen und den Sicherheitsstatus Ihres Unternehmens zu verbessern. Auf dieser Seite wird ein Pop-up-Fenster angezeigt, in dem Sie aufgefordert werden, Ihre Zonenrollen in NGFWs zu bestätigen oder zu aktualisieren, um genaue Empfehlungen zu Sicherheitsdiensten zu erhalten. Sie können dem Link in diesem Pop-up-Fenster folgen, um Zonen Rollen zuzuordnen.

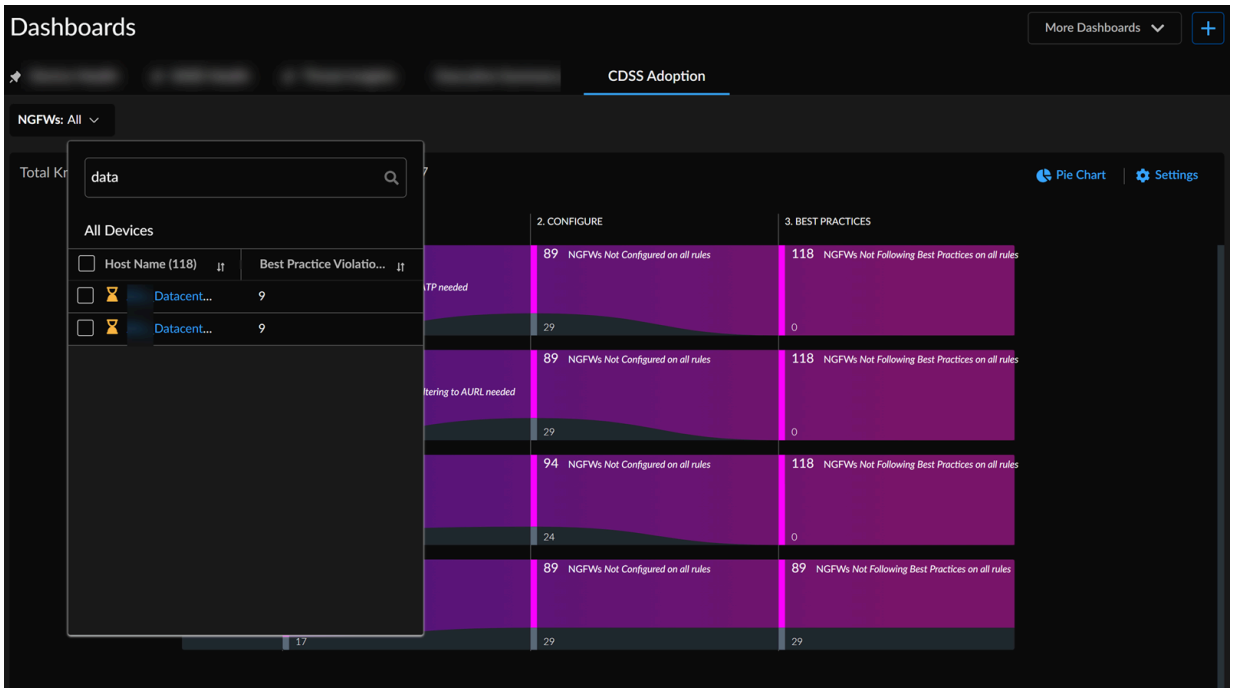
Hier ist ein Video, das zeigt, wie Sie Sicherheitsabonnements mithilfe des Dashboards **Einführung von CDSS** überwachen:

## Wie können Sie die Daten aus dem Dashboard nutzen?

Dieses Dashboard hilft Ihnen wie folgt:

- Oben auf der Übersichtsseite können Sie die Gesamtzahl der bekannten NGFWs und die Anzahl der NGFWs anzeigen, die in Ihrer „AIOps für NGFW“-Instanz Telemetriedaten senden. Die Einführung von CDSS umfasst die schrittweise Aktivierung, Konfiguration und Einhaltung von Best Practices. Um den Fortschritt der einzelnen Abonnements zu verfolgen, klicken Sie einfach auf die Zahlen im Diagramm, um eine Liste der Geräte anzuzeigen, die im Laufe des Vorgangs aktualisiert werden müssen. Um eine Sicherheitsabonnement-Lizenz auf einem Gerät zu verwenden, müssen Sie diese aktivieren und dann den Dienst oder die Funktion entsprechend einrichten.

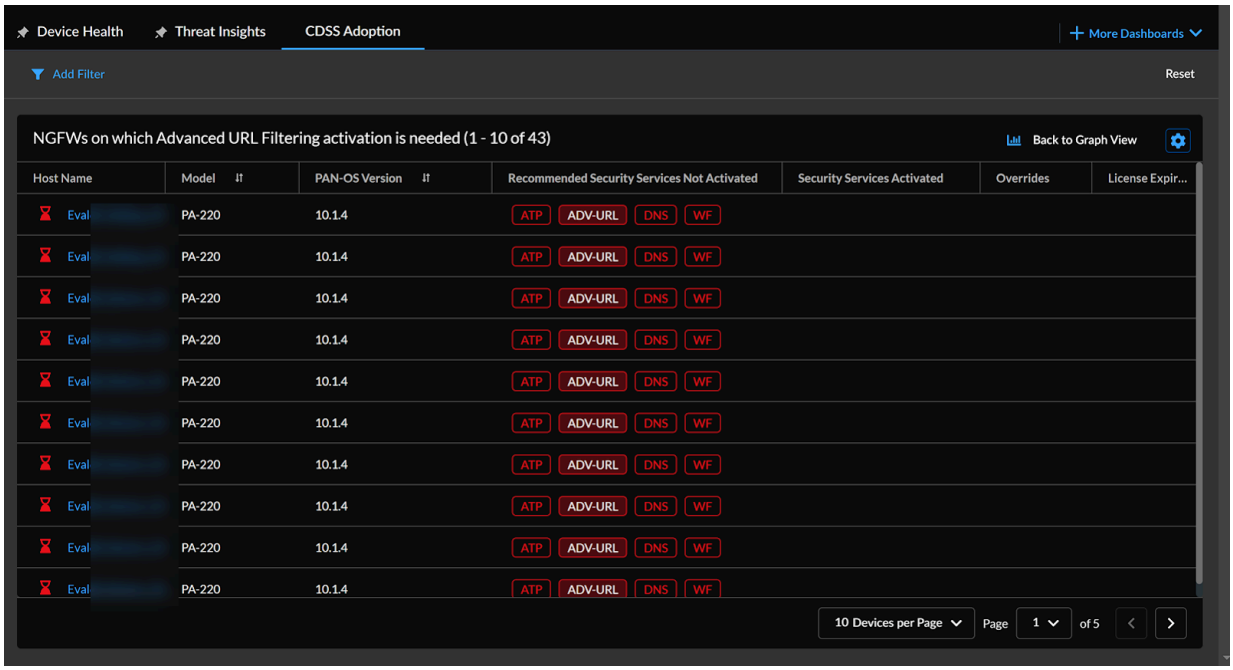
  Um sich auf die Sicherheitsdienstdaten für eine bestimmte NGFW zu konzentrieren, filtern Sie das Diagramm darauf basierend. In dieser Dropdown-Liste können Sie auch die Best-Practice-Verstöße für ein Gerät anzeigen.



- Sie können auf einen der Werte unter **AKTIVIEREN**, **KONFIGURIEREN** oder **BEST PRACTICES** klicken, um Details in einem Tabellenformat anzuzeigen.

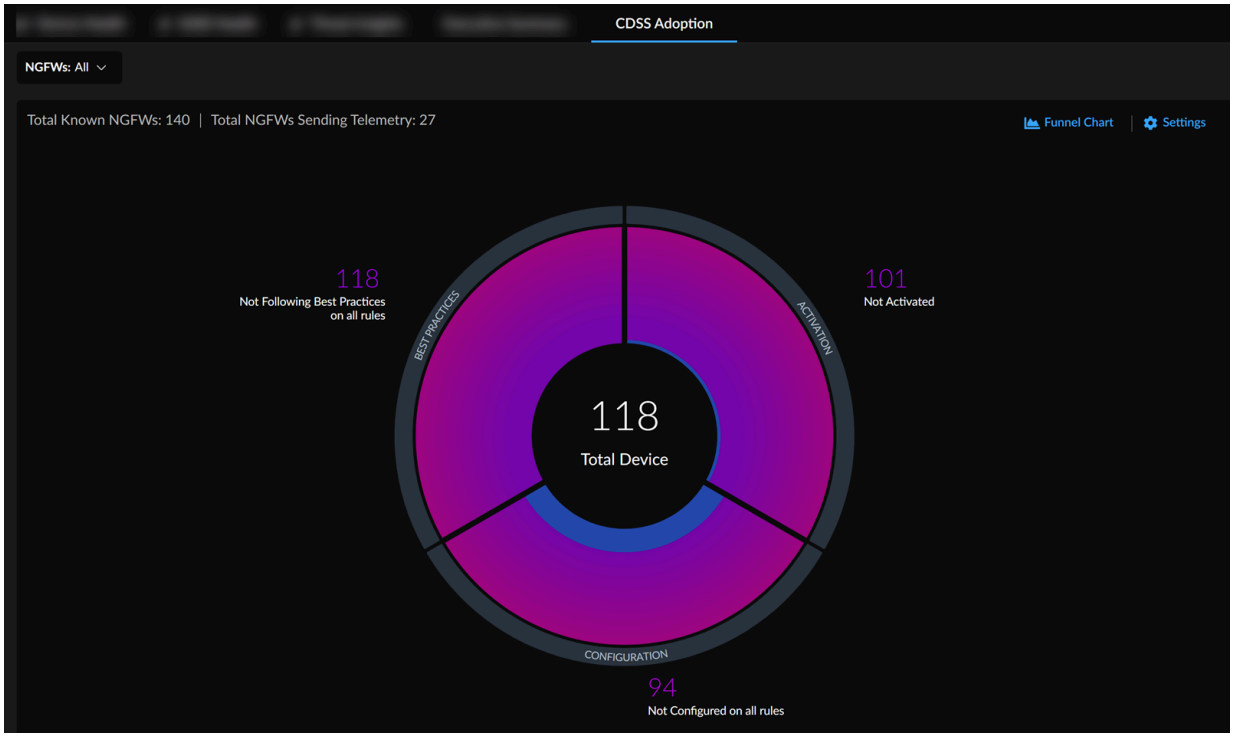
 



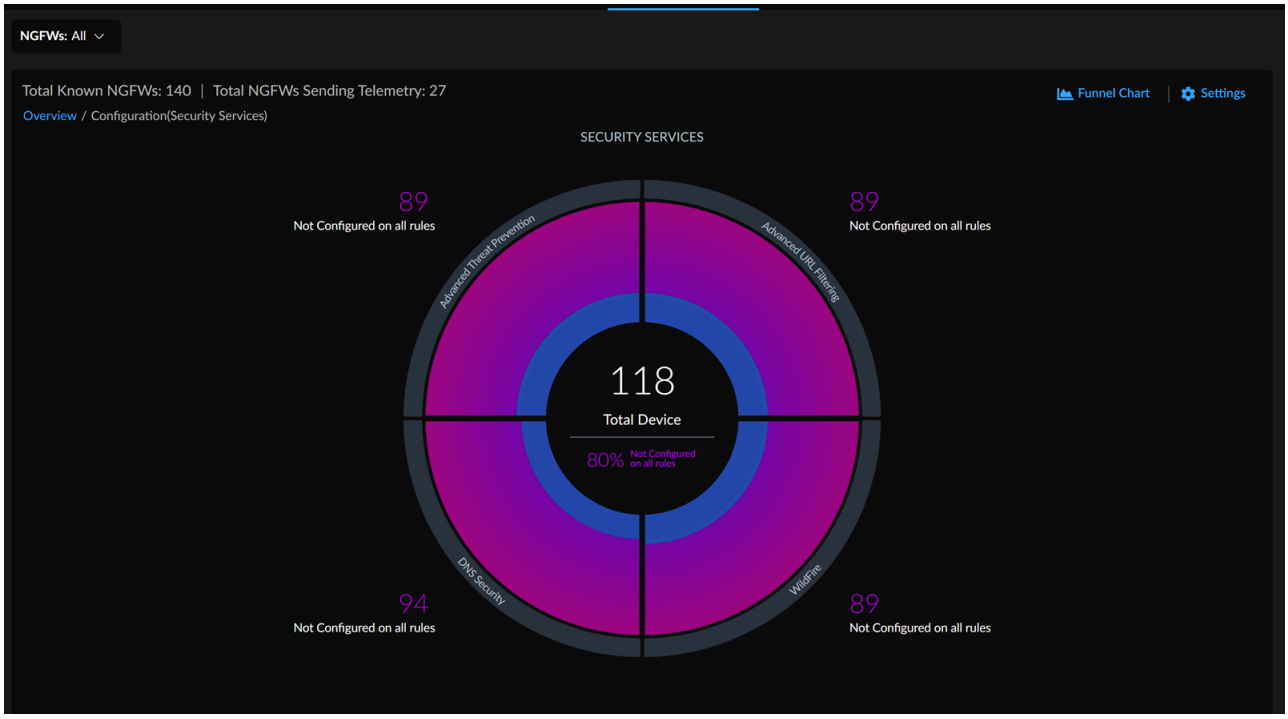
In diesem Beispiel empfiehlt AIOps für NGFW die Aktivierung der erweiterten URL-Filterung (ADV-URL) zusammen mit fortschrittlicher Bedrohungsabwehr (Advanced Threat Prevention, ATP), Domain Name System (DNS) und WF-Sicherheitsdiensten (WildFire) für NGFWs. Sie können auf **Zurück zur Diagrammansicht** klicken, um zur Übersichtsseite zu navigieren.

- Sie können dieselben Sicherheitsstatusdaten auch in einem Kreisdiagramm anzeigen. Klicken Sie auf das Kreisdiagrammsymbol, um die Informationen zu empfohlenen Sicherheitsdiensten in einem Kreisdiagramm anzuzeigen.



- Sie können auf die Abschnitte des Tortendiagramms klicken, um die Informationen über den jeweiligen Sicherheitsdienst anzuzeigen.

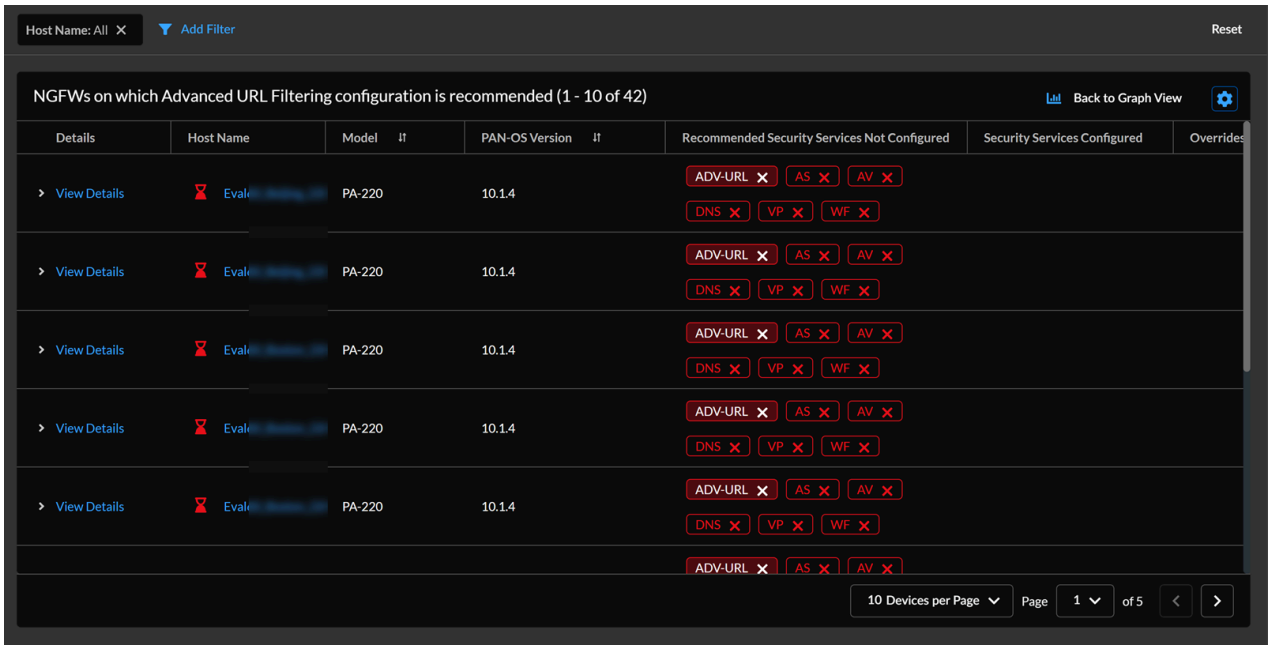



Wenn Sie in diesem Beispiel die NGFW anzeigen möchten, in der DNS Security nicht konfiguriert ist, können Sie entweder auf den Wert oberhalb des Abschnitts **DNS Security** im Kreisdiagramm oder direkt auf den Abschnitt **DNS Security** eines Diagramms klicken.

## Überschreiben empfohlener Sicherheitsdienste

Wenn Sie einen empfohlenen Sicherheitsdienst aus irgendeinem Grund nicht benötigen, können Sie ihn überschreiben. Klicken Sie unter **KONFIGURIEREN** auf einen Wert, um Details in einem Tabellenformat anzuzeigen.

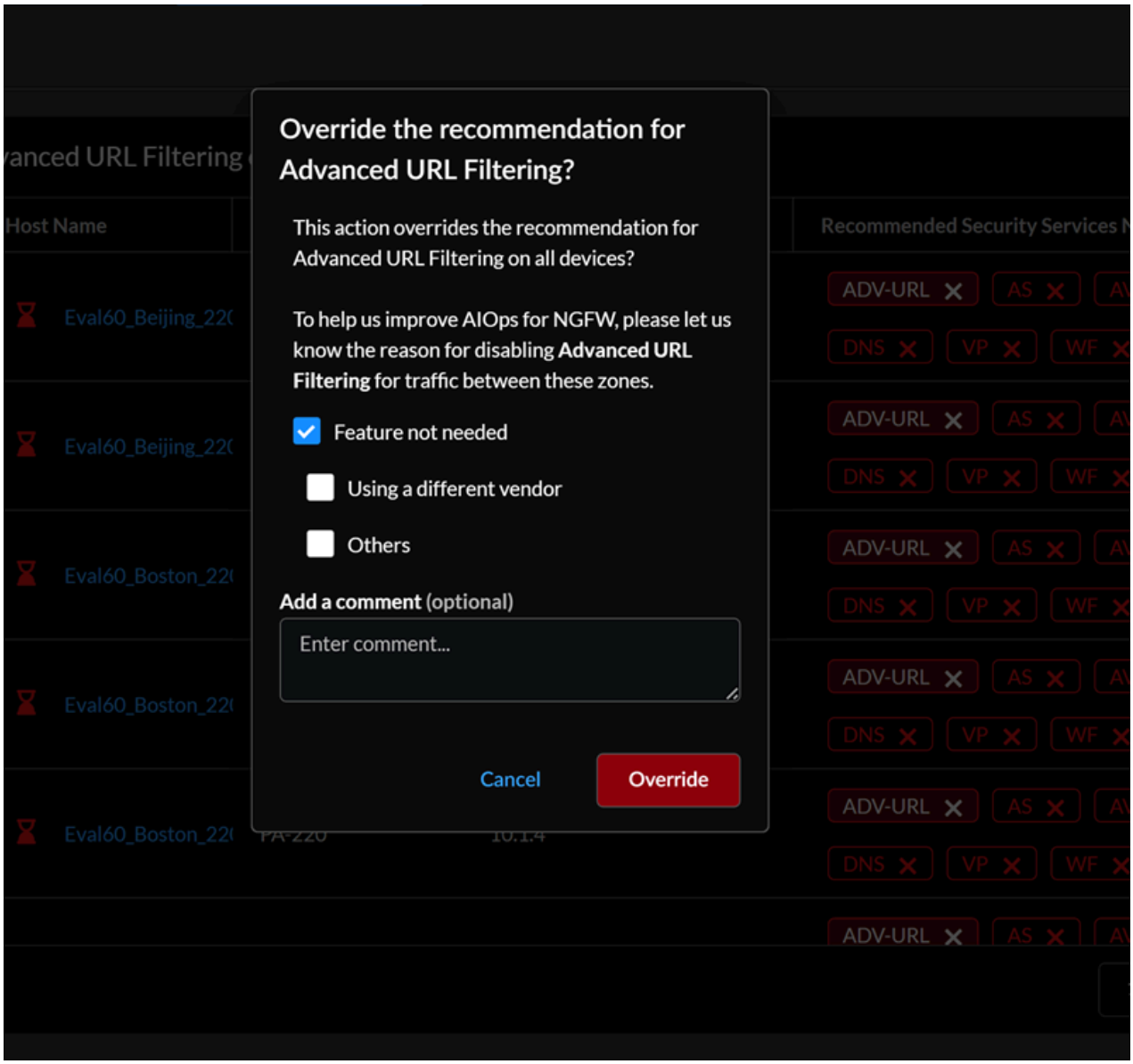
 



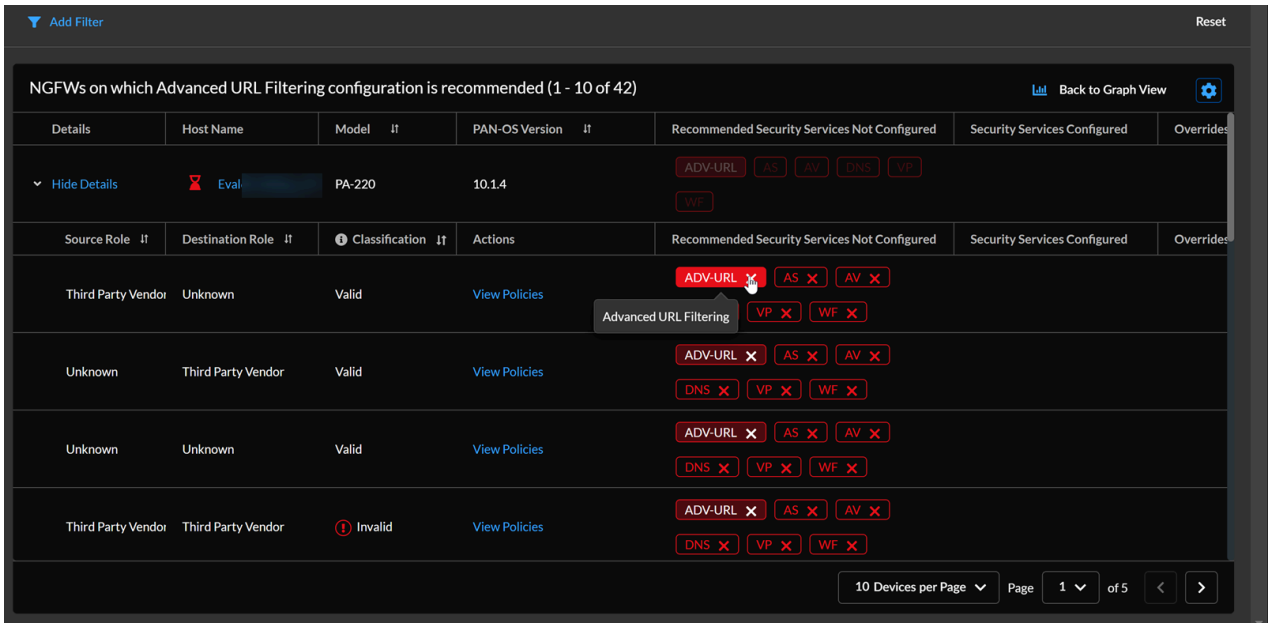
In diesem Beispiel empfiehlt AIOps für NGFW die Konfiguration der erweiterten URL-Filterung (ADV-URL) zusammen mit anderen Sicherheitsdiensten für ein Gerät. Sie können den ADV-URL-Sicherheitsdienst für das NGFW-Gerät und alle darunterliegenden Zonen deaktivieren.



Sie können den empfohlenen Sicherheitsdienst auch auf Zonenebene überschreiben. Wählen Sie **Details anzeigen** für eine NGFW aus, um die Quell- und Zielrollen, die Richtlinien und die empfohlenen Sicherheitsdienste anzuzeigen.

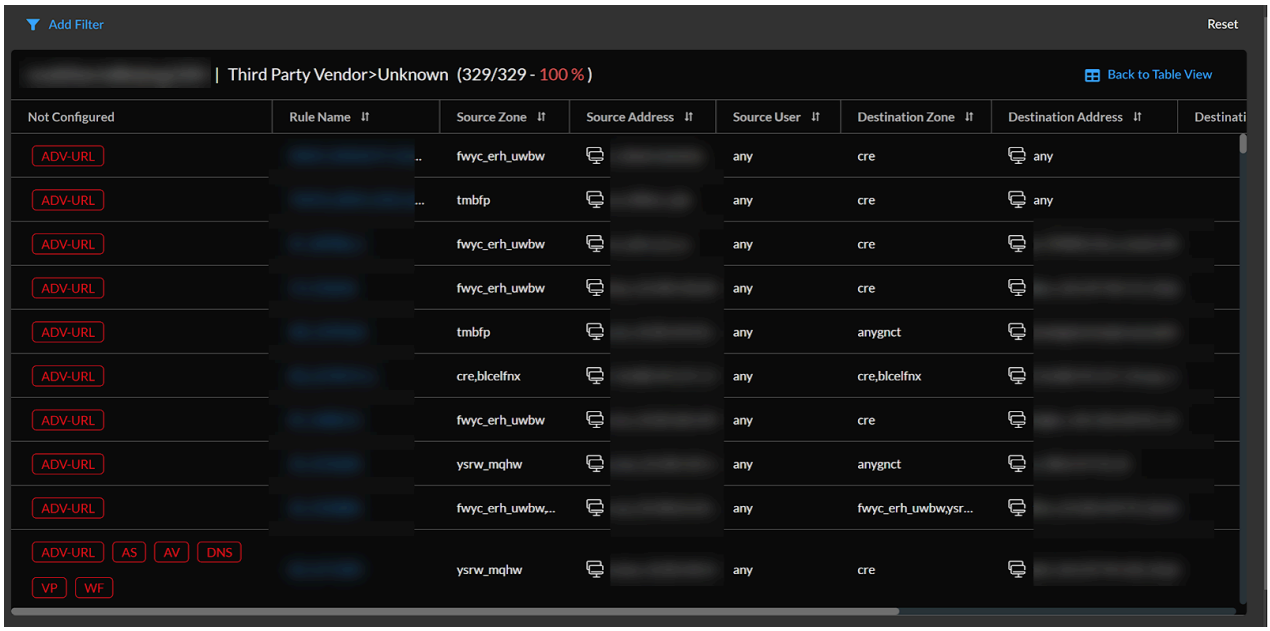


In diesem Beispiel können Sie den **ADV-URL**-Sicherheitsdienst für die Quellrolle als **Drittanbieter** und die Zielrolle als **Unbekannt** überschreiben. Sie können die überschriebene Empfehlung auch wiederherstellen, indem Sie auf den Sicherheitsdienst in der Spalte **Überschreibungen** klicken.

Sie können **Richtlinien anzeigen**, die Rollen zugeordnet sind. Wählen Sie eine Regel aus, um ihre Details anzuzeigen, ohne die App verlassen zu müssen.



Klicken Sie auf **Zurück zur Tabellenansicht**, um die Sicherheitsdienste im Tabellenformat anzuzeigen.

# Dashboard: Funktionsannahme

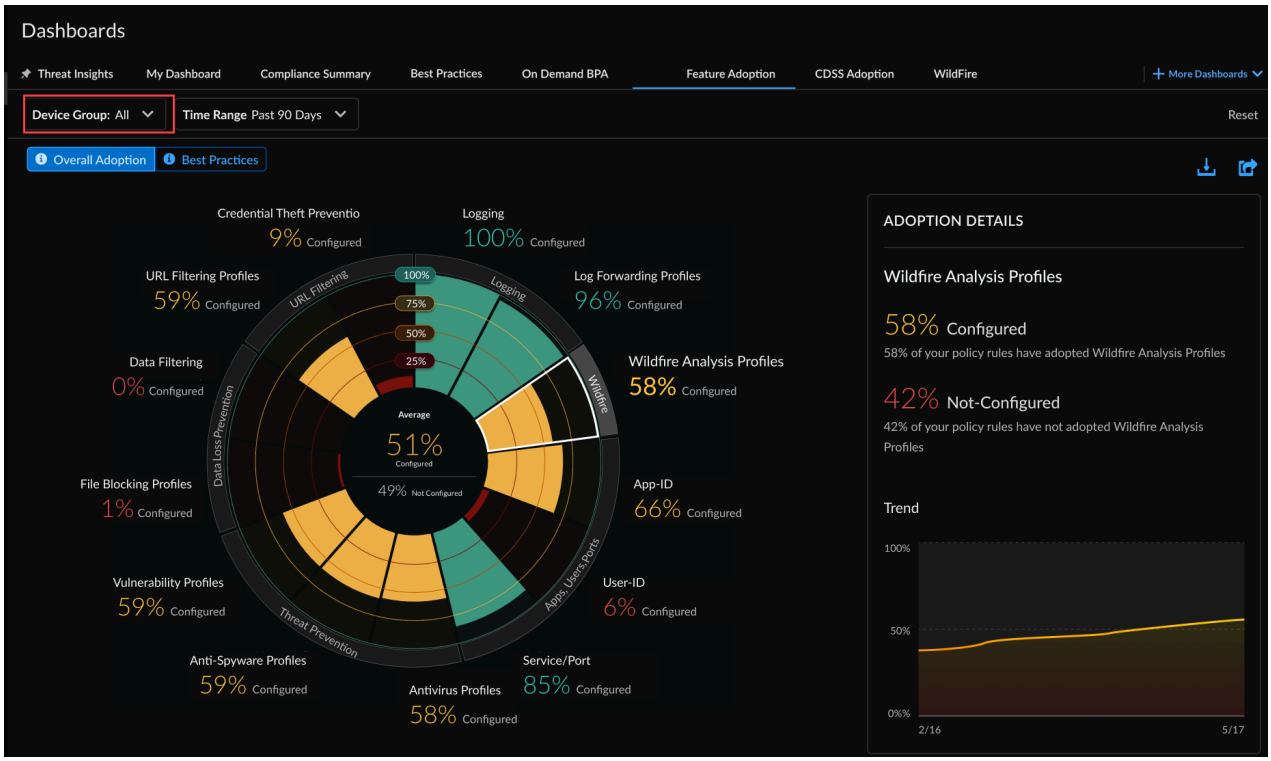
| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | ☐ Strata Cloud Manager Essentials<br>☐ AIOps for NGFW Premium oder Strata Cloud Manager Pro<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

- Klicken Sie auf **Dashboards** > **Funktionsannahme**, um loszulegen.

## Was sehen Sie in diesem Dashboard?

*Das Dashboard zeigt die aggregierten Daten für alle Firewalls, die in Ihre Mandanten eingebunden sind, und sendet auch Telemetriedaten.*

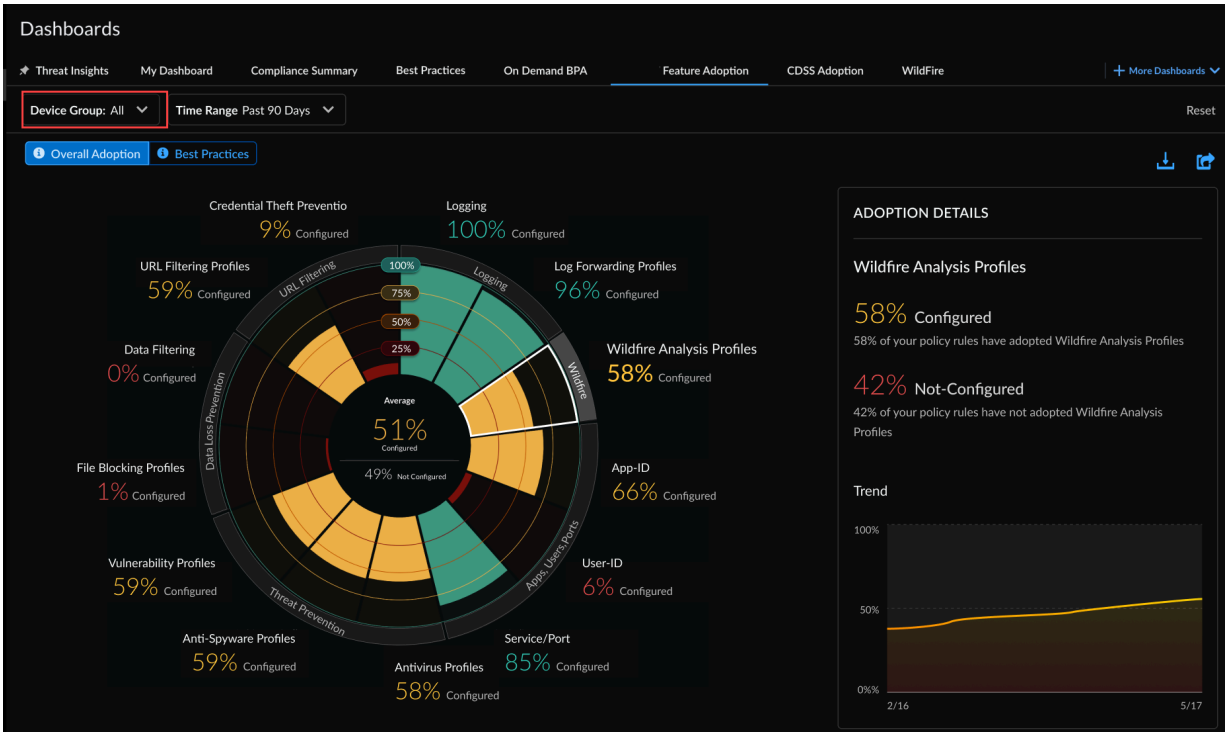
Das Dashboard **Funktionsannahme** zeigt Ihnen die Sicherheitsfunktionen, die Sie in Ihrer Bereitstellung verwenden. Sie können es verwenden, um Lücken bei der Einführung zu identifizieren. So können Sie sicherstellen, dass Sie Ihre Sicherheitsabonnements und Firewall-Funktionen von Palo Alto Networks optimal nutzen.



# So verwenden Sie dieses Dashboard

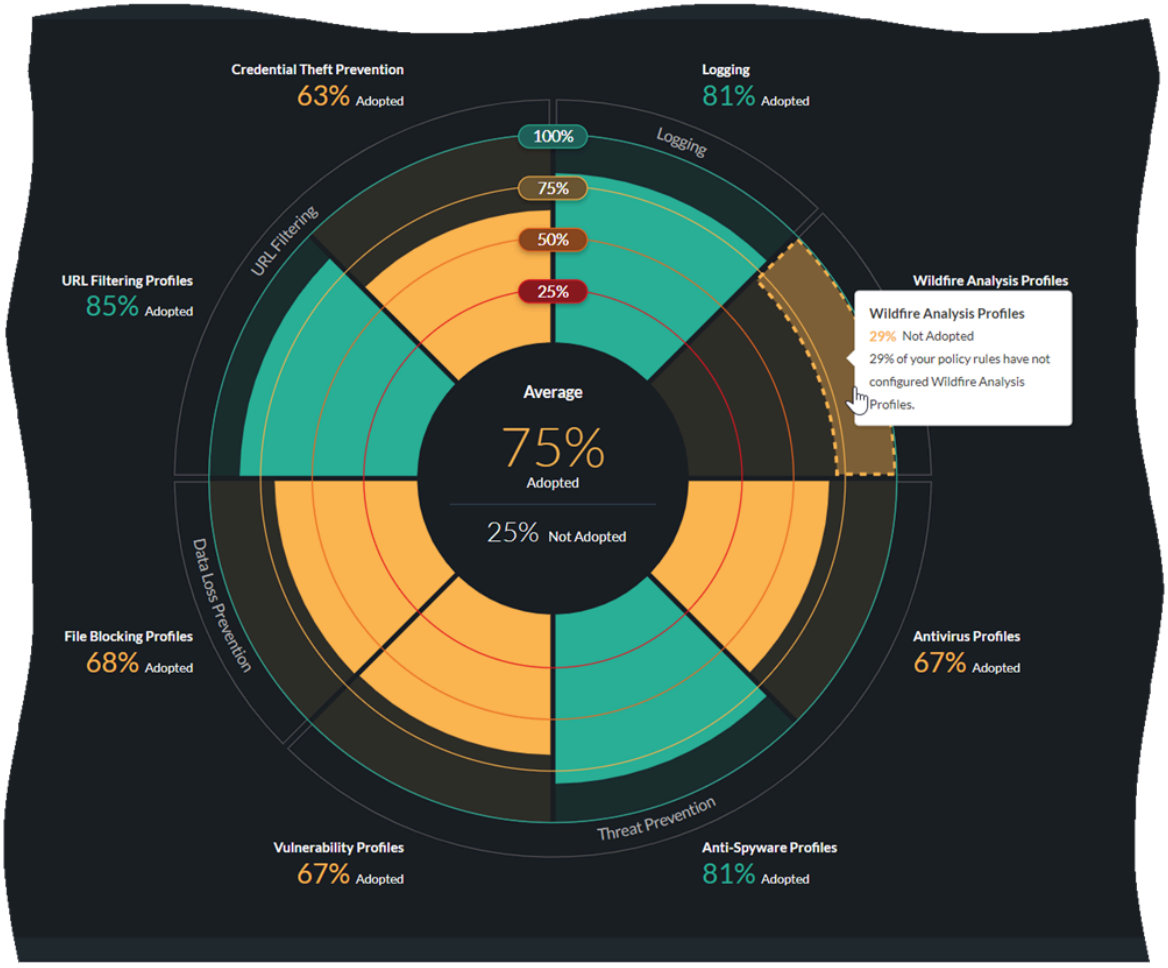
- Um sich auf die Funktionsannahme für eine bestimmte Firewallgruppe zu konzentrieren, können Sie das Diagramm basierend auf der Gerätegruppe filtern, einschließlich von Panorama verwalteter Geräte. Sie können auch Diagramme mit bisherigen Annahmetrends anzeigen.



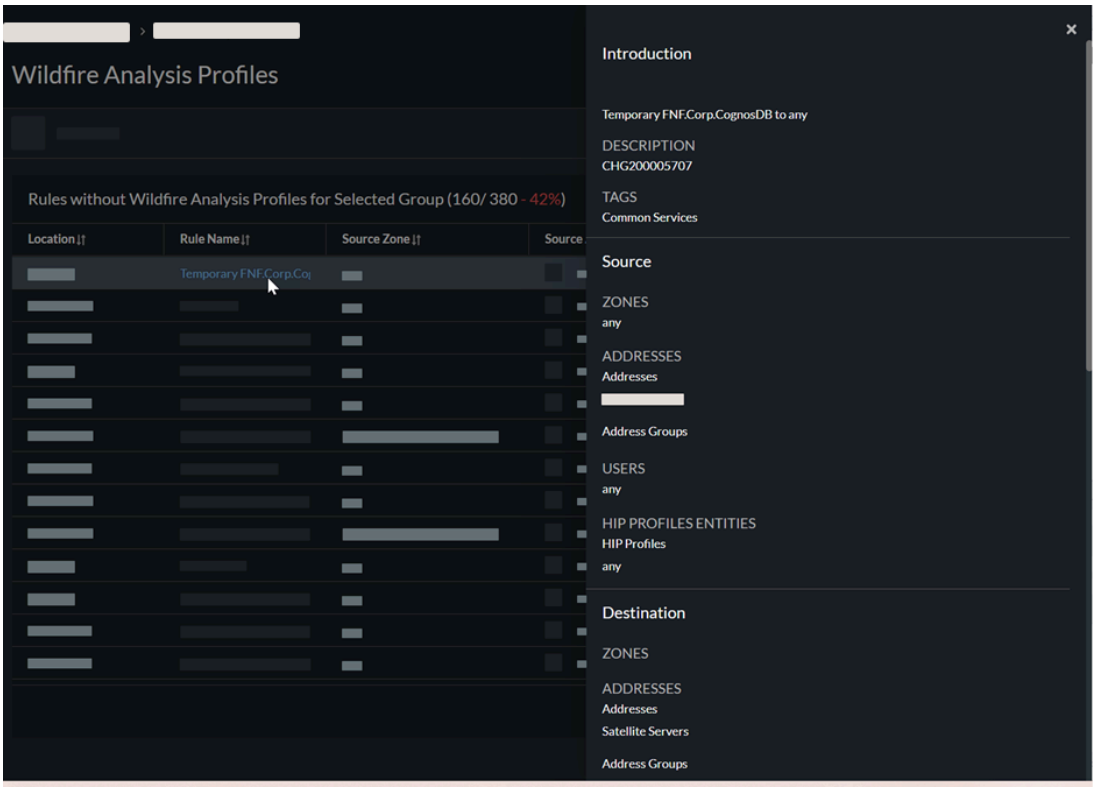
- *Wenn Sie mithilfe einer TSF einen On-Demand-BPA-Bericht generieren, werden die Annahmeinformationen aus Ihrer TSF im Funktionsannahme-Dashboard angezeigt. (TSFs mit PAN-OS 9.1 oder höher)*
- *Sie können Annahmedaten im CSV-Format exportieren, um sie in Anwendungen von Drittanbietern wie Microsoft Excel zu verwenden.*

- Wählen Sie den Abschnitt für eine Funktion im Diagramm aus, um anzuzeigen, bei welchen Richtlinienregeln diese Funktion fehlt.



- Wählen Sie eine Regel aus, um ihre Details anzuzeigen, ohne die App verlassen zu müssen.



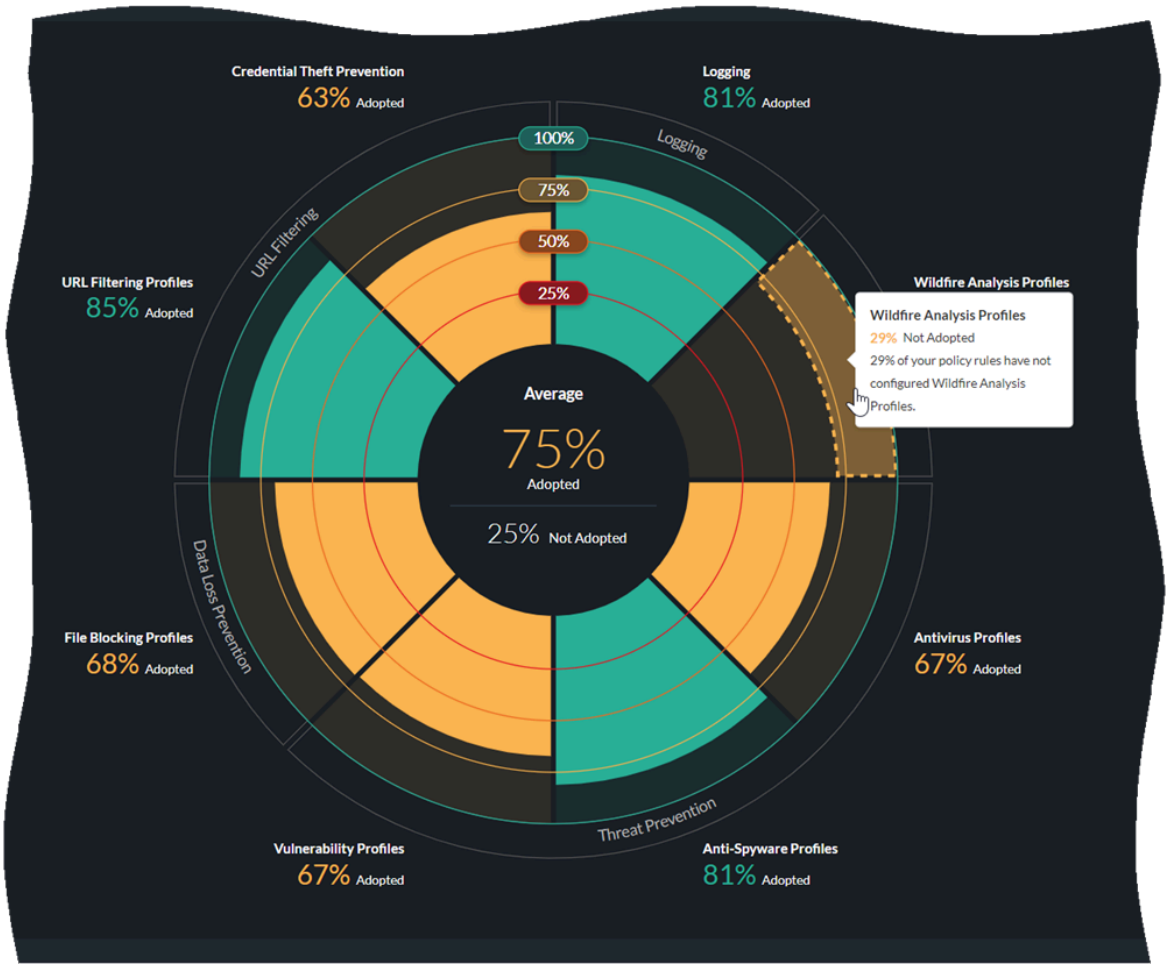

## Identifizieren von Lücken bei der Einführung

Dieses Dashboard zeigt, wo Ihre Sicherheitsrichtlinie stark ist und wo es Lücken bei der Annahme von Funktionen gibt, auf deren Verbesserung Sie sich konzentrieren können. Um maximale Transparenz im Datenverkehr und maximalen Schutz vor Angriffen zu erreichen, legen Sie Ziele für die Annahme von Sicherheitsfunktionen fest und verwenden Sie die folgenden Empfehlungen als Grundlage für Best Practices. Bewerten Sie Ihre aktuelle Situation im Vergleich zur Baseline, um Lücken bei der Umsetzung von Sicherheitsrichtlinien zu identifizieren.

Mithilfe der Annahmeübersicht können Sie Geräte, Zonen und Bereiche identifizieren, in denen Sie die Einführung von Sicherheitsrichtlinien verbessern können. Sie können die Annahmeinformationen nach Gerätegruppe, Seriennummer und Vsys, Zonen, Architekturbereichen, Tags, Regeldetails und Zonenzuordnungen überprüfen. Filtern Sie nach „Gerätegruppe“, um den Umfang einzugrenzen und Lücken zu identifizieren.

Wählen Sie in **Dashboard** > **Funktionsannahme** die Option **Annahme insgesamt** aus, um die Akzeptanzraten der folgenden Funktionen zu überprüfen. Wählen Sie **Best Practices** aus, um die Akzeptanzraten dieser Funktionen anzuzeigen, die den Best Practices von Palo Alto Networks entsprechen. Nutzen Sie diese Informationen als Kriterien, um Lücken zu identifizieren. Wenn die tatsächliche Akzeptanzrate nicht den Empfehlungen entspricht, planen Sie, die Lücke zu schließen:




- Wenden Sie WildFire-Analyse-, Antivirus-, Anti-Spyware-, Sicherheitslücken- und Dateiblockierungsprofile auf alle Regeln an, die Datenverkehr zulassen, mit dem Ziel einer (nahezu) 100-prozentigen Annahme. Wenn Sie ein Profil nicht auf eine Zulassungsregel anwenden, stellen Sie sicher, dass es einen triftigen geschäftlichen Grund dafür gibt, das Profil nicht anzuwenden.

  Durch das Konfigurieren von Sicherheitsprofilen für alle Zulassungsregeln kann die Firewall den entschlüsselten Datenverkehr unabhängig von der Anwendung oder dem Dienst/Port auf Bedrohungen überprüfen. Nachdem Sie die Konfiguration aktualisiert haben, können Sie den BPA-Bericht für Nicht-Telemetriegeräte ausführen, um den Fortschritt zu messen und neue Regeln zu ermitteln, an die keine Sicherheitsprofile angehängt sind.

  *Sie können WildFire-Profile auf Regeln anwenden, ohne über eine WildFire-Lizenz zu verfügen. Die Abdeckung ist hierbei auf PE-Dateien beschränkt, doch dies bietet dennoch nützliche Einblicke in unbekannte schädliche Dateien.*

- Wenden Sie im Anti-Spyware-Profil ein DNS-Sinkhole auf alle Regeln an, um zu verhindern, dass kompromittierte interne Hosts DNS-Abfragen für bösartige und benutzerdefinierte Domänen senden. So können Sie potenziell kompromittierte Hosts identifizieren und verfolgen und Lücken bei der DNS-Überprüfung vermeiden. Durch die Aktivierung eines DNS-Sinkholes wird Ihr Netzwerk geschützt, ohne die Verfügbarkeit zu beeinträchtigen. Deshalb können und sollten Sie es sofort aktivieren.

- Wenden Sie URL-Filterung sowie Schutz vor dem Diebstahl von Anmeldeinformationen (Phishing) auf den gesamten ausgehenden Internetverkehr an.

Überprüfen Sie in der Annahmeübersicht die Zusammenfassung von Anwendungen, Benutzern und Ports, um die Annahmeraten der folgenden Funktionen zu prüfen. Nutzen Sie die Empfehlungen als Kriterien, um Lücken zu identifizieren. Wenn die tatsächliche Akzeptanzrate nicht den Empfehlungen entspricht, planen Sie, die Lücke zu schließen:

- Wenden Sie die Anwendungs-ID auf möglichst 100 % der Regeln an. Wenden Sie die Benutzer-ID auf alle Regeln mit Quellzonen oder Adressbereichen an, in denen ein Benutzer vorhanden ist (einige Zonen verfügen möglicherweise nicht über Benutzerquellen; Quellen in Rechenzentrumszonen sollten beispielsweise Server und keine Benutzer sein). Nutzen Sie die Anwendungs-ID und die Benutzer-ID, um Richtlinien zu erstellen, die entsprechenden Benutzern den Zugriff auf genehmigte (und sanktionierte) Anwendungen ermöglichen. Blockieren Sie bösartige und unerwünschte Anwendungen explizit.
- Streben Sie eine Dienst-/Portannahme von 100 % oder nahezu 100 % an – lassen Sie keine Anwendungen auf nicht standardmäßigen Ports zu, es sei denn, es gibt dafür einen guten geschäftlichen Grund.

Überprüfen Sie in der Protokollierungszusammenfassung der Annahmeübersicht die Annahmeraten der folgenden Funktionen. Nutzen Sie die Empfehlungen als Kriterien, um Lücken zu identifizieren. Wenn die tatsächliche Akzeptanzrate nicht den Empfehlungen entspricht, planen Sie, die Lücke zu schließen:

- Ziel ist eine 100-prozentige oder nahezu 100-prozentige Annahme für Protokollierung und Protokollweiterleitung.
- Konfigurieren Sie Zonenschutzprofile für alle Zonen.

Zusammengefasst:

| Merkmal | Annahmeziel |
|---|---|
| WildFire | Möglichst 100 % der Sicherheitsrichtlinienregeln |
| Antivirus | Möglichst 100 % der Sicherheitsrichtlinienregeln |
| Anti Spyware | Möglichst 100 % der Sicherheitsrichtlinienregeln |
| Sicherheitslücke | Möglichst 100 % der Sicherheitsrichtlinienregeln |
| Dateiblockade | Möglichst 100 % der Sicherheitsrichtlinienregeln |
| URL-Filterung und Schutz vor dem Diebstahl von Anmeldeinformationen | Gesamter ausgehender Internetverkehr |
| App-ID | Möglichst 100 % der Sicherheitsrichtlinienregeln |
| User-ID (Benutzeridentifikation) | Alle Regeln mit Quellzonen oder Adressbereichen, die eine Benutzerpräsenz aufweisen |

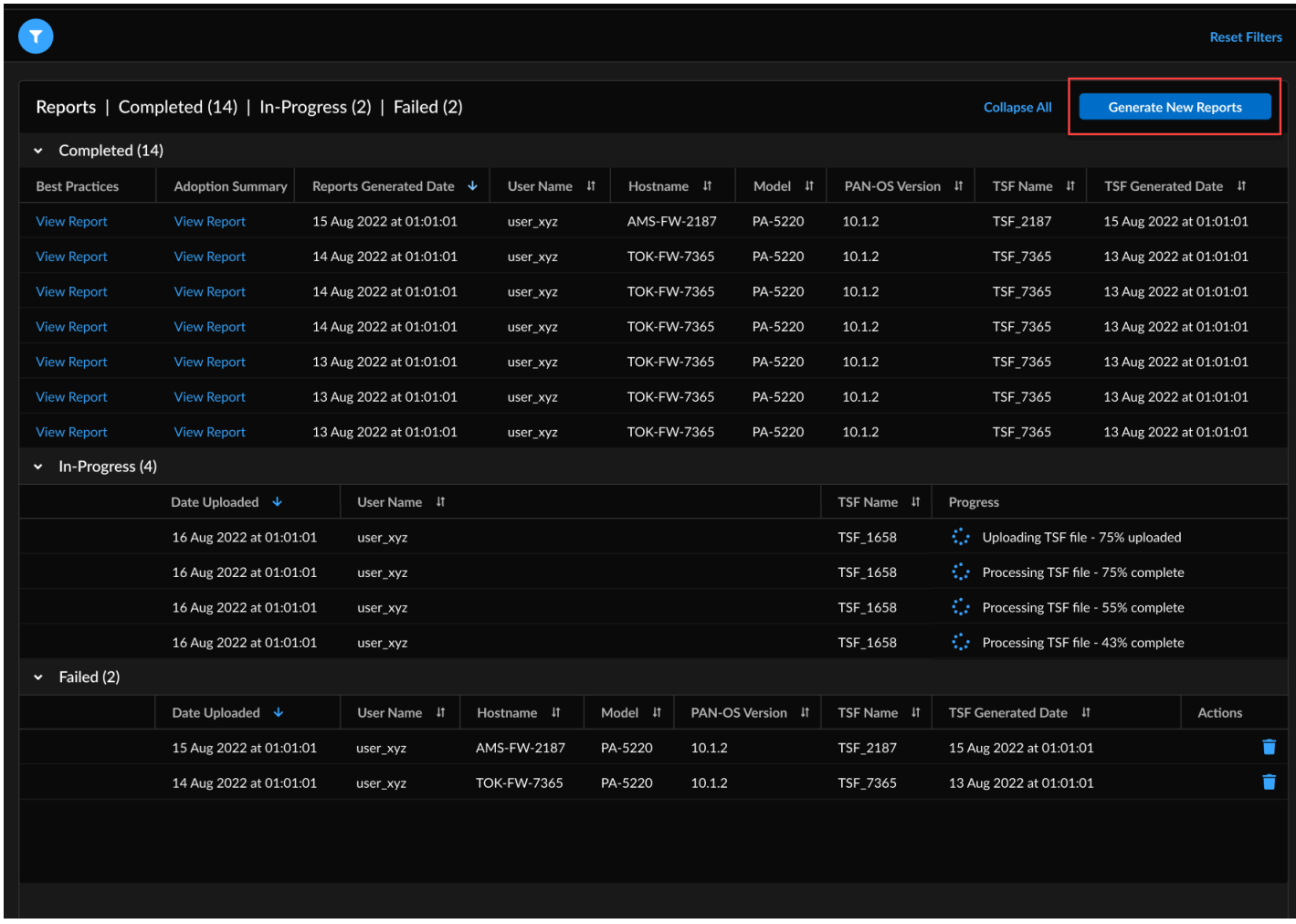
 

| Merkmal | Annahmeziel |
|---|---|
| Dienst/Port | Möglichst 100 % der Sicherheitsrichtlinienregeln |
| Protokollierung | Möglichst 100 % der Sicherheitsrichtlinienregeln |
| Protokollweiterleitung | Möglichst 100 % der Sicherheitsrichtlinienregeln |
| Zonenschutz | Alle Zonen |

# Dashboard: On-Demand-BPA

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | ❑ Strata Cloud Manager Essentials<br>❑ AIOps for NGFW Premium oder Strata Cloud Manager Pro<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

- Gehen Sie zu **Dashboards** > **On-Demand-BPA**, um zu beginnen.



## Was sehen Sie in diesem Dashboard?

*Das Dashboard zeigt den BPA-Bericht (Best Practice Assessment, Best-Practice-Bewertung) an, der auf den hochgeladenen TSF-Dateien von Geräten basiert.*

Sie können nun die BPA und die Funktionsannahmeübersicht direkt über Strata Cloud Manager durchführen bzw. aufrufen. Laden Sie einfach eine Datei für den technischen Support (Tech Support File, TSF) hoch. Sie können den BPA-Bericht auf Abruf für Geräte generieren, die keine Telemetriedaten senden oder nicht in AIOps für NGFW integriert sind.

## Wie können Sie die Daten aus dem Dashboard nutzen?

Bei der BPA wird Ihr Sicherheitsstatus anhand der Best Practices von Palo Alto Networks bewertet und es werden Prioritäten für Verbesserungen der Geräte festgelegt. Sicherheitsrelevante Best Practices verhindern bekannte und unbekannte Bedrohungen, verringern die Angriffsfläche und bieten Einblick in den Datenverkehr, sodass Sie wissen und kontrollieren können, welche Anwendungen, Benutzer und Inhalte sich in Ihrem Netzwerk befinden. Außerdem gehören zu den Best Practices Prüfungen für die Critical Security Controls (CSC) des Center for Internet Security. Sehen Sie sich die Best Practice-Anleitung an, um den Sicherheitsstatus zu stärken und Verbesserungen umzusetzen.

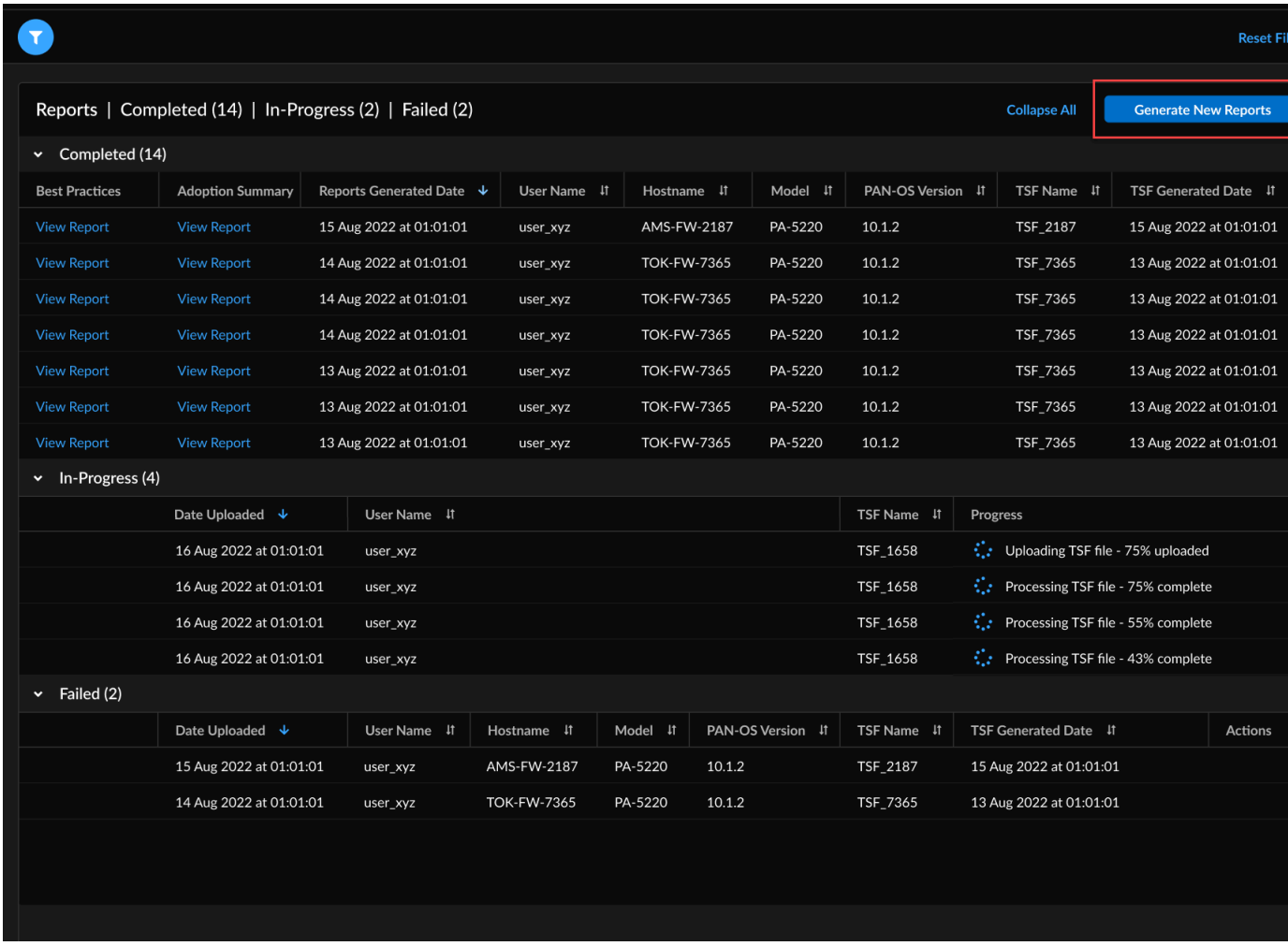
## Generieren eines On-Demand-BPA-Berichts

Führen Sie die folgenden Schritte aus, um den BPA-Bericht bei Bedarf zu generieren.

**STEP 1 |** Gehen Sie zu **Dashboards** > **On-Demand-BPA**.

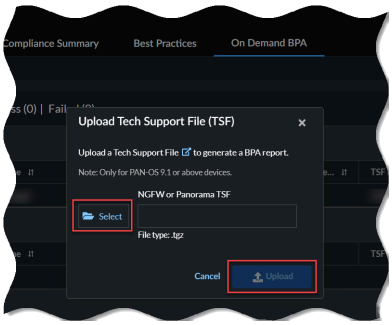
 

## STEP 2 | Generieren Sie einen neuen BPA-Bericht.



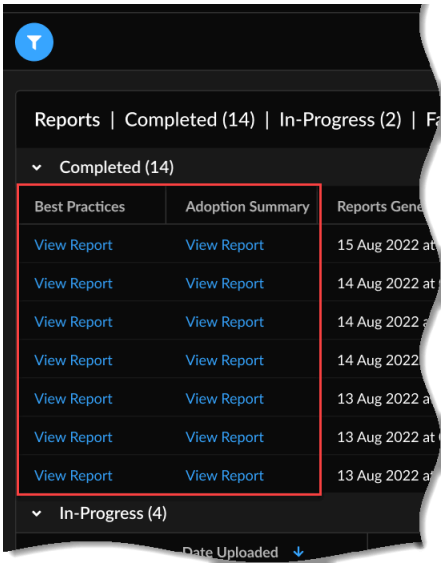
**STEP 3 |** **Wählen Sie die TSF-Datei aus** und **laden Sie die TSF-Datei hoch**.




Die Dauer des Uploads hängt von der Größe Ihrer .tgz-Datei und von Ihrer Internetgeschwindigkeit ab. Bei größeren Dateien kann das Hochladen der Datei einige Minuten dauern. Erweitern Sie **In Bearbeitung**, um den Status der TSF-Dateien anzuzeigen.

- *On-Demand-BPA unterstützt nur die Dateien für den technischen Support (Tech Support Files, TSF) im .tgz-Dateiformat.*
- *On-Demand-BPA unterstützt zur Berichterstellung nur TSF-Dateien von Geräten mit PAN-OS-Version 9.1 oder höher.*
- *Weitere Informationen zur Datenerfassung, -verarbeitung und -speicherung von Palo Alto Networks finden Sie unter* AIOps für NGFW – Datenschutz *im* Trust Center.

**STEP 4 |** Über **Bericht anzeigen** unter **Abgeschlossen** können Sie die Ergebnisse anzeigen.



# Dashboard: SASE-Zustand

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager) | • Eine der folgenden Komponenten:<br>❑ Prisma Access und ADEM-Beobachtbarkeit<br>❑ Strata Cloud Manager Pro<br>• eine Rolle mit der Berechtigung zum Anzeigen des Dashboards<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

## Was sehen Sie in diesem Dashboard?

Dieses Dashboard zeigt Ihnen den Gesamtzustand Ihrer mobilen Benutzer, Remote-Standorte und Anwendungen (wenn Sie eine AI-Powered ADEM-Lizenz besitzen), die derzeit mit Prisma Access verbunden sind. Die Zahlen in den Kreisen repräsentieren die Anzahl der Benutzer oder Websites, die derzeit vom Prisma Access-Standort aus verbunden sind, an dem sie angezeigt werden. Ein Punkt repräsentiert einen einzelnen Benutzer oder einen Standort. Die Bereiche auf der Karte mit blauem Hintergrund zeigen an, dass es sich bei den in dieser Region angezeigten Zahlen um eine Prognose handelt.

Filtern Sie die in diesem Dashboard angezeigten Daten mit einem oder mehreren der folgenden Filter

- Zeitbereich
- Prisma Access-Standort
- Quellort

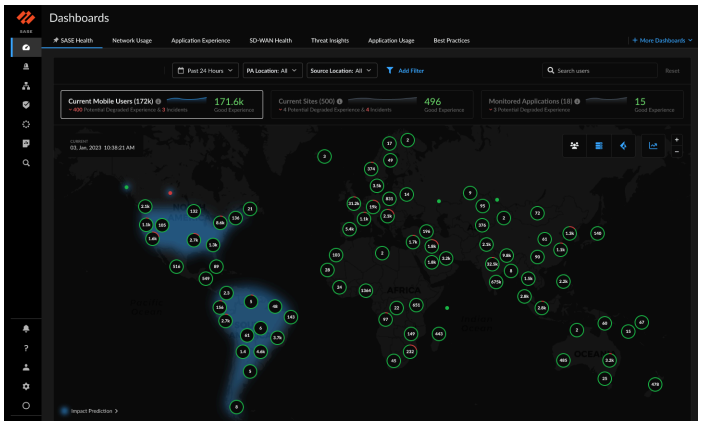
## Wie können Sie die Daten aus dem Dashboard nutzen?

Verwenden Sie das Dashboard, um sich einen allgemeinen Überblick darüber zu verschaffen, wie viele mit Prisma Access verbundene mobile Benutzer und Remote-Standorte nach ihrem Standort auf der Karte kategorisiert sind. Sie können ihren Gesamtzustand auch in diesem Dashboard anzeigen.

# Dashboard „SASE-Zustand“: Aktuelle mobile Benutzer – Kartenansicht

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager) | • Eine der folgenden Komponenten:<br>❑ Prisma Access und ADEM-Beobachtbarkeit<br>❑ Strata Cloud Manager Pro<br>• eine Rolle mit der Berechtigung zum Anzeigen des Dashboards<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Die Registerkarte **Aktuelle mobile Benutzer** im Dashboard **SASE-Zustand** zeigt Ihnen eine Aufschlüsselung der Erfahrung mobiler Benutzer an allen Standorten. Die Zahlen in den Kreisen entsprechen der Anzahl der mobilen Benutzer, die derzeit über GlobalProtect mit Prisma Access verbunden sind. Ein Punkt repräsentiert einen einzelnen Benutzer oder einen Standort. Ein grüner Kreis oder Punkt zeigt einen guten Benutzererfahrungsscore an. Ebenso zeigt ein roter Kreis oder Punkt einen verschlechterten Erfahrungsscore an. Verschlechterte Erfahrungsscores umfassen die Bewertungen „Angemessen“ und „Schlecht“. Das Liniendiagramm rechts neben **Aktuelle mobile Benutzer** zeigt Ihnen einen Trend der durchschnittlichen Erfahrungsscores für alle mobilen Benutzer während des ausgewählten **Zeitbereichs**.



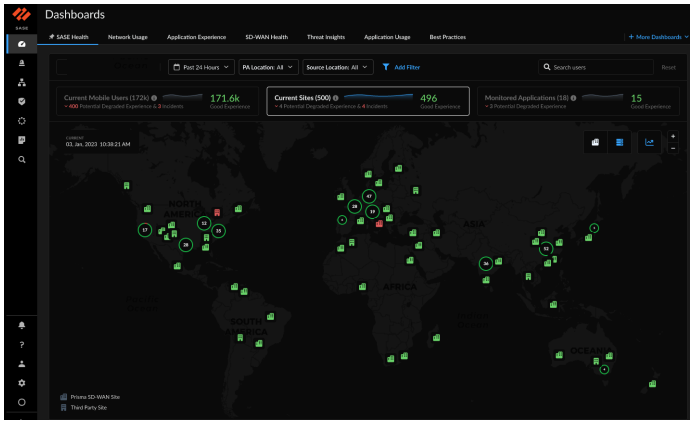

Klicken Sie auf die Zahl (die die Anzahl der Benutzer mit potenziell beeinträchtigter Benutzererfahrung darstellt) neben **Potenziell beeinträchtigte Benutzererfahrung** oder **Vorfälle**, um die Details zur beeinträchtigten Benutzererfahrung in einem Bereich anzuzeigen, der sich links öffnet.

# Dashboard „SASE-Zustand“: Aktuelle Standorte – Kartenansicht

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager) | • Eine der folgenden Komponenten:<br>❑ Prisma Access und ADEM-Beobachtbarkeit<br>❑ Strata Cloud Manager Pro<br>• eine Rolle mit der Berechtigung zum Anzeigen des Dashboards<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Dieses Dashboard zeigt Ihnen die Anzahl der konfigurierten Standorte, die sich mit Prisma Access-Standorten auf der ganzen Welt verbinden. Die in Klammern eingeschlossene Zahl ist die Gesamtzahl der verbundenen Standorte und die Zahl rechts in der Karte ist die Anzahl der Standorte, die gute Erfahrungsscores erhalten. Standorte, deren Erfahrungsscores aus irgendeinem Grund nicht abgerufen werden können, werden bei der Berechnung der Anzahl verbundener Standorte nicht ausgeschlossen. Das blaue Liniendiagramm zeigt den Trend der durchschnittlichen Erfahrungsscores für alle Standorte im Zeitverlauf. Unterhalb der aktuellen Standorte sehen Sie die Anzahl der Standorte mit beeinträchtigter (schlechter) Erfahrung zusammen mit der Anzahl der Vorfälle für alle Standorte. Die Vorfälle können in eine oder mehrere der folgenden Kategorien fallen: Infrastruktur, Netzwerkdienste, Rechenzentren und Drittanbieterstandorte (Rechenzentren ausgefallen).

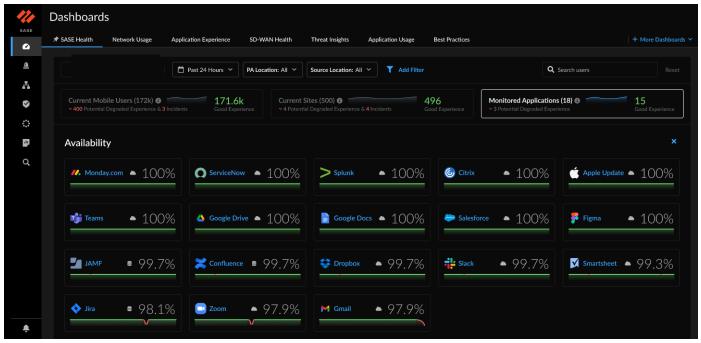


# Dashboard „SASE-Zustand“: Überprüfte Anwendungen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager) | • Eine der folgenden Komponenten:<br>❑ Prisma Access und ADEM-Beobachtbarkeit<br>❑ Strata Cloud Manager Pro<br>• eine Rolle mit der Berechtigung zum Anzeigen des Dashboards<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Sehen Sie sich die Metriken zur Anwendungsverfügbarkeit auf der Registerkarte **Überprüfte Anwendungen** des Dashboards **SASE-Zustand** an. Dieses Dashboard zeigt Ihnen, wie viele Anwendungen durch ADEM überwacht werden und wie viele davon eine beeinträchtigte Bewertung aufweisen. Diese Zahl berücksichtigt die Anwendungserfahrung sowohl für mobile Benutzer als auch für Remote-Standorte. Anwendungen mit schlechten oder angemessenen Anwendungserfahrungsscores gelten als „Anwendungen mit beeinträchtigter Erfahrung“. Sie können sich außerdem die Verfügbarkeit der Anwendung in dem Zeitbereich anzeigen lassen, den Sie per Filter auswählen.




Die Zahl rechts neben dem Anwendungsnamen gibt den Prozentsatz des ausgewählten **Zeitbereichs** an, in dem die Anwendung verfügbar war.

# Überwachen: Strata Cloud Manager

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden<br>• Prisma SD-WAN | Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>❑ Prisma Access<br>❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>❑ Strata Cloud Manager Essentials<br>❑ Strata Cloud Manager Pro<br>❑ Prisma SD-WAN<br>Weitere für Sichtbarkeit erforderliche Lizenzen und Voraussetzungen:<br>❑ ADEM-Beobachtbarkeit<br>❑ Autonomous DEM für Remote-Netzwerke<br>❑ KI-gestütztes ADEM<br>❑ WAN Clarity-Berichterstattung<br>❑ eine Rolle mit der Berechtigung zum Anzeigen des Dashboards<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Verschaffen Sie sich einen umfassenden Überblick über Ihren Netzwerkverkehr und die Produkte und Abonnements, die Sie mit Strata Cloud Manager verwalten. Sie können den Zustand und den Konnektivitätsstatus Ihrer Remote-Netzwerke, Anwendungen, NGFW-Geräte und mobilen Benutzer in Prisma Access schützend überwachen. Strata Cloud Manager bietet auch Funktionen zur Überwachung der Leistung gängiger Netzwerkdienste, Informationen zur Nutzung Ihrer Abonnementlizenzen sowie Funktionen zur Verwaltung des Tools, das zur Analyse von Verbindungsproblemen verwendet wird. Prisma SD-WAN-Benutzer können hier auch zentral den Zustand und den Konnektivitätsstatus von Prisma SD-WAN-Anwendungen, ION-Geräten und Rechenzentren überwachen.

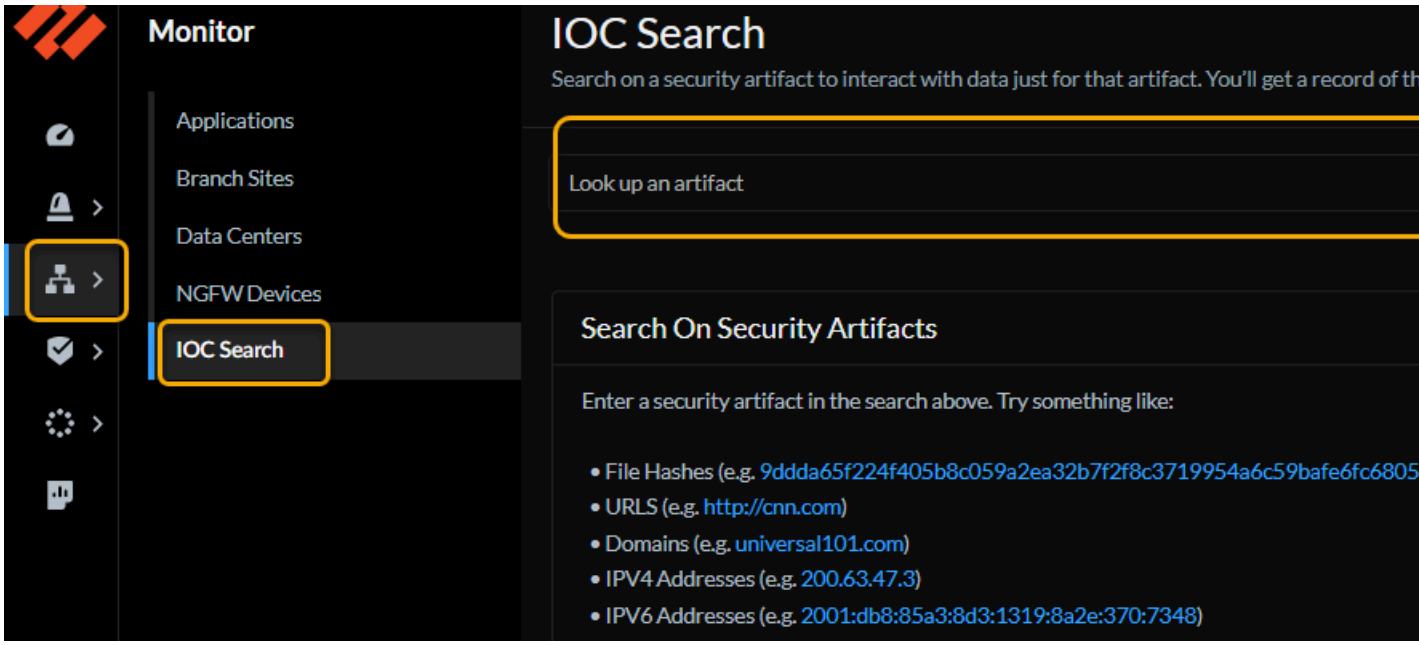
# Überwachen: IOC-Suche

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden<br>• Prisma SD-WAN | Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>❑ Prisma Access<br>❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>❑ Strata Cloud Manager Essentials<br>❑ Strata Cloud Manager Pro<br>❑ Prisma SD-WAN<br>Weitere für Sichtbarkeit erforderliche Lizenzen und Voraussetzungen:<br>❑ ADEM-Beobachtbarkeit<br>❑ Autonomous DEM für Remote-Netzwerke<br>❑ KI-gestütztes ADEM<br>❑ WAN Clarity-Berichterstattung<br>❑ eine Rolle mit der Berechtigung zum Anzeigen des Dashboards<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Sie können ein Sicherheitsartefakt durchsuchen, um mit Daten nur für dieses Artefakt zu interagieren. Zu den Suchergebnissen gehören:

- Der Verlauf und die Aktivität des Artefakts in Ihrem Netzwerk. *Bewerten Sie, wie weit verbreitet das Artefakt in Ihrem Netzwerk ist, und vergleichen Sie es mit Branchenkollegen.*
- Bedrohungsdaten von Palo Alto Networks zum Artefakt, basierend auf der Analyse des gesamten Datenverkehrs, den Palo Alto Networks verarbeitet und analysiert.
- Konsolidierte Analyseergebnisse Dritter für das Artefakt.

Klicken Sie auf **Überwachen** > **IOC-Suche**, um zu beginnen.



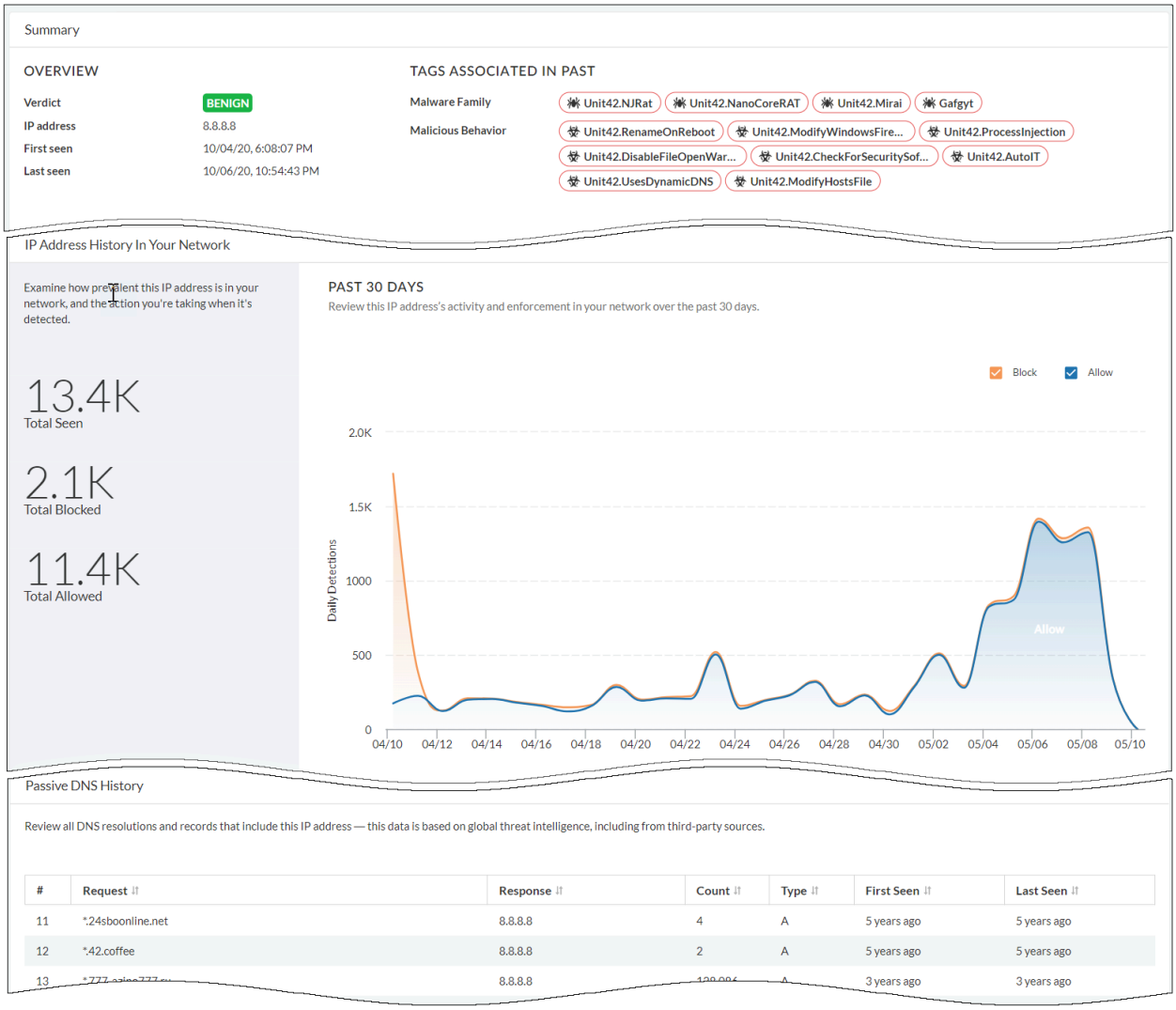

Suchen Sie zunächst nach einem dieser Artefakttypen: einem **Datei-Hash**, einer **URL**, einer **Domäne** oder einer **IP-Adresse** (IPv4 oder IPv6).

## IP-Adresse

Sie können nach einer IP-Adresse suchen, um die Bedrohungsinformationen im Zusammenhang mit IP-Adressaktivitäten in Ihrem Netzwerk zu analysieren. Im Suchergebnis werden folgende Daten angezeigt:

- Gesamtzahl der Erkennungen einer IP-Adresse in Ihrem Netzwerk in den letzten 30 Tagen
- grafische Darstellung der für die IP-Adresse ausgeführten Aktion (Zulassen oder Blockieren)
- Liste der DNS-Anfragen, die die IP-Adresse enthalten, basierend auf den Bedrohungsdaten von Palo Alto Networks und Quellen von Drittanbietern

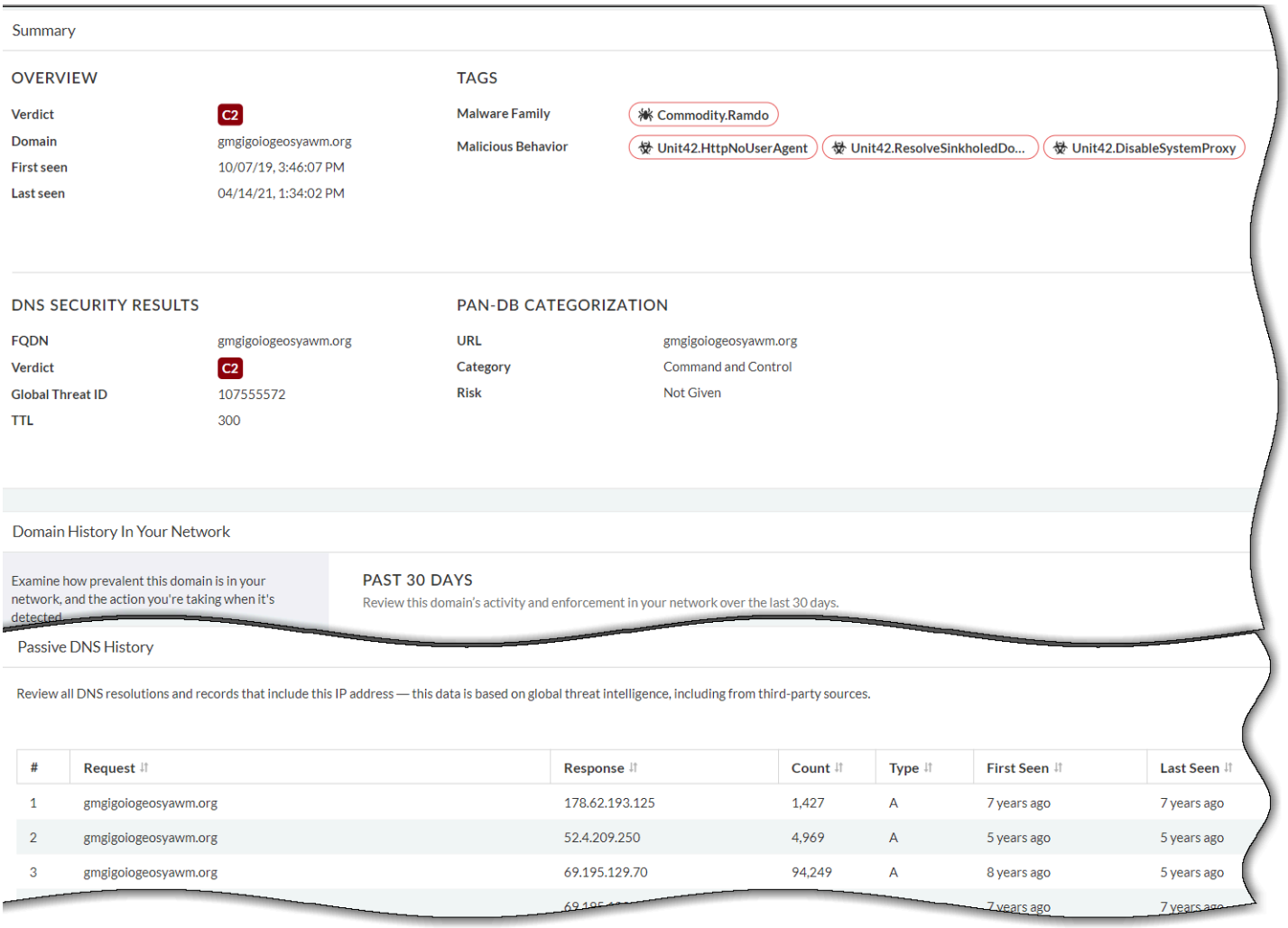



# Domäne

Zeigen Sie eine Zusammenfassung der mit der Domäne in Ihrem Netzwerk verbundenen Aktivitäten an. Die Suchergebnisse umfassen:

- Klassifizierung der Domäne in Ihrem Netzwerk basierend auf der WildFire-Stichprobenanalyse
- Gesamtzahl der mit der Domäne verbundenen Aktivitäten in den letzten 30 Tagen
- Durchsetzung, die auf die einzelnen Aktivitäten angewendet wurde, in einem grafischen Format
- Informationen aus der WildFire-Analyse, die die Daten unterstützen, mit denen das Urteil für die Domäne erstellt wurde
- DNS-Aktivität, die aus allen WildFire-Übermittlungen erfasst wurde, die Instanzen dieser Domäne enthalten

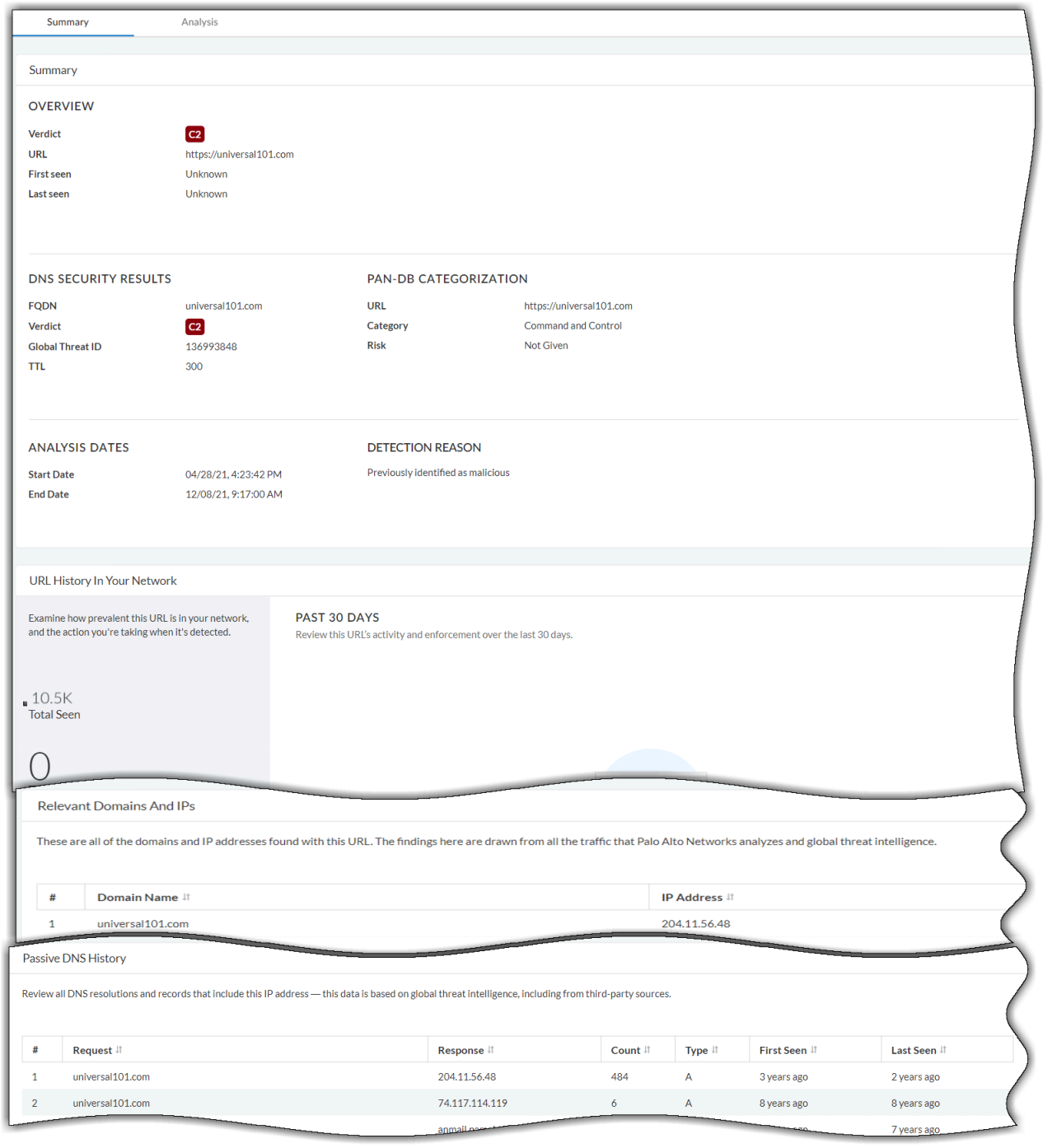



# URL

Informieren Sie sich über die URL-Aktivität im gesamten von Palo Alto Networks analysierten Datenverkehr. Die Suchergebnisse umfassen:

**Zusammenfassung** – Hier finden Sie eine Zusammenfassung der URL-Aktivität in Ihrem Netzwerk. Zu den Daten zählen: DNS-Sicherheitsergebnisse für die URL und die PAN-DB-Kategorisierung.

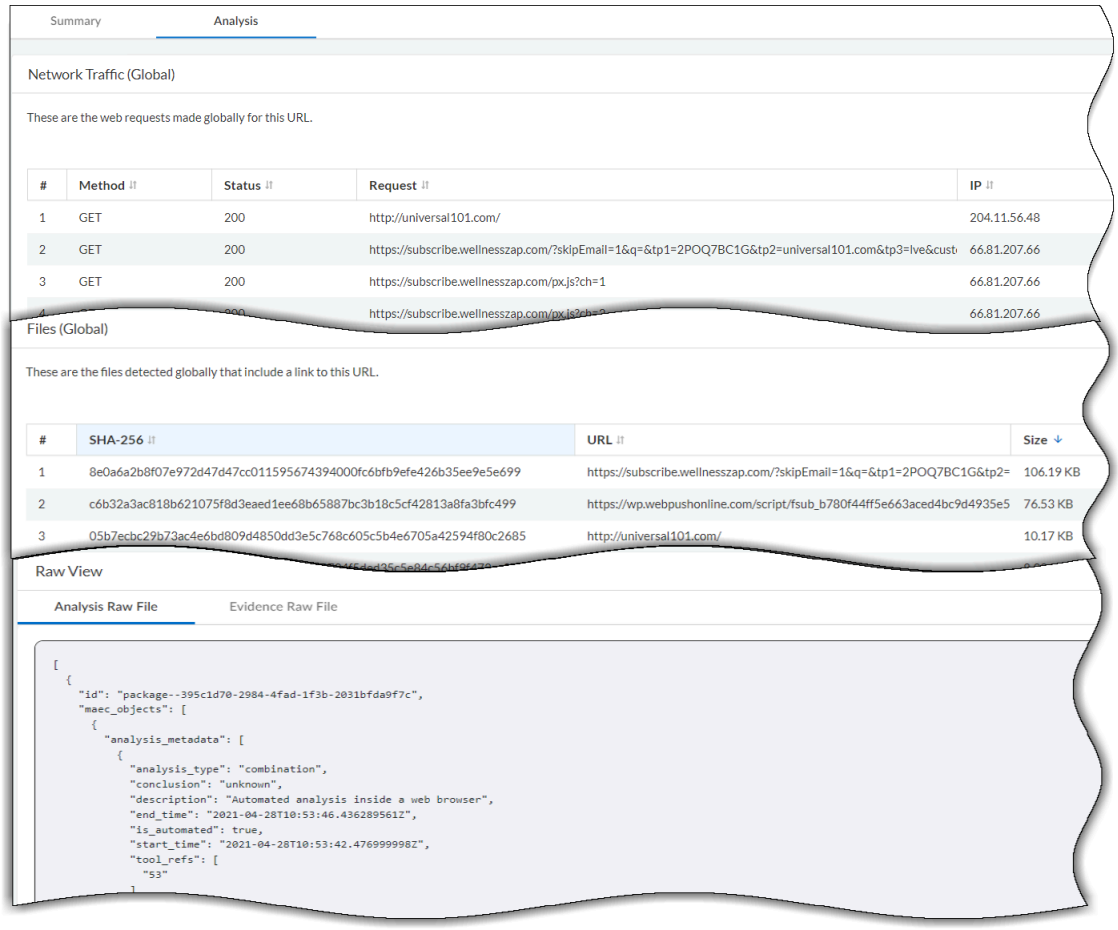
 




**Screenshot** – zeigt einen Screenshot der Website an, wenn Sie nach einem URL-Artefakt suchen.

**Analyse** – Sehen Sie sich die Dateianalysedaten an, einschließlich der Anfragen, die global für diese URL gestellt wurden, sowie der mit dieser URL erkannten Dateien. Sie können den Datei-Hashwert oder die Dateiansicht verwenden, um mehr zu erfahren.

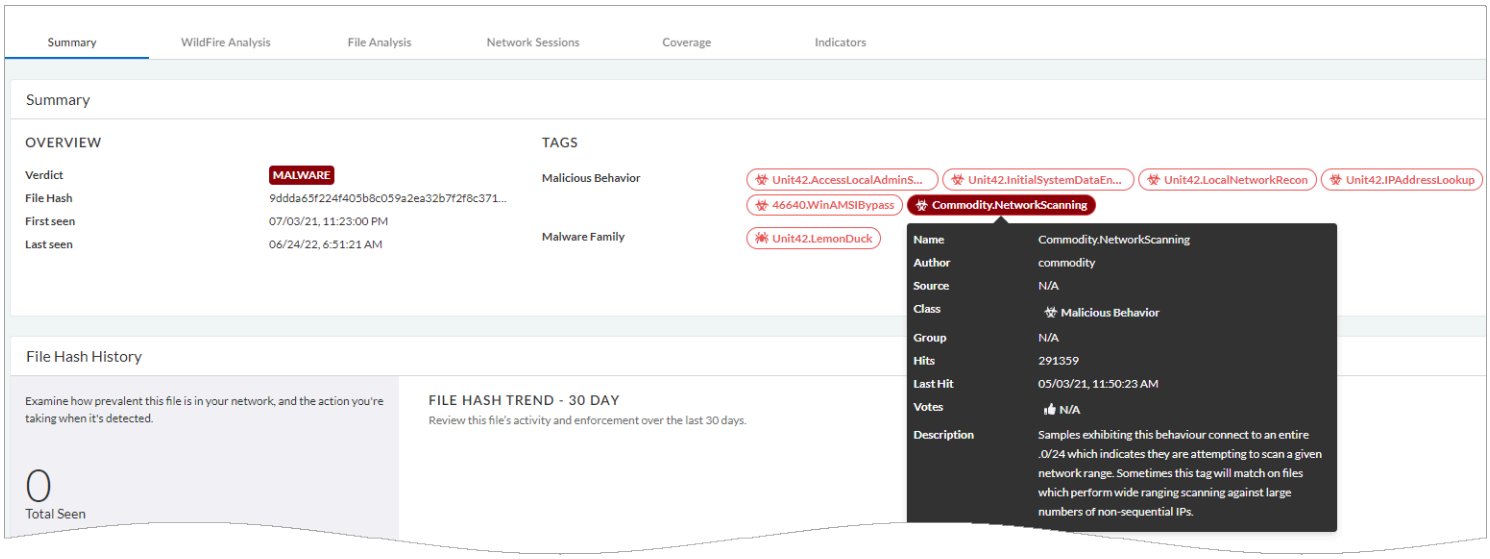



# Datei-Hash

Die Datei-Hash-Suche fasst die Dateiaktivität, die Analyse der Dateieigenschaften sowie Details aus der WildFire-Stichprobenanalyse zusammen. Sie können im Suchergebnis detaillierte Informationen anzeigen, um die folgenden Daten zu überprüfen:

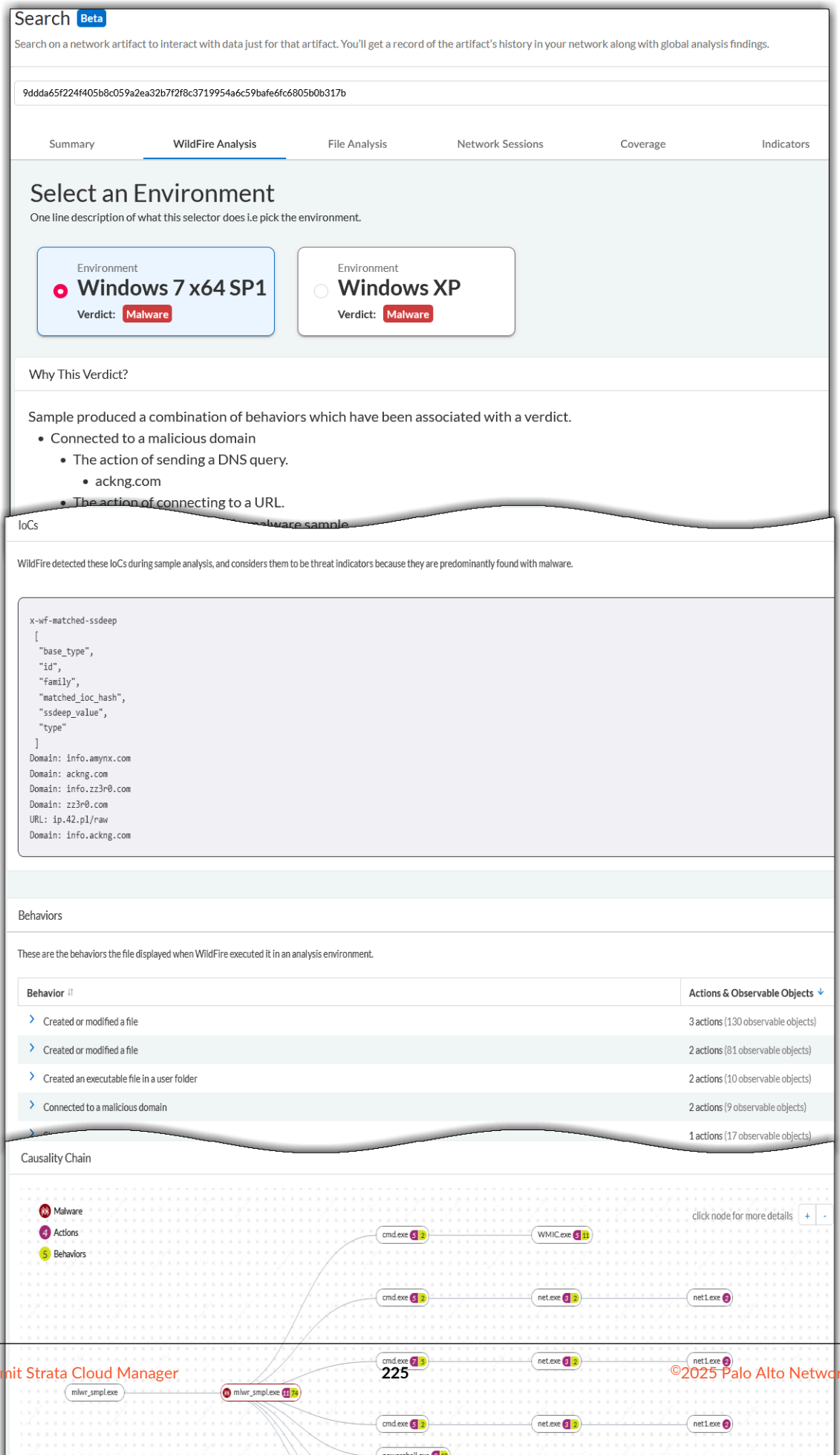
**Zusammenfassung** – Zeigen Sie das Datei-Hash-Urteil und den Verlauf der Dateiaktivität in Ihrem Netzwerk an. Klicken Sie auf den Tag-Namen, um die Details des Tags anzuzeigen. Mithilfe von Tags können Sie erkennen, ob die Datei zu einer Bedrohungsfamilie, einer Bedrohungskampagne oder einem bestimmten Angreifer gehört.




**WildFire-Analyse** – Bewerten Sie, wie sich die Stichprobe (Datei) während der WildFire-Analyse verhalten hat. Sie können Informationen zum Stichprobenurteil, zu den während der Stichprobenanalyse erkannten Bedrohungsindikatoren sowie zum Verhalten während der Verarbeitung der Stichprobe in der Analyseumgebung anzeigen. Sie können sich auch die Screenshots der verschiedenen Prozessmeilensteine ansehen, die während der WildFire-Stichprobenanalyse erstellt wurden.

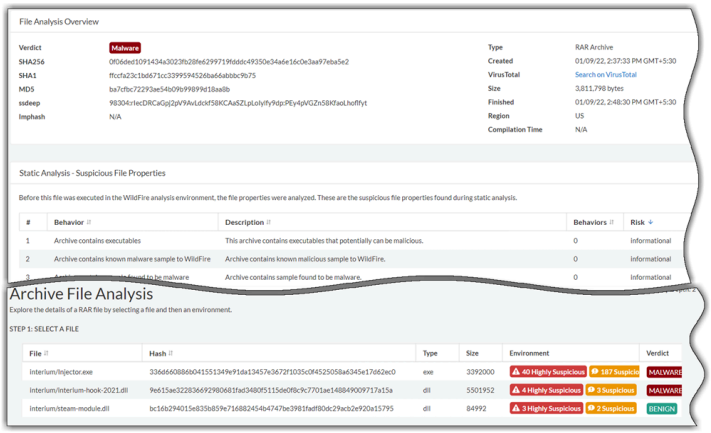
 



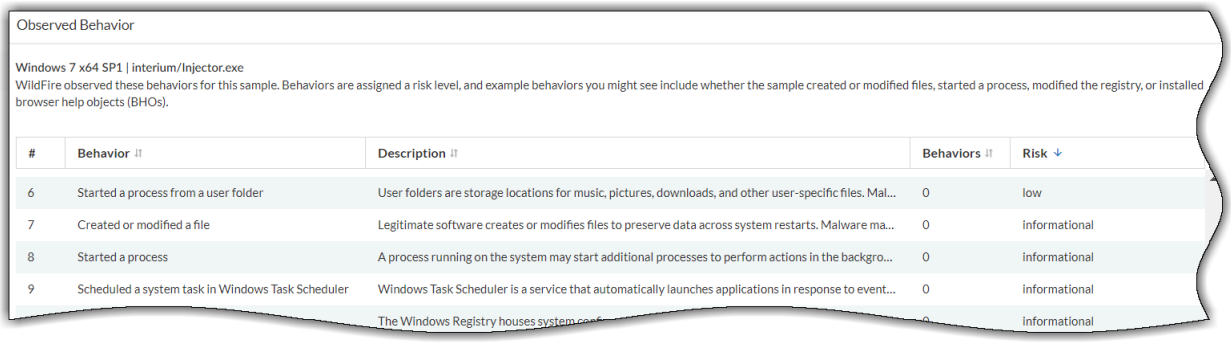
**Dateianalyse** – Vergleichen Sie die Analyse vor und nach der Ausführung der Stichprobe (Datei) in der WildFire-Analyseumgebung.

**Übersicht** – Sehen Sie sich hier das Urteil zur Stichprobe an. Bei falscher Einordnung des Urteils können Sie eine Urteilsänderung anfordern. Das Bedrohungsteam von Palo Alto Networks untersucht die Stichprobe weiter und aktualisiert das Urteil, wenn es sich als falsch herausstellt.


**Statische Analyse** – Bei der statischen Analyse wird der Inhalt einer bestimmten Datei untersucht, bevor die Datei in der WildFire-Analyseumgebung ausgeführt wird. Die Suche zeigt auch die verdächtigen Dateieigenschaften an, die während der statischen Analyse gefunden wurden. Das Suchergebnis variiert je nach Dateityp. Der Screenshot hier zeigt eine statische Analyse für eine Archivdatei.

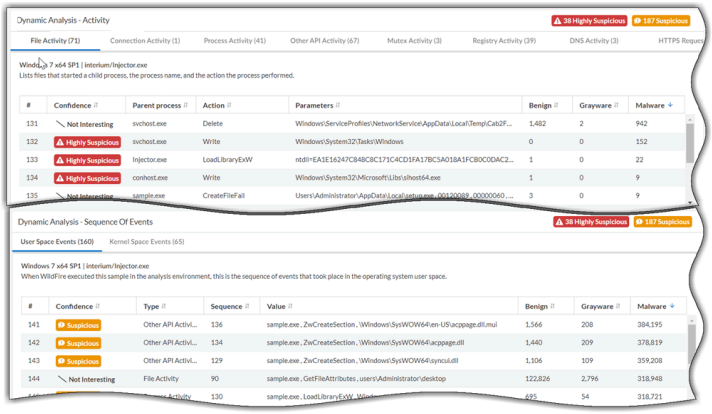



**Beobachtetes Verhalten** – Überprüfen Sie die WildFire-Verhaltensanalyse der Stichprobe in einer bestimmten Umgebung.

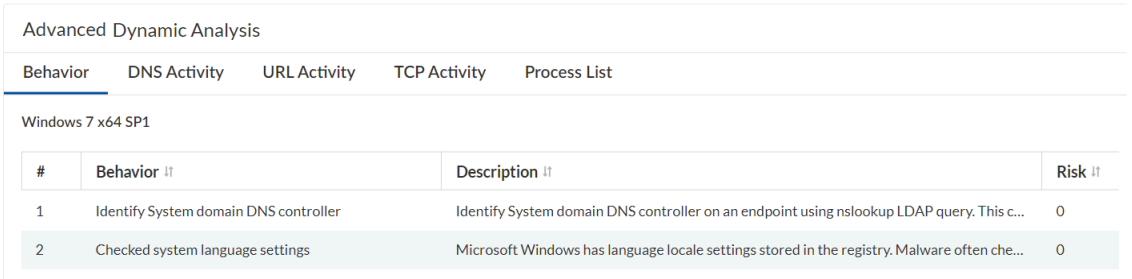


**Dynamische Analyse** – untersucht die Datei im Detail und extrahiert zusätzliche Informationen und Indikatoren eines kompromittierten Netzwerks. Sie können die beteiligten Prozessaktivitäten und die Ereignisfolge überprüfen, die während der Ausführung der Datei in Ihrem System stattgefunden haben.



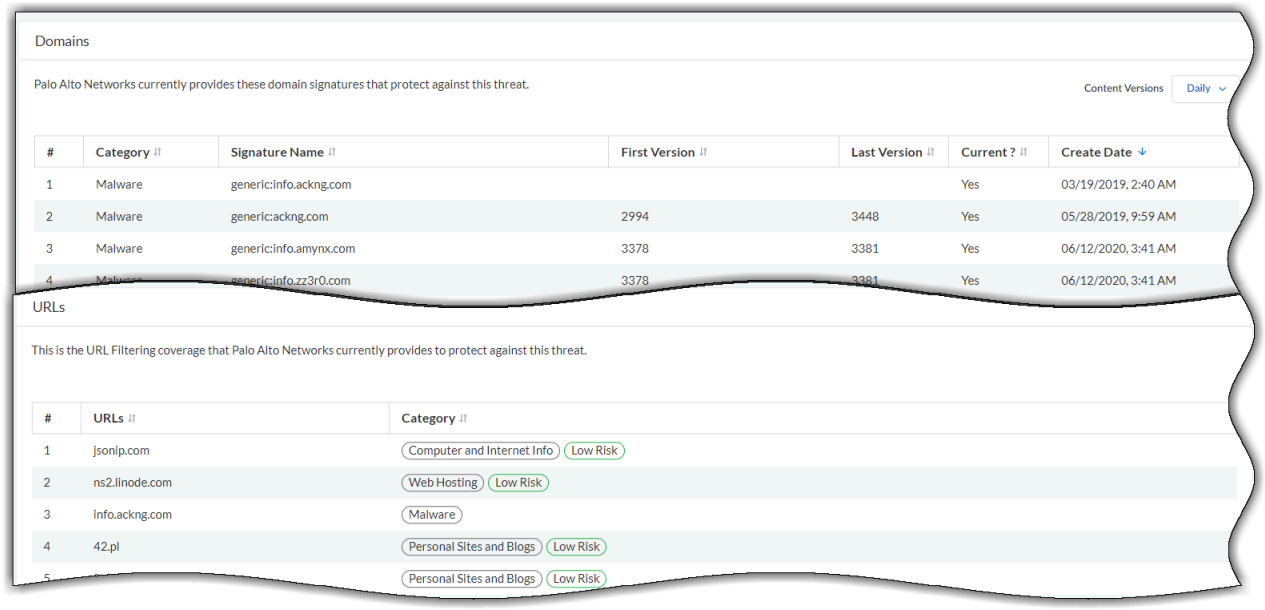

**Fortgeschrittene dynamische Analyse** – Zeigen Sie die Analyseergebnisse von Stichproben an, die mit erweiterten WildFire-Techniken (intelligente Laufzeitspeicheranalyse, dynamische Hypervisor-Analyse, Abhängigkeitsemulation usw.) analysiert wurden. Diese cloudbasierte Engine erkennt und verhindert hochgradig invasive Malware-Bedrohungen. Sie können das beobachtete Verhalten anzeigen und diese Informationen für die Analyse nach der Ausführung verwenden.




**Netzwerksitzungen** – Erfahren Sie mehr über die Netzwerksitzung einer Stichprobe. Nutzen Sie diese Daten, um mehr über den Kontext der Bedrohung zu erfahren und die betroffenen Hosts und Clients sowie die zum Verteilen der Malware verwendeten Anwendungen zu ermitteln.

**Abdeckung** – Überprüfen Sie die Signaturabdeckung einer Stichprobe, um den Bedrohungsschutz zu beurteilen. Sie können die Signaturen anzeigen, die den Domänen zugeordnet sind, von denen die Stichprobe heruntergeladen wurde, sowie die URLs, auf die aus der Stichprobe zugegriffen wird.




**Indikatoren** – Zeigen Sie die Artefakte an, die Indikatoren für ein bestehendes Netzwerk darstellen. Die Indikatoren werden basierend auf den Artefakttypen kategorisiert: Domäne, IP-Adresse, URL, User-Agent-Header sowie Objekte für gegenseitigen Ausschluss. Artefakte mit hohem Risiko werden als „Verdächtig“ oder „Äußerst verdächtig“ gekennzeichnet.

Domain

2 Highly Suspicious 4 Suspicious 4 Interesting

These domains - seen when this sample was executed in the WildFire analysis environment - are predominantly found with malware, and can indicate a compromised network.

| # | Confidence | Indicator | Matching Indicators | Benign | Grayware | Malware |
|---|---|---|---|---|---|---|
| 1 | Highly Suspicious | info.ackng.com | | 0 | 0 | 234 |
| 2 | Highly Suspicious | 42.pl | | 97 | 5 | 499 |
| 3 | Suspicious | ns3.epik.com | | 555 | 43 | 28,611 |
| | | | | | 44 | 28,595 |

IPv4

1 Highly Suspicious 2 Suspicious

These IP addresses - seen when this sample was executed in the WildFire analysis environment - are predominantly found with malware, and can indicate a compromised network.

| # | Confidence | Indicator | Matching Indicators | Benign | Grayware | Malware |
|---|---|---|---|---|---|---|
| 1 | Highly Suspicious | 88.214.207.96 | | 30 | 1 | 277 |
| 2 | Suspicious | 127.0.0.1 | | 273,674 | 891,030 | 7,528,431 |
| | | | | | 8 | 562 |

URL

1 Highly Suspicious 4 Interesting

These URLs - seen when this sample was executed in the WildFire analysis environment - are predominantly found with malware, and can indicate a compromised network.

| # | Confidence | Indicator | Matching Indicators | Benign | Grayware | Malware |
|---|---|---|---|---|---|---|
| 1 | Highly Suspicious | /e.png?id= | | 0 | 0 | 233 |
| 2 | Suspicious | ip.42.pl/raw | | 104 | 7 | 507 |
| 3 | Interesting | zz3r0.com/e.png?id=GVZ823834177364.GVZ823834177364.local&ma... | | -- | -- | -- |
| | | | | | -- | -- |

User Agent

1 Suspicious

These user agent headers - seen for HTTP requests that were sent when this sample was executed in the WildFire analysis environment - are predominantly found with malware, and can indicate a compromised network.

| # | Confidence | Indicator | Matching Indicators | Benign | Grayware | Malware |
|---|---|---|---|---|---|---|
| 1 | Suspicious | Python-urllib/2.7 | | 5,162 | 26,246 | 54,432 |

Mutex

5 Interesting

A mutex (mutual exclusion object) allows programs to share the same resource, though the resource cannot be used by more than one program simultaneously. These mutexes are predominantly found with malware, and can indicate a compromised network.

| # | Confidence | Indicator | Matching Indicators | Benign | Grayware | Malware |
|---|---|---|---|---|---|---|
| 1 | Interesting | testmutex_{D0E858DF-985E-4907-B7FB-8D732C3FC3B9} | | 1 | 0 | 0 |
| 2 | Interesting | Local\c:!users!jgs9ctxe4sno!appdata!roaming!microsoft!windows!cookies! | | -- | -- | -- |
| | | | | | -- | -- |

# Überwachen: Zweigstellen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden<br>• Prisma SD-WAN | Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>❑ Prisma Access<br>❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>❑ Strata Cloud Manager Essentials<br>❑ Strata Cloud Manager Pro<br>❑ Prisma SD-WAN<br>Weitere für Sichtbarkeit erforderliche Lizenzen und Voraussetzungen:<br>❑ ADEM-Beobachtbarkeit<br>❑ Autonomous DEM für Remote-Netzwerke<br>❑ KI-gestütztes ADEM<br>❑ WAN Clarity-Berichterstattung<br>❑ eine Rolle mit der Berechtigung zum Anzeigen des Dashboards<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

**Zweigstellen: Prisma Access**

Wählen Sie **Überwachen** > **Zweigstellen** > **Prisma Access** aus, um den Zustand und die Konnektivität Ihrer Remote-Netzwerke sowie die Nutzung all Ihrer Remote-Netzwerke anzuzeigen, die an verschiedenen Prisma Access-Standorten bereitgestellt werden. Hier sehen Sie den Echtzeit-Konnektivitätsstatus, Details zum Bandbreitenverbrauch sowie andere Bereitstellungsdetails. Mobile Benutzer, Zweigstellen und Einzelhandelsstandorte stellen eine Verbindung zu Remote-Netzwerken her. Sie können auch den Zustand der Tunnel anzeigen, die für Ihre Remote-Netzwerke und mobilen Benutzer konfiguriert sind.

Zusätzlich zu den Widgets, die mit der Prisma Access-Lizenz angezeigt werden, zeigt dieses Dashboard auch den Standort-Erfahrungsscore sowie Prisma SD-WAN-Zweigestellendetails an, sofern Sie über die ADEM Observability- oder AI-Powered ADEM-Lizenz verfügen.

**Zweigstellen: Prisma SD-WAN**

Wählen Sie **Überwachen** > **Zweigstellen** > **Prisma SD-WAN** aus, um eine Zweigstelle in Prisma SD-WAN einzurichten. Zu den Zweigstellen gehören Zweigstellen, die in Ihrem WAN in Prisma SD-WAN enthalten sind. Sie können eine Zweigstelle einrichten, bevor oder nachdem die

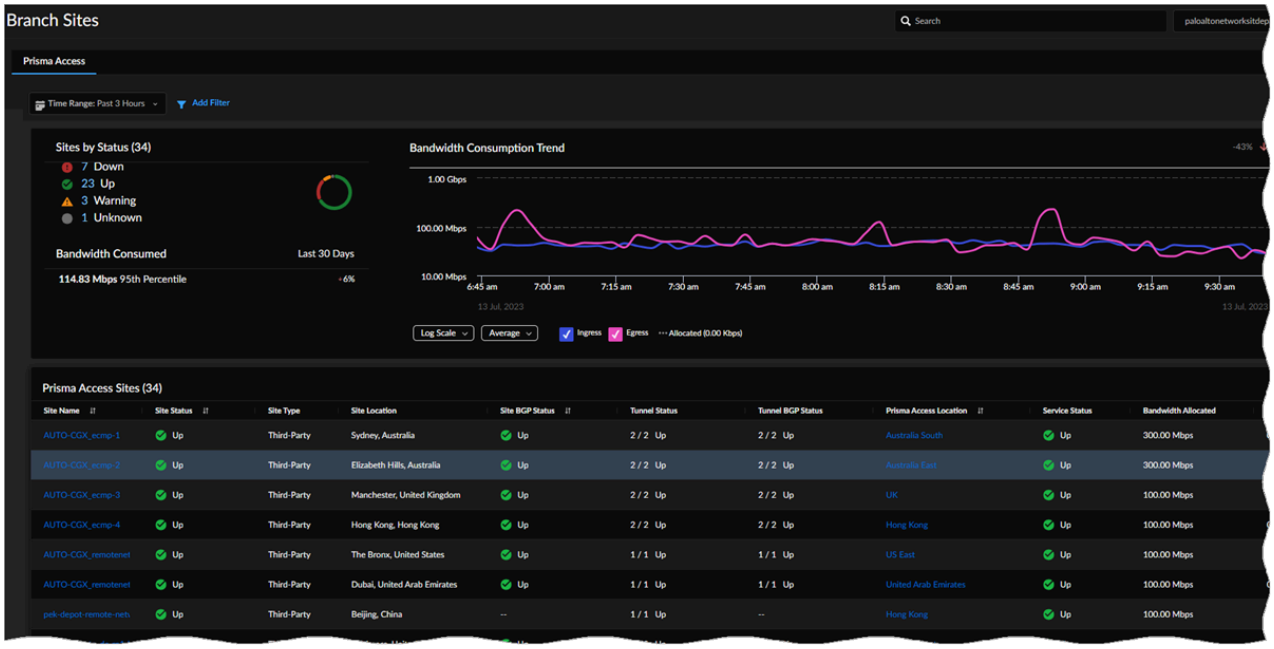
 

ION-Geräte an einem bestimmten Standort eintreffen. Die Zweigstelle in Prisma SD-WAN bietet die folgenden Ansichten:

- Die **Kartenansicht** der Zweigstelle zeigt den Konnektivitätsstatus zwischen Zweigstellengeräten und Controller sowie den Alarmstatus für die Zweigstelle.
- Die **Listenansicht** zeigt Ihnen, wie viele Standorte während des ausgewählten **Zeitbereichs** aktiv waren, und zeigt die allgemeinen Integritätsmetriken der Zweigstellen.
- In der **Aktivitätsansicht** werden wichtige Anwendungsanalysen, der aktuelle Standortzustandsscore sowie die Verteilung des Standortzustands im Zeitverlauf angezeigt.
- Prisma Access
- Prisma SD-WAN

## Zweigstellen (Prisma Access)

Wählen Sie **Zweigstellen** > **Prisma Access** aus, um den Zustand und die Konnektivität Ihrer Remote-Netzwerke sowie die Nutzung all Ihrer Remote-Netzwerke anzuzeigen, die an verschiedenen Prisma Access-Standorten bereitgestellt werden.




Hier sehen Sie den Echtzeit-Konnektivitätsstatus, Details zum Bandbreitenverbrauch sowie andere Bereitstellungsdetails. Mobile Benutzer, Zweigstellen und Einzelhandelsstandorte stellen eine Verbindung zu Remote-Netzwerken her. Sie können auch den Zustand der Tunnel anzeigen, die für Ihre Remote-Netzwerke und mobilen Benutzer konfiguriert sind. Eine ausführliche Beschreibung dieser Widgets finden Sie unter Anzeigen und Überwachen von Zweigstellen.

Mögliche Aktionen:

- Zeigen Sie Ihre Remote-Netzwerkstandorte nach Status an.
- Zeigen Sie Trends im Bandbreitenverbrauch von Remote-Netzwerken an.
- Sehen Sie sich Ihre Prisma Access-Standorte an und wählen Sie einen beliebigen Standort aus, um weitere Details anzuzeigen.

- Öffnen Sie **Details zur Nutzung des IPSec-Terminierungsknotens** aus, um die Details zum Bandbreitenverbrauch jedes SPN am Standort anzuzeigen.
- Zeigen Sie Tunneldaten und Tunneltrends für einen Standort an.
- Zeigen Sie Informationen zum Standortstatus, zum Standortzustand, zur Standortkonnektivität und zum Standortverbrauch an.

## Zweigstellen (Prisma SD-WAN)

Sie können eine Zweigstelle einrichten, bevor oder nachdem die ION-Geräte an einem bestimmten Standort eintreffen. Die Zweigstelle in Prisma SD-WAN bietet die folgenden Ansichten:

- In der **Kartenansicht** der Zweigstelle finden Sie den Konnektivitätsstatus zwischen Zweigstellengeräten und Controller sowie den Alarmstatus für die Zweigstelle. Wenn eine Zweigstelle ausgewählt wird, werden folgende Informationen angezeigt:
  - Standortzusammenfassung: wird für Analysen und Fehlerbehebung verwendet.
  - Konfigurationen: wird für die Standort- und Gerätekonfiguration verwendet.
  - Overlay-Verbindungen: wird verwendet, um den Status aller VPN-Overlay-Verbindungen anzuzeigen.
- Die **Listenansicht** zeigt Ihnen, wie viele Standorte während des ausgewählten **Zeitbereichs** aktiv waren, und zeigt die allgemeinen Integritätsmetriken der Zweigstellen. Der durchschnittliche Score eines schlechten Standorts ist der Durchschnitt aller schlechten Stichproben von Standorten, die als schlecht identifiziert wurden. Das Zeitreihendiagramm wird basierend auf der gewählten Dauer berechnet und aktualisiert. Unterstützte Dauern sind beispielsweise 1 Stunde, 3 Stunden, 24 Stunden, 7 Tage, 30 Tage und 90 Tage; das Intervall beträgt 1 Minute, 5 Minuten, 1 Stunde bzw. 1 Tag.
  - **Standort-Konnektivitätszustandsverteilung**: Das Diagramm mit der Verteilung von guten, angemessenen und schlechten Standorten für einen Mandanten basierend auf der neuesten Standort-Konnektivitätszustandsverteilung.
  - **Standort-Konnektivitätszustandsverteilung im Zeitverlauf**: Das Zeitreihendiagramm des Zustandsscores von Geräten mit Software 5.6.1 oder höher.
  - **Bewertung der Standortanwendungserfahrung:** Der Score der Standortanwendungserfahrung.
  - **Prisma SD-WAN-Zweigstellen**: Zeigen Sie den Standortzustand, den Standortkonnektivitätszustand, den Schaltkreiszustand, den Secure Fabric-Zustand und den Schwellenwert für Annäherung an maximale Kapazität einer Zweigstelle an. Sie können eine Zweigstelle weiter nach Standortprognose, Alarmstatus und ADEM-Status untersuchen und filtern.

- In der **Aktivitätsansicht** werden wichtige Anwendungsanalysen, der aktuelle Standortzustandsscore sowie die Verteilung des Standortzustands im Zeitverlauf angezeigt. Dazu gehören:
  - Standortzustandsverteilung: zeigt das Diagramm der Verteilung von guten, angemessenen und schlechten Standorten für einen Mandanten basierend auf dem neuesten Standortzustandsscore an.
  - Standortzustandsverteilung im Zeitverlauf: zeigt das Zeitreihendiagramm der Standortzustandsverteilung für einen bestimmten Mandanten im Zeitverlauf an, basierend auf dem Zustandsscore für eine Zweigstelle.
  - Bandbreitennutzung: zeigt die Bandbreitennutzung jeder Anwendung an einem Standort und WAN-Pfad an, einschließlich Daten zu den Top-10-Apps, die die meiste Bandbreite im Netzwerk verbrauchen.
  - Transaktionsstatistiken: bietet Transaktionsstatistiken über TCP-Flüsse, einschließlich Initiierungs-/Transaktionserfolgen und -fehlschlägen für eine bestimmte Anwendung oder alle Anwendungen, für einen bestimmten Pfad oder alle Pfade sowie für alle Zustandsereignisse.
  - Neue Flüsse: zeigt die neuen TCP- und UDP-Datenverkehrsflüsse für eine Anwendung, einen bestimmten Satz von Anwendungen oder alle Anwendungen in einem bestimmten Zeitraum an.
  - Gleichzeitige Flüsse: hilft Ihnen zu verstehen, wie viele Verbindungen in Ihrem Netzwerk aktiv sind (nach Anwendung).

# Überwachen: Rechenzentren

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden<br>• Prisma SD-WAN | Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>❑ Prisma Access<br>❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>❑ Strata Cloud Manager Essentials<br>❑ Strata Cloud Manager Pro<br>❑ Prisma SD-WAN<br>Weitere für Sichtbarkeit erforderliche Lizenzen und Voraussetzungen:<br>❑ ADEM-Beobachtbarkeit<br>❑ Autonomous DEM für Remote-Netzwerke<br>❑ KI-gestütztes ADEM<br>❑ WAN Clarity-Berichterstattung<br>❑ eine Rolle mit der Berechtigung zum Anzeigen des Dashboards<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

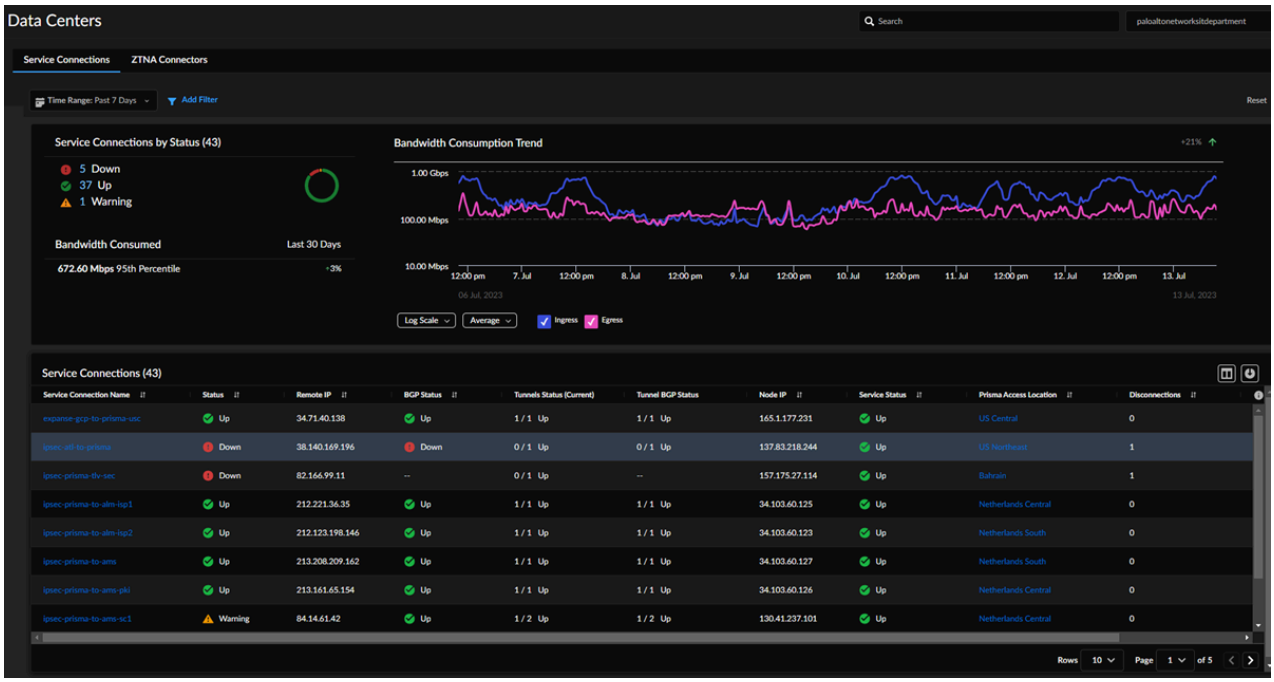
Überwachen Sie die Leistung der Dienstverbindungen, der ZTNA-Connectors und der Standortkonnektivität in Prisma SD-WAN-Rechenzentren an. Wählen Sie die Registerkarte **Überwachen** > **Prisma Access** > **Rechenzentren** > **Dienstverbindungen** oder **ZTNA-Connectors** aus, um den Zustand und Status der Dienstverbindungen und ZTNA-Connectors in Prisma Access anzuzeigen.

Wählen Sie für jedes Prisma SD-WAN-Rechenzentrum **Überwachen** > **Rechenzentren** > **Prisma SD-WAN** aus, um die Standortkonnektivitätsinformationen sowie den Status der VPN-Overlay-Verbindungen anzuzeigen.

- Dienstverbindungen
- ZTNA-Connectors
- Prisma SD-WAN

## Dienstverbindungen

Wählen Sie **Überwachen** > **Rechenzentren** > **Dienstverbindungen** aus, um zu beginnen.




Zeigen Sie aggregierte Dienstverbindungsdaten sowie Informationen zu einzelnen Dienstverbindungen an. Dienstverbindungen stehen sowohl mobilen Benutzern als auch Remote-Netzwerken zur Verfügung. Neben dem Zugriff auf Unternehmensressourcen ermöglichen Dienstverbindungen Ihren mobilen Benutzern auch die Verbindung zu Zweigstellen. Eine ausführliche Beschreibung dieser Widgets finden Sie unter Anzeigen und Überwachen von Rechenzentren im *Prisma Access-Administrationshandbuch*.

- Wählen Sie einen Zeitbereich aus, um Dienstverbindungen nach Status und ihrem Bandbreitenverbrauchstrend anzuzeigen.
- Zeigen Sie den Zustand all Ihrer Dienstverbindungen an.
- Zeigen Sie den Bandbreitenverbrauchstrend für all Ihre Dienstverbindungen an.
- Zeigen Sie Daten zu Ihren Dienstverbindungen an, beispielsweise den Status, die Remote-IP-Adresse, den BGP-Status, den aktuellen Tunnelstatus und andere Daten. Wählen Sie eine beliebige Dienstverbindung aus, um ihre Details anzuzeigen.

## ZTNA-Connectors

Wählen Sie **Überwachen** > **Rechenzentren** > **ZTNA-Connectors** aus, um zu beginnen.

Der ZTNA-Connector (Zero Trust Network Access) vereinfacht den Zugriff auf private Anwendungen für all Ihre Anwendungen. Die ZTNA-Connector-VM in Ihrer Umgebung bildet automatisch Tunnel zwischen Ihren privaten Anwendungen und Prisma Access. Zeigen Sie eine Übersicht aller konfigurierten ZTNA-Connectors an, einschließlich der mit dem Connector verknüpften **Anwendungsziele** , seiner durchschnittlichen und mittleren Bandbreite und des **Status** (aktiv, teilweise aktiv oder inaktiv). Eine ausführliche Beschreibung dieser Widgets finden Sie unter Anzeigen und Überwachen von Rechenzentren im *Prisma Access-Administrationshandbuch*.

Mögliche Aktionen:

- Zeigen Sie den Zustand und Status einer ZTNA-Connector-Gruppe an.

- Zeigen Sie den Zustand und Status einzelner ZTNA-Connectors an.

## Rechenzentren (Prisma SD-WAN)

Prisma SD-WAN-Standorte umfassen Rechenzentren, die in Ihrem Wide Area Network enthalten sein sollen. Sie können Unternehmensanwendungen und -dienste in einem Rechenzentrum hosten. Beim Erstellen eines Rechenzentrums können Sie eine Standarddomäne und einen Standardrichtliniensatz auswählen sowie WAN-Netzwerke, Schaltkreiskategorien, Schaltkreisbezeichnungen und Schaltkreisspezifikationen einrichten. Auf dem Prisma SD-WAN-Bildschirm **Rechenzentrum** wird die Liste der Rechenzentren angezeigt, mit dem Namen des Rechenzentrums, dem ION-Gerät und allen offenen Alarmen für den Standort.

Bei einem Rechenzentrum sehen Sie Folgendes:

- Auf der Registerkarte **Konfiguration** werden Ihnen Standortkonnektivitätsinformationen, Bereitstellungsmodi, WAN-Multicast-Peer-Gruppenprofile, Internet- und private WAN-Schaltkreise sowie IP-Präfixe angezeigt. Sie können auch einen Benutzer-Agent konfigurieren und Details der Clusterkonfiguration für das Rechenzentrum anzeigen.
- Die Registerkarte **Overlay-Verbindungen** zeigt Ihnen den Status aller VPN-Overlay-Verbindungen. Die Konnektivität jedes Standorts wird basierend auf dem Status seiner VPN-Overlay-Verbindungen berechnet.

# Überwachen: Netzwerkdienste

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden<br>• Prisma SD-WAN | Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>❑ Prisma Access<br>❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>❑ Strata Cloud Manager Essentials<br>❑ Strata Cloud Manager Pro<br>❑ Prisma SD-WAN<br>Weitere für Sichtbarkeit erforderliche Lizenzen und Voraussetzungen:<br>❑ ADEM-Beobachtbarkeit<br>❑ Autonomous DEM für Remote-Netzwerke<br>❑ KI-gestütztes ADEM<br>❑ WAN Clarity-Berichterstattung<br>❑ eine Rolle mit der Berechtigung zum Anzeigen des Dashboards<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Auf der Seite **Überwachen** > **Netzwerkdienste** können Sie die Leistung allgemeiner Netzwerkdienste anzeigen, die sich auf die Benutzererfahrung beim Zugriff auf Anwendungen auswirken. Wählen Sie die Registerkarte **GlobalProtect-Authentifizierung** aus, um die Anzahl der erfolgreichen oder fehlgeschlagenen GlobalProtect-Authentifizierungen für verschiedene Standorte anzuzeigen. Wählen Sie **Remote-Netzwerkdienste: DNS** aus, um DNS-Proxy-Anfragen und -Antworten anzuzeigen, die von Mandanten empfangen wurden (in Bezug auf Prisma Access-DNS-Proxy).

- GlobalProtect-Authentifizierung
- DNS

## GlobalProtect-Authentifizierung

Wählen Sie **Überwachen** > **Netzwerkdienste** > **GlobalProtect-Authentifizierung** aus, um zu beginnen.


Sie können die Leistung allgemeiner Netzwerkdienste anzeigen, die sich auf die Benutzererfahrung beim Zugriff auf Anwendungen in Insights auswirken. Netzwerkdienste umfassen Funktionen zur Meldung der Anzahl erfolgreicher und fehlgeschlagener GlobalProtect-Authentifizierungen als Maß dafür, ob mobile Benutzer eine Verbindung zu Prisma Access herstellen können. Hier wird Ihnen Folgendes angezeigt:

- Spezielle Angaben zur Anzahl erfolgreicher GlobalProtect-Authentifizierungen für verschiedene Standorte.
- Anzahl fehlgeschlagener GlobalProtect-Authentifizierungen für verschiedene Standorte.
- Anzahl von GlobalProtect-Authentifizierungen mit Zeitüberschreitung für verschiedene Standorte.

Eine ausführliche Beschreibung dieser Widgets finden Sie unter Anzeigen und Überwachen von Netzwerkdiensten.

## DNS

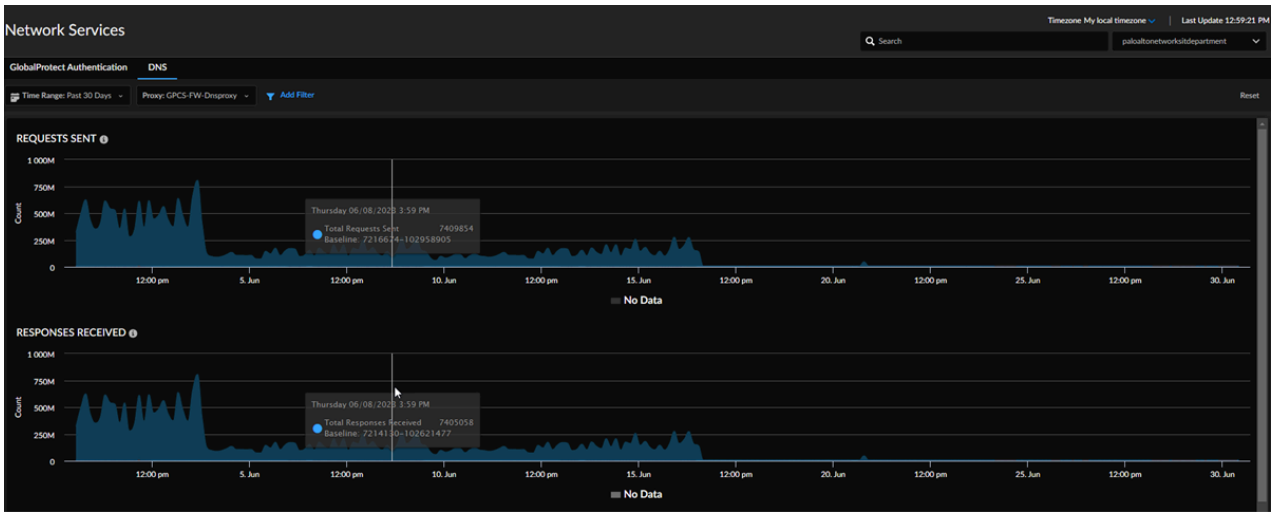
Wählen Sie **Überwachen** > **Netzwerkdienste** > **DNS** aus, um zu beginnen.

**Netzwerkdienste: DNS** zeigt DNS-Proxy-Anfragen und -Antworten an. Sie können die folgenden Filter verwenden:

- **Zeitbereich**
- **DNS-Proxy-Namen**

Die DNS-Proxy-Filterwerte beziehen sich auf die letzten 30 Tage und werden beim Laden automatisch ausgewählt (d. h., wenn keine Daten für explizite Proxys vorhanden sind, gibt es keinen Filter für explizite Proxys). Weitere Informationen finden Sie unter Anzeigen und Überwachen von Netzwerkdiensten.

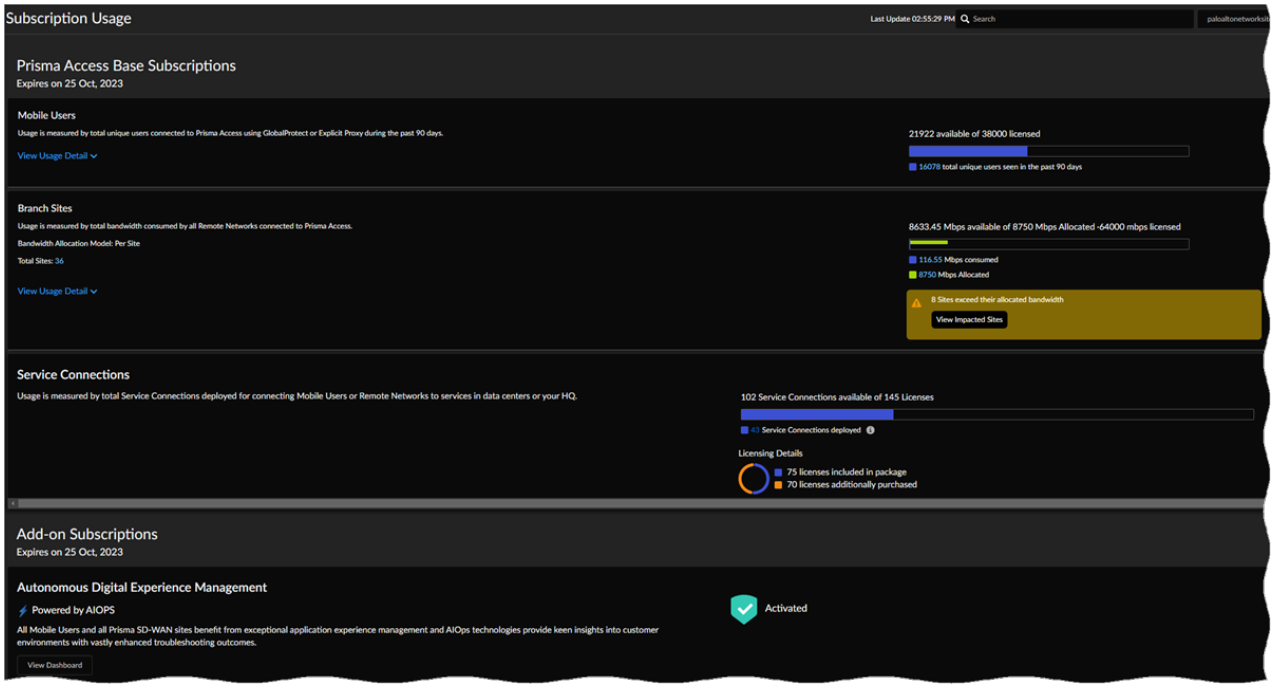


# Überwachen: Nutzung des Abonnements

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)* | ❑ Prisma Access-Lizenz<br>❑ AI-Powered ADEM, um bestimmte Funktionen freizuschalten. |

Wählen Sie **Überwachen** > **Nutzung des Abonnements** aus, um Details zur Nutzung Ihrer **Prisma Access-Basisabonnements** anzuzeigen, einschließlich der Gesamtzahl der verbundenen eindeutigen Benutzer, der von Remote-Netzwerkbenutzern verbrauchten Bandbreite, der Gesamtzahl der bereitgestellten Dienstverbindungen sowie Details zu etwaigen Add-on-Abonnements.




- **Mobile Benutzer**: Zeigen Sie an, wie viele Lizenzen für eindeutige **mobile Benutzer** Sie bisher verbraucht haben. Das Widget zeigt an, wie viele Lizenzen insgesamt von einzelnen mobilen Benutzern verbraucht werden, die in den letzten 90 Tagen eine Verbindung zu Prisma Access hergestellt haben, da Lizenzen immer auf den Prisma Access-Anmeldedaten der letzten 90 Tage basieren. Ein Benutzer, der sich in den letzten 90 Tagen mindestens einmal bei Prisma Access angemeldet hat, trägt zum Verbrauch einer „Mobiler Benutzer"-Lizenz bei.
- **Zweigstellen**: Zeigen Sie die gesamte Bandbreitennutzung aller Remote-Netzwerke an, die mit Prisma Access verbunden sind. Sehen Sie sich an, wie viel Bandbreite Sie zugewiesen und wie viel Sie verbraucht haben (in Mbit/s). Zeigen Sie die Nutzung anhand der gesamten Bandbreite an, die von allen mit Prisma Access verbundenen Remote-Netzwerken verbraucht wird.
- **Abonnementnutzung**: Sehen Sie, wie viele **Dienstverbindungen**-Lizenzen Sie bisher verbraucht haben.

Im Abschnitt **Add-on-Abonnements** auf dieser Seite finden Sie die zusätzlichen Lizenzen, die Sie erworben haben, z. B. die **Autonomous Digital Experience Management**-Lizenzen für mobile Benutzer und Remote-Netzwerke. Sie können die Gesamtzahl der erworbenen Lizenzen sowie die Anzahl der bisher nicht genutzten Lizenzen sehen. **Anwendungstests für die Überwachung mobiler Benutzer** – die Anzahl der verbleibenden Anwendungstests, die Sie für Ihre mobilen Benutzer erstellen können. Anwendungstests werden durch die Anzahl der überprüften mobilen Anwender bestimmt, wobei bis zu 10 Anwendungstests pro mobilem Benutzer zulässig sind.

Weitere Informationen finden Sie unter Anzeigen und Überwachen der Abonnementnutzung.

# Überwachen: ION-Geräte

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma SD-WAN | ❑ Prisma SD-WAN-Lizenz |

ION-Geräte in Prisma SD-WAN ermöglichen es Ihnen, unterschiedliche WAN-Netzwerke wie MPLS, LTE und Internetverbindungen in einem einzigen, leistungsstarken, hybriden Wide Area Network (WAN) zu kombinieren.

Der Bildschirm **Geräteliste** bietet Informationen zur Liste der Prisma SD-WAN-Geräte, einschließlich der Softwareversion und des Status des ION-Geräts. Hier können Sie die Softwareversion des Geräts aktualisieren oder ein Gerät konfigurieren.

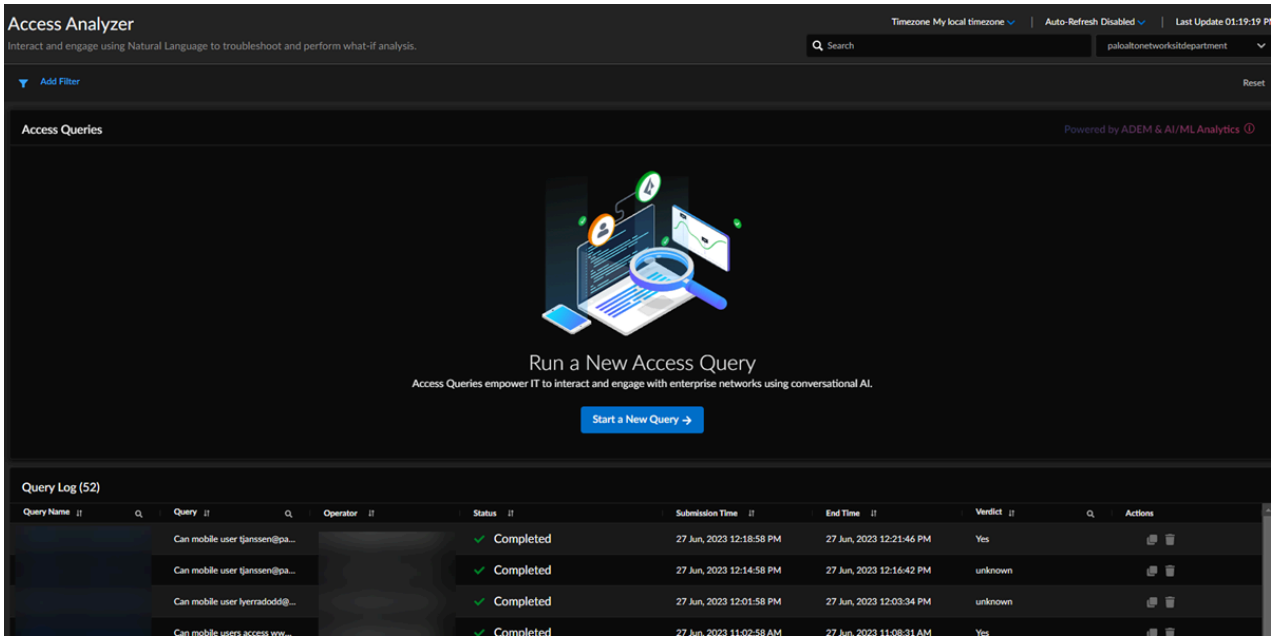
| Entität | Beschreibung |
|---|---|
| Gerätename | Zeigt den für das ION-Gerät konfigurierten Namen an. |
| Geräteinformationen | Zeigt den Typ und die Seriennummer des ION-Geräts an. |
| Software | Zeigt die aktuelle Softwareversion des Geräts an. Klicken Sie auf **Upgrade**, um die Gerätesoftwareversion zu ändern. |
| Letzte Aktivität | Zeigt Informationen darüber an, wann das ION-Gerät zuletzt konfiguriert und aktualisiert wurde. |
| Status | Zeigt den aktuellen Status des ION-Geräts an. |
| Redundanz | Zeigt an, ob das ION-Gerät Teil einer HA-Konfiguration (High Availability, hohe Verfügbarkeit) ist. |
| Actions (Aktionen) | Sie können das ION-Gerät über das Drei-Punkte-Menü konfigurieren. |

Der Bildschirm **Geräteaktivität** zeigt verschiedene Berichte zur Geräteaktivität eines Standorts in den letzten 24 Stunden an.

# Überwachen: Auf Analyzer zugreifen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)* | ❑ Prisma Access-Lizenz<br>❑ AI-Powered ADEM-Lizenz |

Wählen Sie **Überwachen** > **Auf Analyzer zugreifen**, um eine neue Zugriffsanalyse-Abfrage zu starten und eine Tabelle mit vorhandenen Abfragen anzuzeigen.




Die Zugriffsanalyse bietet eine automatische Überwachung Ihrer SASE-Umgebung. Sie bietet ein dialogorientiertes KI-Tool zur kontextbezogenen Fehlerbehebung und Was-wäre-wenn-Analysen zur Analyse von Zugriffs- und Konnektivitätsproblemen in Ihrer SASE-Umgebung.

Mögliche Aktionen:

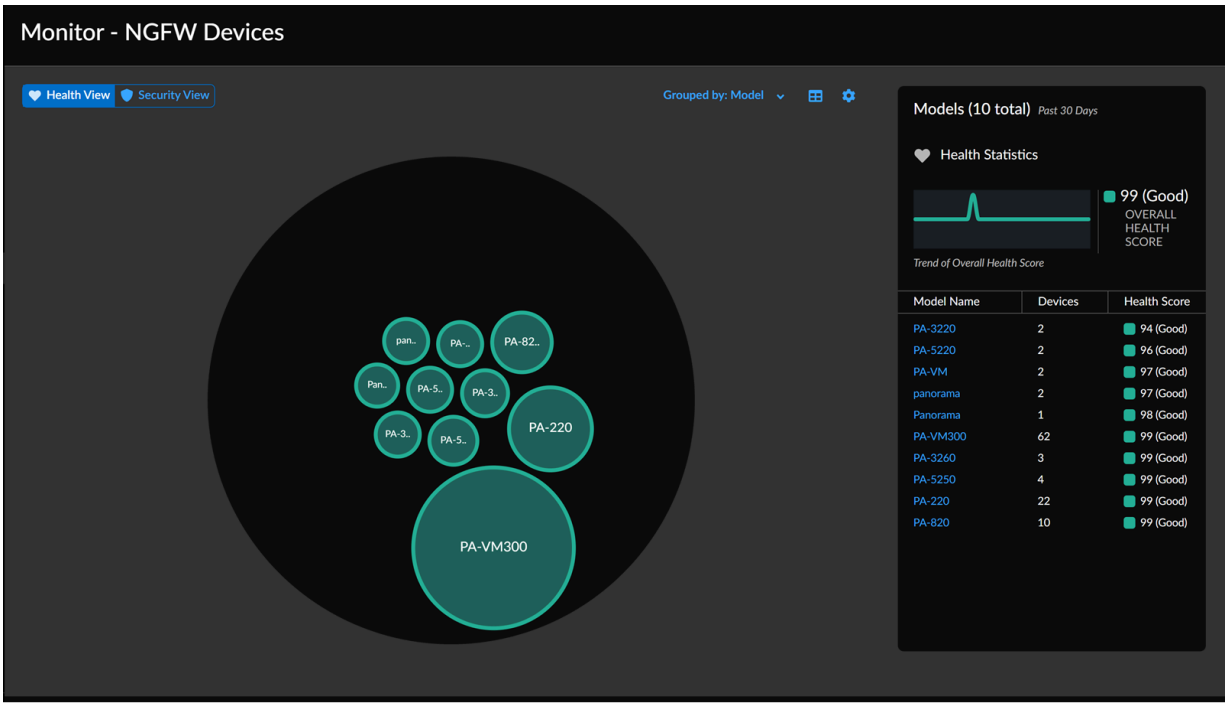
- Erfahren Sie, wie Sie in der Zugriffsanalyse eine Abfrage in natürlicher Sprache erstellen.
- Starten Sie eine neue Zugriffsanalyse-Abfrage.
- Zeigen Sie eine Liste der vorhandenen Abfragen an und wählen Sie eine beliebige Abfrage aus der Tabelle aus, um weitere Details anzuzeigen.

# Überwachen: NGFW-Geräte

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • NGFWs<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)* | ❑ AIOps for NGFW Free (use the AIOps for NGFW Free ap<br>oder<br>AIOps for NGFW Premium license (use the Strata Cloud<br>❑ Software-NGFW-Credits<br>*(für Software-NGFWs der VM-Series)* |

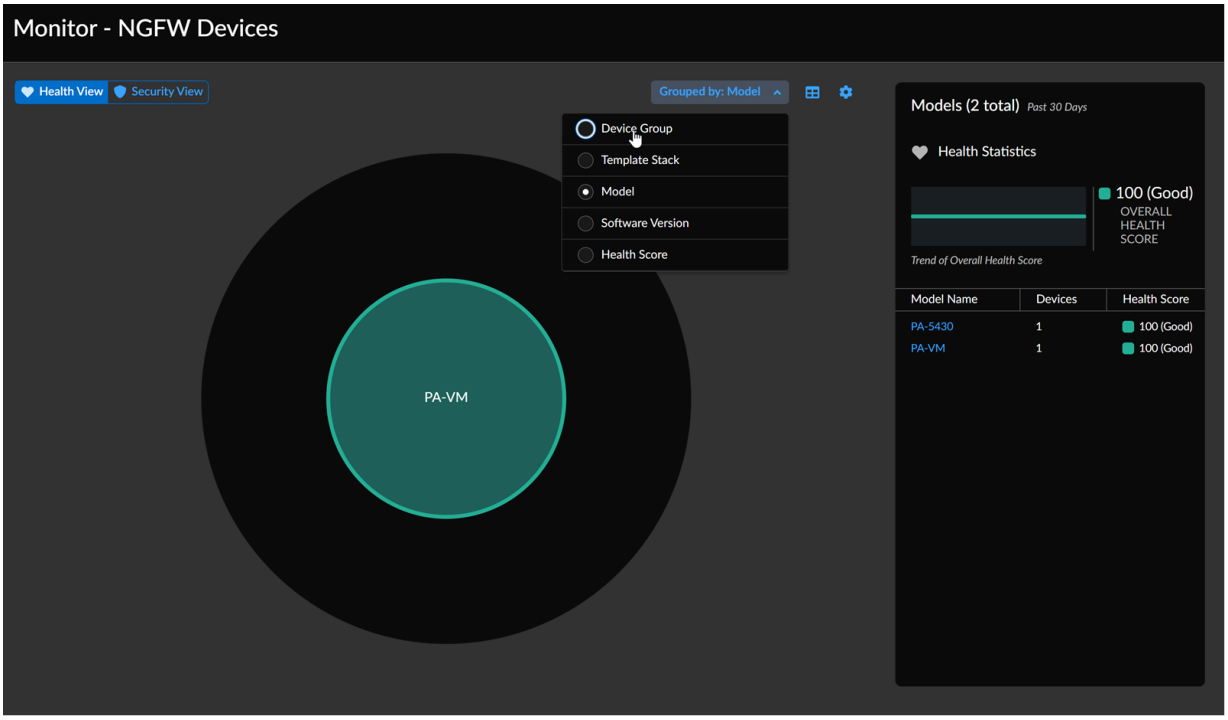
In **Überwachen** > **NGFW-Geräte** erhalten Sie eine farbcodierte, interaktive Darstellung der Geräte in Ihrer Bereitstellung zur einfachen und intuitiven Verwaltung und Untersuchung.

**STEP 1 |** Wählen Sie **Überwachen** > **NGFW-Geräte** aus.




**STEP 2 |** Wählen Sie **„Zustand“** oder **„Sicherheit“**aus.

**STEP 3 |** Wählen Sie unter **Gruppiert nach** aus, nach welchem Attribut die Visualisierung gruppiert werden soll.



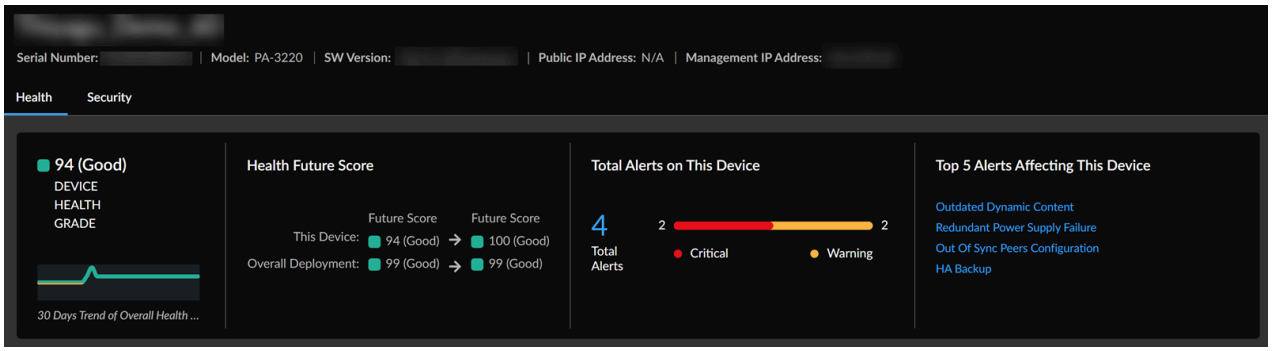

*Die Gruppierungsoptionen **Gerätegruppe** und **Vorlagenstack** sind nur in von Panorama verwalteten Bereitstellungen verfügbar, in denen Panorama Gerätetelemetriedaten sendet.*

**STEP 4 |** Wählen Sie eine Gruppe aus, um die darin enthaltenen Geräte anzuzeigen, und wählen Sie ein Gerät aus, um allgemeine Informationen dazu anzuzeigen.

Wenn Sie mehr über ein Gerät erfahren möchten, wählen Sie es aus.

## Anzeigen von Gerätedetails

Indem Sie ein Gerät in der **NGFW-Gerätevisualisierung** auswählen oder einem Link an einer anderen Stelle in der App folgen, können Sie spezifische Details zu einer Firewall oder einem Panorama-Gerät anzeigen, z. B. Zustand, Metriken, Verbindungen und mehr.




**Statusbewertung des Geräts**

Der aktuelle Zustand des Geräts sowie ein Diagramm mit seinem Verlauf der letzten 30<x> Tage. Mögliche Zustände sind „Gut“, „Angemessen“, „Schlecht“ und „Kritisch“.

**Zustandsbewertung nach der Korrektur**

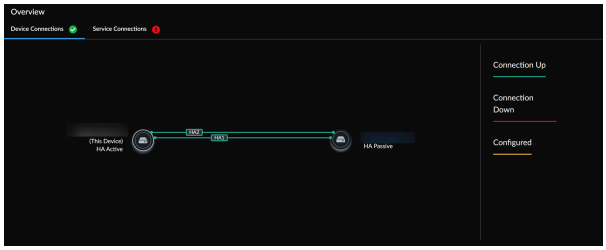
Der Zustand des Geräts, nachdem Sie offene Benachrichtigungen behoben haben. Diese Kachel zeigt Ihnen auch den Zustand Ihrer gesamten Bereitstellung nach dem Schließen von Benachrichtigungen.

**Total Alerts (Gesamtbenachrichtigungen)**

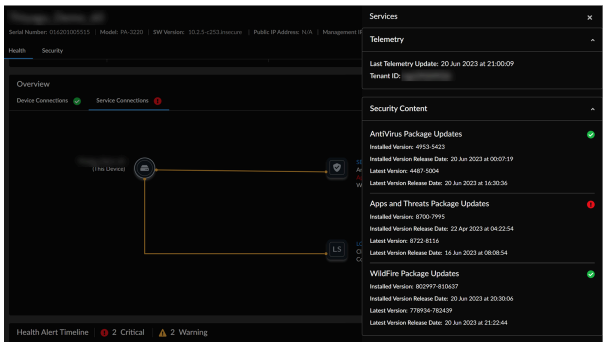
Die Gesamtzahl der offenen Benachrichtigungen zu dem Gerät.

**Top-5-Benachrichtigungen**

Fünf der häufigsten Benachrichtigungen auf diesem Gerät in den letzten 30 Tagen.

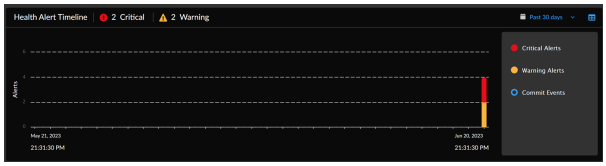
| | |
|---|---|
| **Übersicht > Geräteverbindungen**<br>Die anderen Geräte, die mit dem Gerät verbunden sind, das Sie gerade anzeigen. Wählen Sie ein Gerät aus, um seine Details anzuzeigen. |  |
| **Übersicht > Dienstverbindungen**<br>Eine Übersicht aller im Gerät integrierten Sicherheits- und Protokollierungsdienste. Wählen Sie einen Dienst aus, um seine Details anzuzeigen. |  |



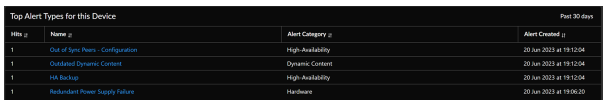

### Benachrichtigungszeitachse

Eine Zeitleiste mit Gerätebenachrichtigungen und Commit-Ereignissen. Benachrichtigungen werden als kritisch, Warnung oder Commit-Ereignis kategorisiert. Schalten Sie die Ansicht um, um die Warndaten im Tabellenformat anzuzeigen.




### Top-Benachrichtigungstypen für dieses Gerät

Die häufigsten Benachrichtigungen der letzten 30 Tage. Wählen Sie eine Benachrichtigung aus, um ihre Benachrichtigungsdetails anzuzeigen.




### Top-10-Anwendungsnutzung

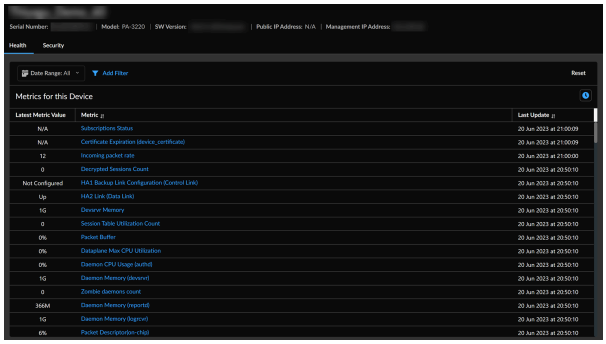
Die zehn Anwendungen, die die meisten Daten auf der Firewall verbrauchen.

### Metriken für dieses Gerät

Eine Liste aller Zustandsmetriken, die für die auf dem Gerät ausgeführten Sicherheitsprüfungen erfasst wurden, einschließlich HA-Verbindungsdaten.

Wählen Sie eine Metrik aus, um ihre Details anzuzeigen.



# Überwachen: Kapazitätsanalyse

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • NGFW | ❑ AIOps for NGFW Premium oder Strata Cloud Manager Pro<br><br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Mit der Kapazitätsanalyse können Sie die Ressourcenkapazität Ihrer Geräte überwachen, indem Sie die Nutzung von Metriken basierend auf ihren Modelltypen verfolgen. Die Kapazitätsanalyse bietet folgende Vorteile:

- Ein umfassendes Verständnis der vorhandenen Metrikauslastung und der verbleibenden Metrikkapazität bis zur Maximalgrenze.
- Eine Heatmap-Visualisierung, die die Metriknutzung in Bezug auf die Hardwareplattformen in einer einzigen Ansicht zeigt und dabei hilft, detaillierte Untersuchungen durchzuführen.
- Die Möglichkeit, ein Upgrade auf Firewalls mit höherer Kapazität zu planen, um Ihre spezifischen Anforderungen zu erfüllen.

*Die Funktion **Kapazitätsanalyse** wird für die Firewalls der VM-Series nicht unterstützt.*

Hier ist ein Video, das die Verwendung der Funktion „Kapazitätsanalyse“ zeigt:

Die Kapazitätsanalyse wurde erweitert und unterstützt nun Benachrichtigungen, die Sie darüber informieren, dass sich der Ressourcenverbrauch der maximalen Kapazität nähert. Die Benachrichtigungen der Kapazitätsanalyse werden drei Monate im Voraus generiert und weisen auf potenzielle Kapazitätsengpässe hin. Auf diese Weise können Sie die Konfigurationsbereinigung oder die Erweiterung der NGFW-Kapazitäten planen, bevor diese ihre maximale Auslastung erreichen, und so die Systemstabilität aufrechterhalten. Eine Liste der unterstützten Kapazitätsbenachrichtigungen finden Sie unter Premium-Zustandsbenachrichtigungen.

Die Kapazitätsanalyse gruppiert die Metriken basierend auf den folgenden Typen:

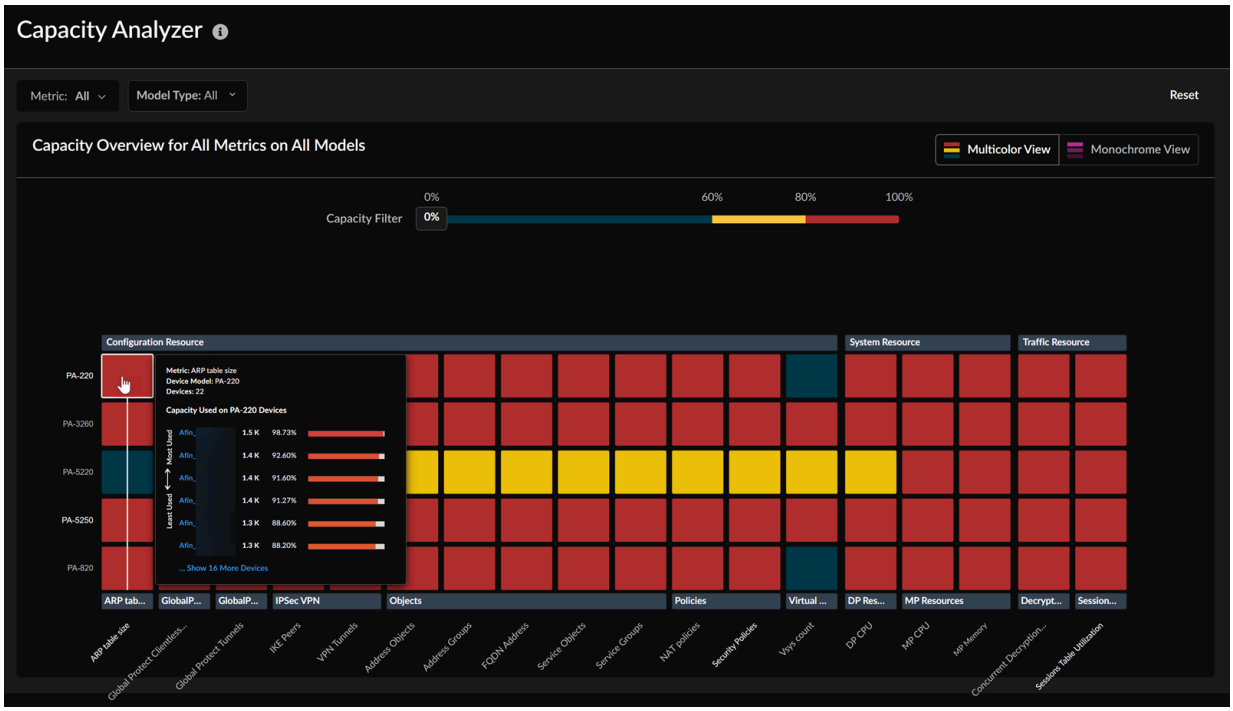
- Konfigurationsressourcen-Metriken, wie z. B. NAT-Richtlinien und Adressobjekte
- Betriebsressourcenmetriken des Systems, wie z. B. CPU, Speicher, Festplatten und Protokolle
- Metriken für Verkehrsressourcen, wie z. B. Entschlüsselungsnutzung und Sitzungstabellenauslastung


Die Heatmap zeigt die Metriknutzung für jedes Gerät. Die dunklere Farbe steht für eine höhere Auslastung und die hellere Farbe für eine niedrigere Auslastung. Standardmäßig ist die **mehrfarbige Ansicht** ausgewählt. Sie können auch zur **monochromen Ansicht** wechseln.

Sie können die Heatmap der Kapazitätsanalyse auf unterschiedliche Weise nutzen, um Informationen zur Metriknutzung zu erhalten:

- Bewegen Sie den Mauszeiger über einen Metrikblock für ein Gerät, um einen Tooltip mit den folgenden Details anzuzeigen:
  - Name der Metrik
  - Gerätemodell und Geräteliste
  - Gerätekapazitätsbereich




- Filtern Sie Daten mithilfe der folgenden Attribute:
  - **Metrik** – Wählen Sie eine oder mehrere Metriken aus, die Sie anzeigen möchten, oder suchen Sie anhand des Metriknamens.
  - **Modell** – Wählen Sie ein oder mehrere Gerätemodelle aus oder suchen Sie anhand des Modellnamens.
  - **Kapazität** – Wählen Sie die Kapazität auf der **Kapazitätsfilter**-Skala aus.

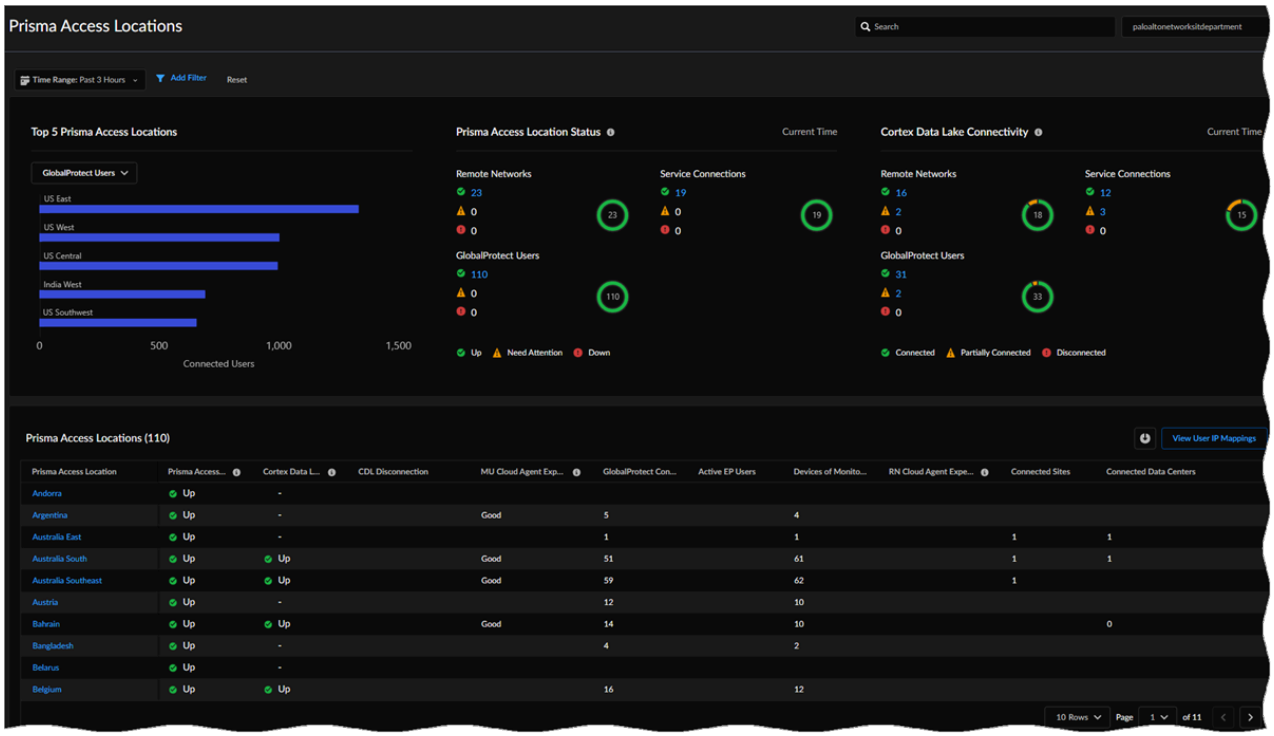
Weitere Informationen zur Verwendung der Kapazitätsanalyse-Heatmap finden Sie unter Analysieren der Metrikkapazität.

# Überwachen: Prisma Access-Standorte

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)* | ❑ Prisma Access-Lizenz<br>Dies ist eine Funktion von Prisma Access Insights. |

Wählen Sie **Überwachen** > **Prisma Access-Standorte** aus, um zu beginnen. Hier können Sie den Zustand all Ihrer Prisma Access-Standorte für Ihre Remote-Netzwerke und mobilen Benutzer anzeigen. Eine ausführliche Beschreibung dieser Widgets finden Sie unter Anzeigen und Überwachen von Prisma Access-Standorten im *Prisma Access-Administrationshandbuch*.

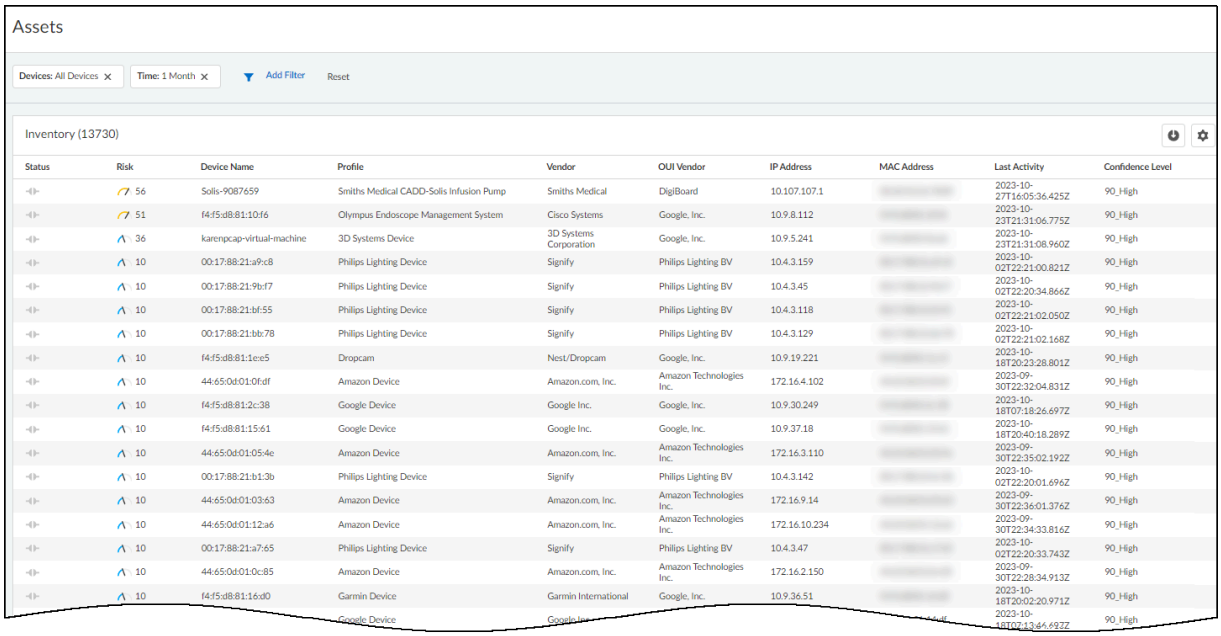



- Sehen Sie sich die Top 5 der Prisma Access-Standorte für Remote-Netzwerke, Dienstverbindungen, mobile GlobalProtect-Benutzer oder Benutzer expliziter Proxys an, basierend auf der insgesamt verbrauchten Bandbreite.
- Zeigen Sie den Status Ihrer Prisma Access-Standorte an.
- Zeigen Sie die Strata Logging Service-Konnektivität an.
- Zeigen Sie die Tabelle „Prisma Access-Standorte“ an, in der alle Prisma Access-Standorte aufgelistet sind, und wählen Sie einen einzelnen Prisma Access-Standort nach Namen aus, um dessen Details anzuzeigen.

# Überwachen: Assets

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • NGFWs<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)* | ❑ IoT Security-Abonnement<br>❑ Software-NGFW-Credits<br>*(für Software-NGFWs der VM-Series)* |

Wählen Sie zunächst **Überwachen > Assets** aus. Von hier aus können Sie einen dynamisch verwalteten Bestand der IoT-, OT- und IT-Geräte in Ihrem Netzwerk anzeigen – mit zahlreichen Attributen für jedes Gerät wie etwa IP- und MAC-Adresse, Profil, Anbieter, Modell und Betriebssystem sowie (bei Advanced IoT Security-Produkten) den Risikoscore auf Geräteebene.




Verwenden Sie die Daten in diesem Bestand, um mehr über die Assets in Ihrem Netzwerk zu erfahren:

- Zeigen Sie einen dynamisch generierten und aktuellen Bestand der in Ihrem Netzwerk erkannten Geräte an, einschließlich IoT-, OT- und IT-Geräten.
- Während das IoT-Dashboard Ihre Gerätetypen auf übergeordneter Ebene anzeigt, können Sie über den Asset-Bestand einzelne Geräte untersuchen, um weitere Details anzuzeigen und Ihren Sicherheitsstatus zu beurteilen.
- Filtern Sie die im Dashboard angezeigten Daten nach Standort, Gerätetyp, Zeitraum und einem oder mehreren Geräteattributen, um Daten zu den Geräten anzuzeigen, die Sie interessieren.
- Zeigen Sie Spalten an bzw. blenden Sie sie aus, um die für Sie wichtigen Geräteattribute anzuzeigen. Es stehen über 100 Attributspalten zur Auswahl.

- Laden Sie die auf der derzeit aktiven Seite angezeigten Daten als CSV-Datei herunter, um sie in Berichte einzubinden oder später darauf zurückzugreifen. Die Datei enthält die Geräte und Geräteattribute, die Ihnen zum Zeitpunkt des Downloads angezeigt werden.

# Vorfälle und Benachrichtigungen: Strata Cloud Manager

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden<br>• Prisma SD-WAN | Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>❑ Prisma Access<br>❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>❑ Prisma SD-WAN<br>❑ Strata Cloud Manager Essentials<br>❑ Strata Cloud Manager Pro<br>Weitere für Sichtbarkeit erforderliche Lizenzen und Voraussetzungen:<br>❑ eine Rolle mit der Berechtigung zum Anzeigen des Dashboards<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

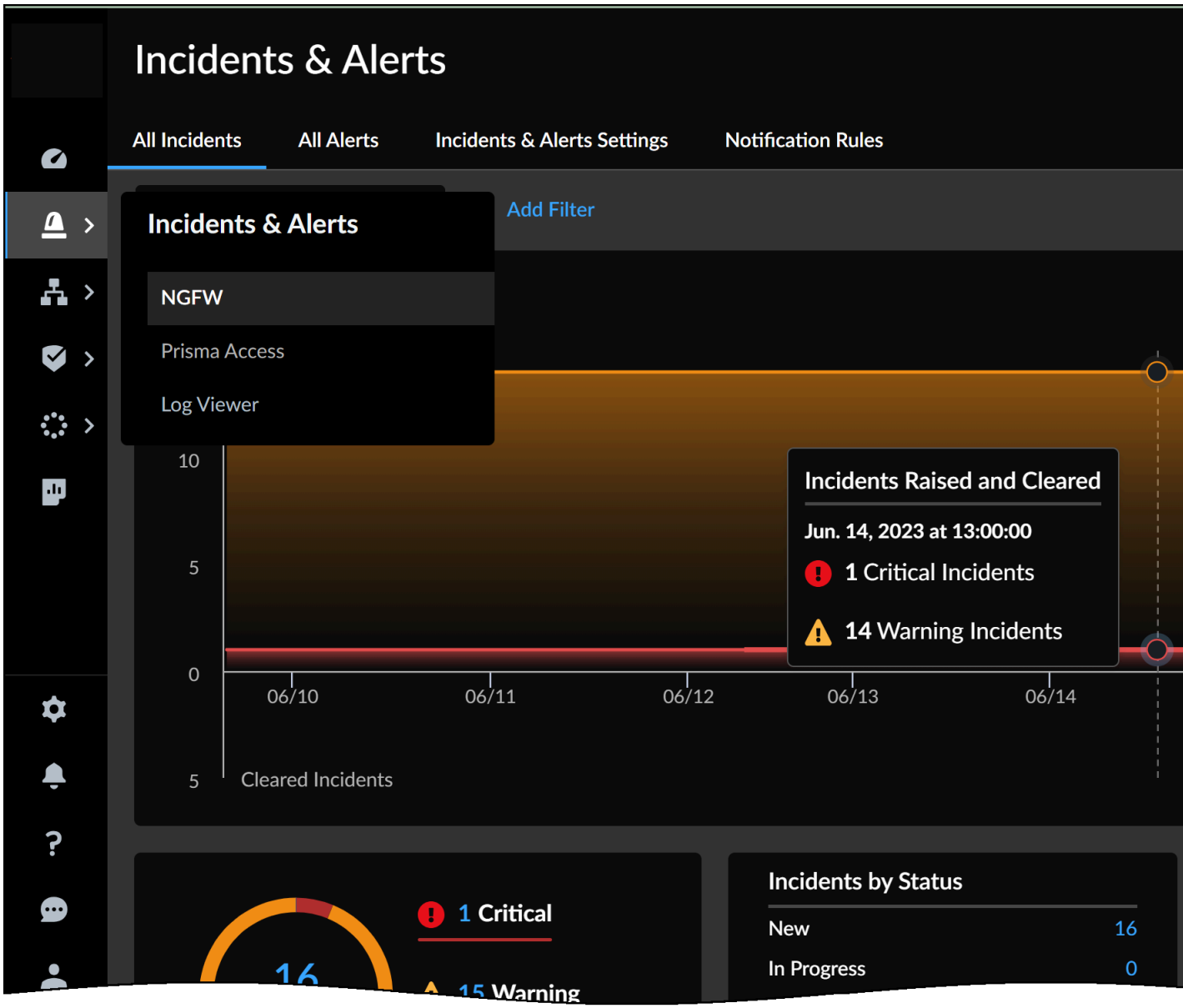
Strata Cloud Manager bietet Ihnen ein gemeinsames Framework für die Interaktion und Untersuchung der Vorfälle und Benachrichtigungen, die von Palo Alto Networks-Produkten und -Abonnements in Ihrem Unternehmen erkannt werden:

- Vorfälle und Benachrichtigungen: NGFW
- Vorfälle und Benachrichtigungen: Prisma Access
- Vorfälle und Benachrichtigungen: Prisma SD-WAN

Damit Sie die Funktionsfähigkeit Ihrer Geräte und Bereitstellungen dauerhaft gewährleisten und Störungen in Ihrem Geschäftsbetrieb vermeiden können, sehen Sie sich die einzelnen Seiten mit Vorfällen und Benachrichtigungen an. Hier können Sie …

- Vorfälle und Benachrichtigungen in Ihrem gesamten Netzwerk anzeigen und eine detaillierte Untersuchung durchführen
- Regeln erstellen und überprüfen, die Vorfälle und Benachrichtigungen auslösen

zwischen Ihren Vorfällen/Benachrichtigungen und dem Vorfälle und Benachrichtigungen: Protokoll-Viewer wechseln, um Aktivitäten in Ihrem Netzwerk zu untersuchen, die Vorfälle und Benachrichtigungen auslösen oder damit in Zusammenhang stehen



# Vorfälle und Benachrichtigungen: NGFW

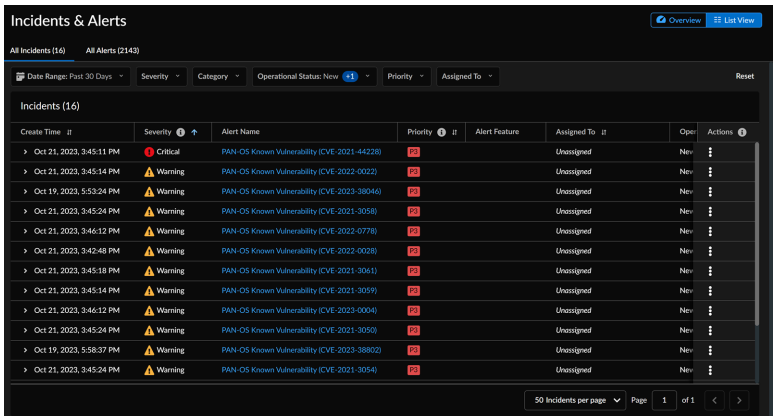
| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | ❑ Eine der folgenden Lizenzen:<br>❑ AIOps for NGFW Free (use the AIOps for NGFW Free app) oder AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>❑ Strata Cloud Manager Essentials<br>❑ Strata Cloud Manager Pro |

Damit Sie den laufenden Zustand Ihrer Geräte aufrechterhalten und Vorfälle vermeiden können, die Ihr Unternehmen stören, generieren Ihre Anwendungen Vorfälle und Benachrichtigungen basierend auf einem oder mehreren Problemen, die bei Ihrer Firewallbereitstellung festgestellt wurden. Mit **Vorfälle und Benachrichtigungen** > **NGFW** erhalten Sie einen zentralen Überblick über Vorfälle und Benachrichtigungen in allen NGFWs.

So richten Sie **NGFW-Vorfälle und #Benachrichtigungen** ein:

- Durch Vorfälle werden Sie über Sicherheitslücken auf dem Laufenden gehalten. Sie können sie untersuchen und gegebenenfalls vorbeugende Maßnahmen ergreifen.

  Navigieren Sie zu **Vorfälle und Benachrichtigungen** > **NGFW** > **Alle Vorfälle**, um Vorfälle in Ihrem Netzwerk anzuzeigen und mit ihnen zu interagieren.




- Eine Benachrichtigung weist auf ein bestimmtes Problem hin (Verschlechterung oder Ausfall der Firewall-Funktionalität), das behoben werden muss. Benachrichtigungen können auch auf Grundlage von Korrelation oder Aggregation mehrerer Ereignisse generiert werden. Diese Aggregation von Ereignissen zu einer einzigen Benachrichtigung hilft bei der Triage, beim Optimieren der Benachrichtigungsweiterleitung zwischen Teams sowie bei der Zentralisierung

kritischer Informationen und sorgt dafür, dass Mitarbeiter nicht in einer Flut von Nachrichten untergehen und so wichtige Nachrichten übersehen.

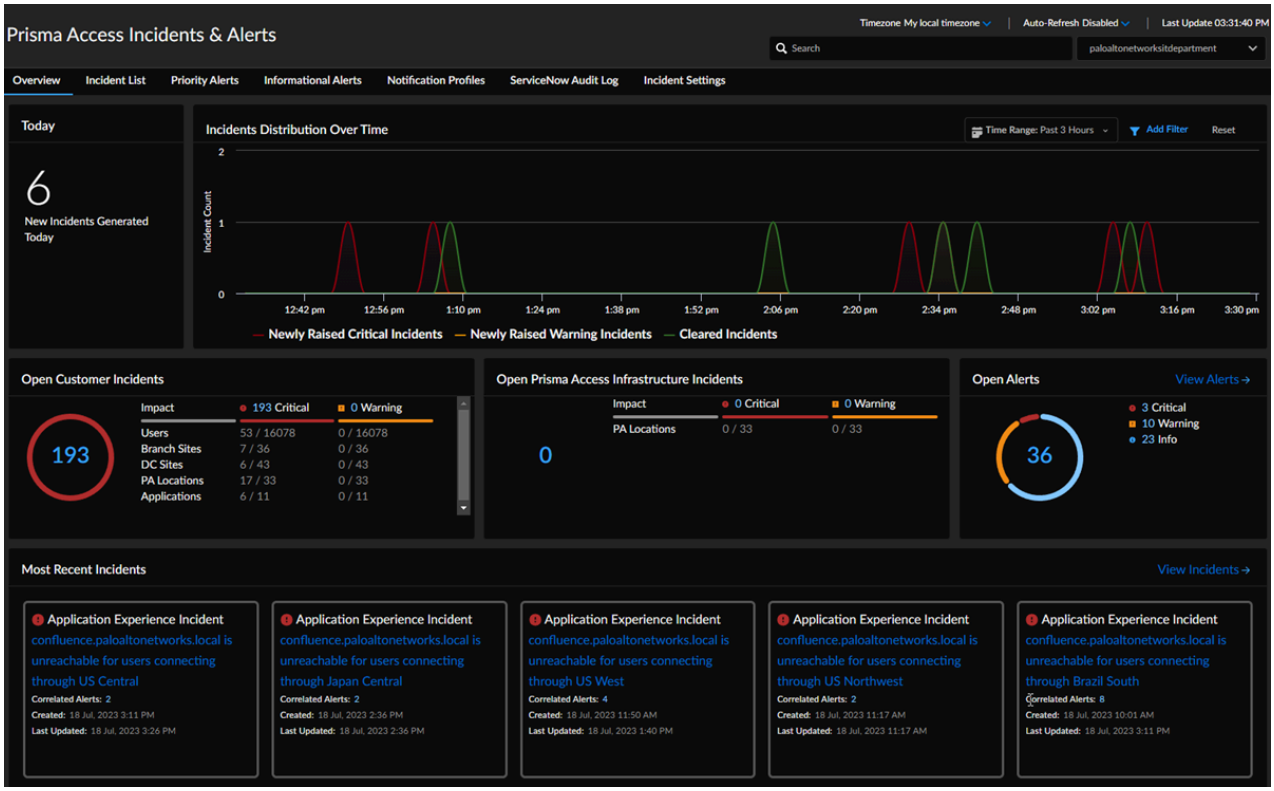
Navigieren Sie zu **Vorfälle und Benachrichtigungen** > **NGFW** > **Alle Benachrichtigungen**, um Benachrichtigungen in Ihrem Netzwerk anzuzeigen und mit ihnen zu interagieren.

# Vorfälle und Benachrichtigungen: Prisma Access

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)* | ❑ AI-Powered ADEM-Lizenz<br>❑ ADEM Observability-Lizenz<br>❑ Prisma Access-Lizenz |

Wählen Sie **Vorfälle und Benachrichtigungen** > **Prisma Access-Vorfälle und -Benachrichtigungen**, um loszulegen. Die in Ihrer Umgebung verfügbaren Vorfälle und Benachrichtigungen hängen von Ihren Lizenzen ab.




## Ganzheitliche Übersicht

Sehen Sie sich eine Übersicht der Vorfälle und Benachrichtigungen im Zusammenhang mit Ihrer Prisma Access-Umgebung an. Die in Ihrer Umgebung verfügbaren Vorfälle und Benachrichtigungen hängen von Ihren Lizenzen ab.

## Alle Vorfälle auf einen Blick

Sehen Sie sich die Liste der Vorfälle an, die alle Vorfälle in Ihrer Umgebung anzeigt. Verwenden Sie das Drop-down-Menü **Filter hinzufügen**, um Vorfälle anhand der Spalten in der Tabelle auszuwählen (Sie können nach mehreren filtern). Wählen Sie in der Tabelle einen beliebigen **Vorfall** aus, um dessen detaillierte Informationen anzuzeigen.

## Benachrichtigungen mit Priorität

Siehe Benachrichtigungen mit Priorität, die den Status Ihrer Prisma Access-Umgebung beschreiben.

## Informative Benachrichtigungen

Sehen Sie sich informative Benachrichtigungen an, die Sie über bevorstehende Software-Upgrades oder den Status von Upgrades informieren, die gerade ausgeführt oder abgeschlossen werden.

## Benachrichtigungsprofile

In den Benachrichtigungsprofilen können Sie Informationen zu **Benachrichtigungsabonnements** einsehen und ein neues **Benachrichtigungsprofil** erstellen oder ein vorhandenes ändern.

## ServiceNow-Überwachungsprotokoll

Wenn Sie ServiceNow verwenden, können Sie das ServiceNow-Überwachungsprotokoll überprüfen, das Ihnen jede ServiceNow-**Vorfall-ID** anzeigt. Es zeigt Ihnen auch die ServiceNow-Vorgänge, die für jeden Vorfall ausgeführt wurden, z. B. Erstellen, Aktualisieren und Löschen.

## Vorfalleinstellungen

In den Vorfalleinstellungen können Sie die Vorfälle, die Sie erhalten, nach Vorfallkategorie und -code anpassen.

## Vorfälle und Benachrichtigungen nach Code

Sehen Sie sich Vorfälle und Benachrichtigungen anhand ihrer Code-IDs an, machen Sie sich ein Bild von den Problemen, die sie beschreiben, und finden Sie heraus, wie Sie diese beheben können. Vorfälle und Benachrichtigungen sind nach Lizenz kategorisiert:

- Vorfälle hinsichtlich KI-gestütztem ADEM
- ADEM-Vorfälle
- Prisma Access-Vorfälle
- Benachrichtigungen mit Priorität
- Informative Benachrichtigungen

Informationen zu Vorfällen und Benachrichtigungen finden Sie im Referenzhandbuch für Vorfälle and Benachrichtigungen.

Informationen zur ServiceNow-Integration finden Sie unter Integrieren von ServiceNow in Prisma Access im *Integrationshandbuch*.

# Vorfälle und Benachrichtigungen: Prisma SD-WAN

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma SD-WAN | ❑ Prisma SD-WAN-Lizenz |

Prisma SD-WAN generiert Vorfälle und Benachrichtigungen, wenn das System system- oder kundendefinierte Schwellenwerte erreicht oder ein Fehler im System vorliegt. Verwenden Sie diese Vorfälle und Benachrichtigungen zur Fehlerbehebung im System.

Wählen Sie **Vorfälle und Benachrichtigungen** > **Prisma SD-WAN**, um Vorfälle und Benachrichtigungen in Strata Cloud Manager anzuzeigen.

Verwenden Sie die folgenden Registerkarten, um durch Vorfälle und Benachrichtigungen in Prisma SD-WAN zu navigieren.

- Übersicht
- Vorfälle
- Benachrichtigungen
- Einstellungen

**Übersicht**

Zeigen Sie Vorfälle und Benachrichtigungen sowie deren Kategorien in Prisma SD-WAN an. Die Registerkarte **Übersicht** ist Ihre Standardansicht.

Zeigen Sie die wichtigsten Vorfälle und Benachrichtigungen an, die die folgenden Informationen umfassen.

| | |
|---|---|
| Art des Vorfalls | Zeigt die Kategorie des Vorfalls an. |
| Beschreibung | Zeigt die Beschreibung des Vorfalls an. |
| Severity (Schweregrad) | Zeigt den Schweregrad des Vorfalls an. |
| Priorität | Zeigt die Priorität des Vorfalls an. |
| Korrelierte Warnungen | Zeigt die Anzahl der in diesem Vorfall zusammengefassten Vorfälle an. |
| Status | Zeigt den Status des Vorfalls an. |
| Erstellt | Zeigt an, wann der Vorfall vom System gemeldet wurde. |
| Last Updated (Zuletzt aktualisiert) | Zeigt an, wann der Vorfall zuletzt vom System aktualisiert wurde. |

### Vorfälle

Ein Vorfall ist ein Hinweis auf einen Fehler im System. Vorfälle werden gemeldet und behoben und können unterschiedliche Schweregrade aufweisen:

- Kritisch – Das gesamte Netzwerk oder Teile davon sind ausgefallen und es ist sofortiges Eingreifen erforderlich.
- Warnung – Beeinträchtigt das Netzwerk und erfordert sofortiges Eingreifen.
- Informativ – Das Netzwerk ist beeinträchtigt und erfordert bald Aufmerksamkeit.

### Benachrichtigungen

Eine Benachrichtigung kann ein Hinweis auf einen Fehler im Netzwerk sein, muss es aber nicht. Wenn das System system- oder kundendefinierte Schwellenwerte erreicht, wird eine Benachrichtigung ausgelöst.

### Einstellungen

Verwenden Sie die Registerkarte **Einstellungen**, um Vorfallrichtlinien zu erstellen und die Unterdrückung von Ereigniscodes basierend auf den angegebenen Klassifizierungen und konfigurierten Aktionsattributen zu verwalten. Sie können Richtlinienregeln für Vorfälle verwenden, um Vorfälle zu unterdrücken oder zu eskalieren, die während eines geplanten Zeitraums auftreten. Darüber hinaus können Sie die Standardpriorität systemgenerierter Vorfälle auf eine Prioritätsstufe ändern, die besser auf Ihre Geschäftsanforderungen abgestimmt ist.

# Vorfälle und Benachrichtigungen: Protokoll-Viewer

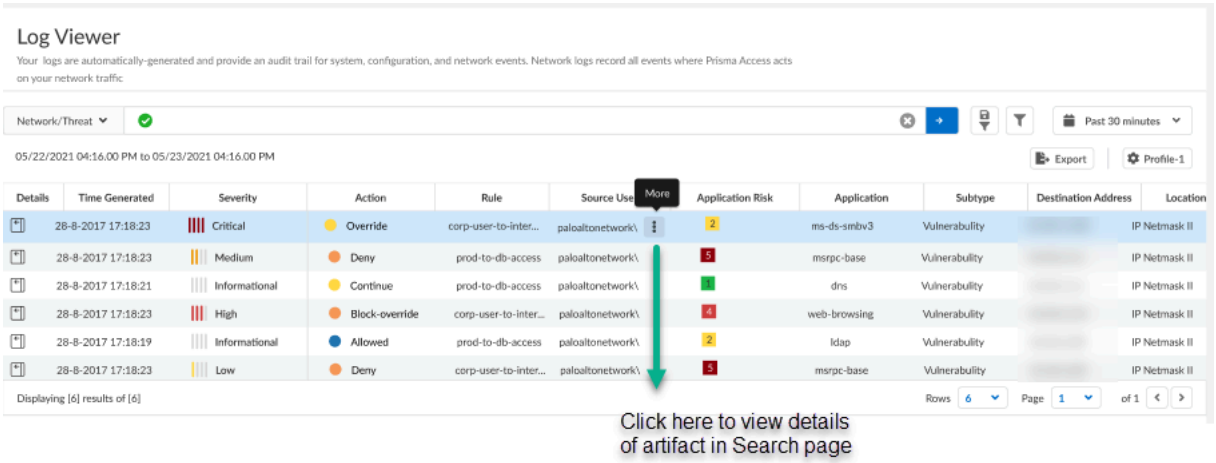
| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)*<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | ❑ Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>❑ Prisma Access<br>❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) oder AIOps for NGFW Free (use the AIOps for NGFW Free app)<br>❑ Strata Cloud Manager Essentials<br>❑ Strata Cloud Manager Pro<br>❑ eine Rolle mit der Berechtigung zum Anzeigen des Dashboards |

Der **Protokoll-Viewer** bietet die Funktionen von Erkunden: Sie können Ihre in Strata Logging Service gespeicherten Protokolle anzeigen und mit ihnen interagieren.

Der **Protokoll-Viewer** bietet einen Prüfpfad für System-, Konfigurations- und Netzwerkereignisse. Springen Sie von einem Dashboard zu Ihren Protokollen, um Details zu erhalten und Ergebnisse zu untersuchen. Ein Abfragefeld und Zeitbereichseinstellungen helfen Ihnen, sich auf die spezifischen Protokolle zu konzentrieren, die Sie interessieren.

- Erfahren Sie mehr darüber, wie Sie Ihre Abfragen erstellen.
- Entdecken Sie neue Protokoll-Viewer-Funktionen in den Strata Logging ServiceVersionshinweisen.

Der **Protokoll-Viewer** hebt Aktionen und den Schweregrad der Protokolle hervor, damit Sie verstehen, wie Regeln in Sitzungen durchgesetzt werden. Sie können auch die Details zu den Sicherheitsartefakten der Protokolle auf der Suchseite anzeigen.




* Sie können Details in der Suche für folgende Protokolltypen und -felder anzeigen:

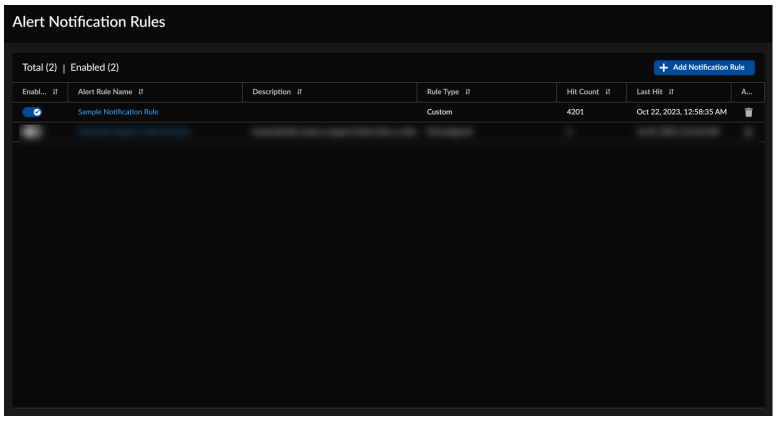
| Protokolltyp | Spaltenname |
|---|---|
| Verkehr, Bedrohung, URL, Datei | • Quelladresse<br>• Zieladresse<br>• NAT-Quelle<br>• NAT-Ziel |
| Bedrohung, Datei | Datei-Hash |
| URL | • URL<br>• URL-Domäne |
| DNS Security | • Quelladresse<br>• Zieladresse<br>• Domäne<br>• FQDN |

# Vorfall- und Benachrichtigungseinstellungen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | ❑ AIOps for NGFW Free (use the AIOps for NGFW Free app) oder AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>❑ Strata Cloud Manager Essentials<br>❑ Strata Cloud Manager Pro |

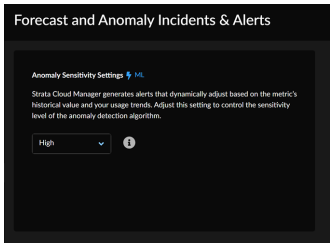
- Sie können Benachrichtigungseinstellungen definieren, z. B. welche Alarme Benachrichtigungen auslösen, wie und wie oft Sie Benachrichtigungen erhalten, und Sie können eine Benachrichtigungsregel erstellen.

  Navigieren Sie zu **Vorfälle und Benachrichtigungen** > **Vorfall- und Benachrichtigungseinstellungen** > **Benachrichtigungsregeln**, um Regeln zum Auslösen von Benachrichtigungen anzuzeigen und hinzuzufügen.




- Strata Cloud Manager generiert Benachrichtigungen und Vorfälle, die basierend auf dem historischen Wert der Metrik und Ihren Nutzungstrends dynamisch angepasst werden. Sie können diese Einstellung anpassen, um die Empfindlichkeit des Anomalieerkennungsalgorithmus zu steuern.

  Navigieren Sie zu **Vorfälle und Benachrichtigungen** > **Vorfall- und Benachrichtigungseinstellungen** > **Anomalieempfindlichkeit**, um die Empfindlichkeitsstufe des Algorithmus zur Anomalieerkennung zu konfigurieren.



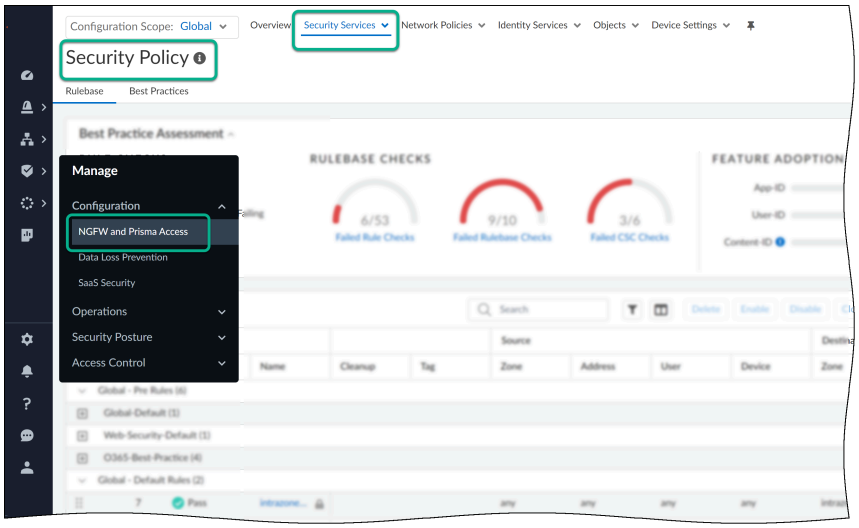
 

# Verwalten: NGFW und Prisma Access

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>❑ Prisma Access<br>❑ AIOps for NGFW Premium<br>❑ Strata Cloud Manager Essentials<br>❑ Strata Cloud Manager Pro<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Mit Strata Cloud Manager können Sie eine Sicherheitsrichtlinie konfigurieren, die an all Ihre NGFWs und Prisma Access-Bereitstellungen weitergegeben wird. Erste Schritte:

- ❑ Richten Sie Prisma Access, Ihre NGFWs oder beides mit Strata Cloud Manager ein.
- ❑ Richten Sie Ordner ein, um NGFWs zu gruppieren, die ähnliche Einstellungen erfordern. Prisma Access-Ordner sind vordefiniert und ermöglichen es Ihnen, die Konfiguration basierend auf dem Bereitstellungstyp vorzunehmen: mobile Benutzer, Remote-Netzwerke, Dienstverbindungen.
- ❑ Legen Sie den Verwalten: Konfigurationsumfang fest, in dem Sie arbeiten möchten. Sie können Einstellungen konfigurieren, die global gelten, sowohl für Ihre NGFWs als auch für die Prisma Access-Umgebung. Alternativ können Sie die Konfiguration auch auf bestimmte NGFWs oder Prisma Access-Bereitstellungen basierend auf Ordnern ausrichten.
- ❑ Verwenden Sie Verwalten: Snippets, um eine gemeinsame Basiskonfiguration für eine Gruppe von NGFWs oder Bereitstellungen zu standardisieren. Mit Snippets können Sie neue Geräte, Benutzer oder Standorte mit einer als funktionsfähig bekannten Konfiguration schnell einbinden und so die Zeit für das Onboarding neuer Geräte reduzieren.
- ❑ Gehen Sie zu **Verwalten** > **Konfiguration** > **NGFWs und Prisma Access**, um mit der Erstellung Ihrer Sicherheitsrichtlinie zu beginnen und sie mithilfe der oben beschriebenen Verwaltungsfunktionen an Ihre NGFWs und Prisma Access weiterzugeben.



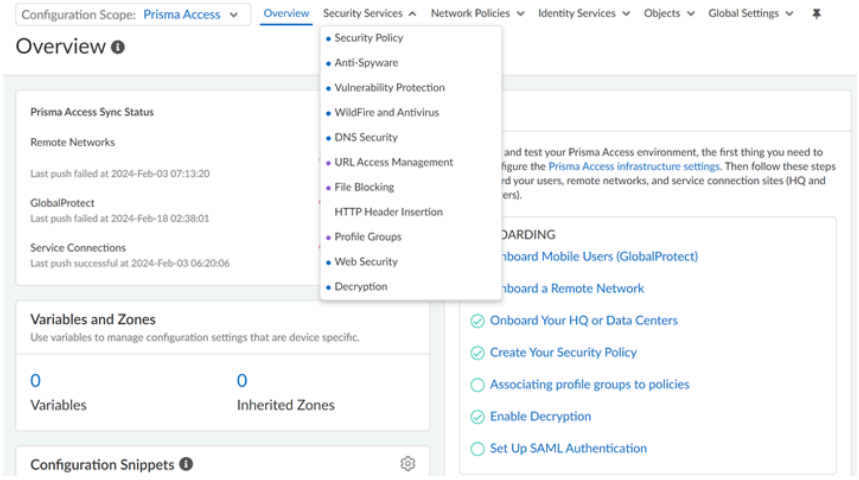
# Verwalten: Konfigurationsumfang

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>❑ Prisma Access<br>❑ AIOps for NGFW Premium<br>❑ Strata Cloud Manager Essentials<br>❑ Strata Cloud Manager Pro<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Mit Strata Cloud Manager können Sie Konfigurationseinstellungen anwenden und Richtlinien global in Ihrer gesamten Umgebung durchsetzen oder Einstellungen und Richtlinien auf bestimmte Teile Ihrer Organisation ausrichten. Bei der Arbeit in Ihrer Strata Cloud Manager-Konfigurationsverwaltung: Der aktuelle **Konfigurationsumfang** ist für Sie immer sichtbar und Sie können Ihre Ansicht umschalten, um eine umfassendere oder detailliertere Konfiguration zu verwalten.

Sie erhalten Klarheit darüber, welche Konfigurationselemente für einen bestimmten Konfigurationsumfang anwendbar sind und ob sie aus einem gemeinsamen Konfigurationsumfang geerbt oder vom System generiert werden. Die farbcodierten Konfigurationsindikatoren helfen Ihnen, zu erkennen, woher die Konfigurationen übernommen werden, und unterscheiden die Objekttypen optisch, um den Überblick zu erleichtern.

- Ein grauer Punkt zeigt eine übernommene Konfiguration an.
- Ein violetter Punkt zeigt eine vordefinierte Konfiguration an.
- Ein blauer Punkt zeigt an, dass das Objekt im aktuellen Konfigurationsumfang vorhanden ist.



Mithilfe **globaler** Konfigurationseinstellungen können Sie Richtlinienanforderungen, die für Ihren gesamten Netzwerkverkehr gelten, problemlos verwalten und durchsetzen. Alternativ können Sie Richtlinien- und Konfigurationseinstellungen auf die Bereitstellungstypen ausrichten, bei denen sie sinnvoll sind.

- **Prisma Access**
  - **Container für mobile Benutzer** – Einstellungen gelten für alle Verbindungstypen für mobile Benutzer: GlobalProtect und expliziter Proxy oder individuell für jeden Verbindungstyp.
  - **Remote-Netzwerke** – Einstellungen gelten für Remote-Netzwerkstandorte (Zweigstellen, Einzelhandelsstandorte usw.).
  - **Dienstverbindungen** – Einstellungen gelten für Dienstverbindungsstandorte (Hauptsitz und Rechenzentren).
- **Alle Firewalls** – Einstellungen gelten für all Ihre NGFWs oder für bestimmte Ordner, in denen NGFWs gruppiert sind, die gemeinsame oder bestimmte Konfigurationseinstellungen oder die Durchsetzung von Richtlinien erfordern.

Erfahren Sie mehr über:

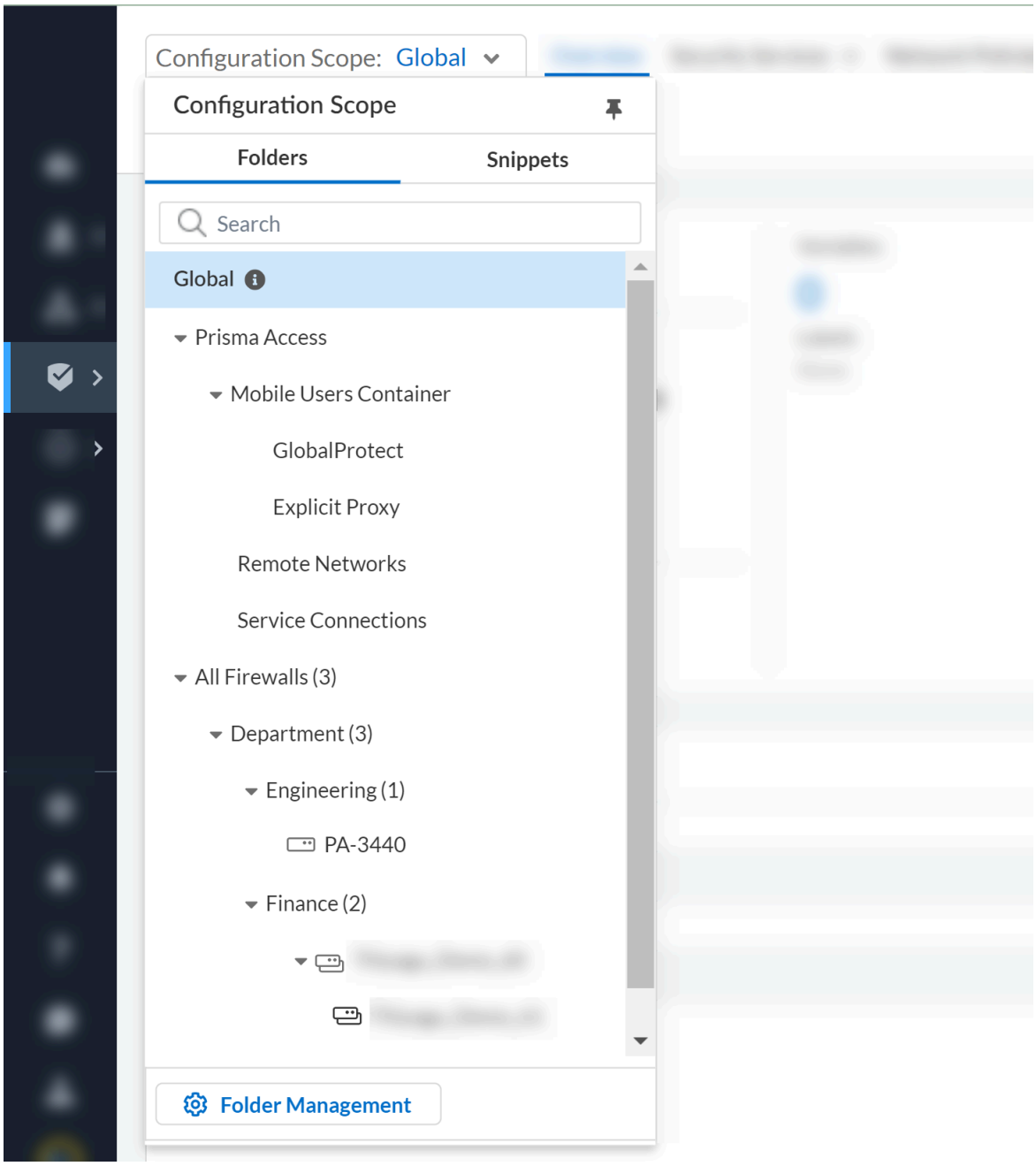
- **Workflows: Ordnerverwaltung**

  Erstellen Sie Ordner, um Ihre Geräte und Bereitstellungstypen logisch zu gruppieren und die Konfigurationsverwaltung zu vereinfachen.
- **Verwalten: Snippets**

  Verwenden Sie Snippets, um Konfigurationen zu gruppieren, die Sie schnell an Ihre Firewalls oder Bereitstellungen übertragen können.
- **Verwalten: Variablen**

  Verwenden Sie Variablen für Ihre Konfigurationen, um geräte- oder bereitstellungsspezifische Konfigurationsobjekte zu berücksichtigen.




# Verwalten: Snippets

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>☐ Prisma Access<br>☐ AIOps for NGFW Premium<br>☐ Strata Cloud Manager Essentials |

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| | ❑ Strata Cloud Manager Pro<br><br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Verwenden Sie Snippets, um Konfigurationen zu gruppieren, die Sie schnell an Ihre Firewalls oder Bereitstellungen übertragen können.

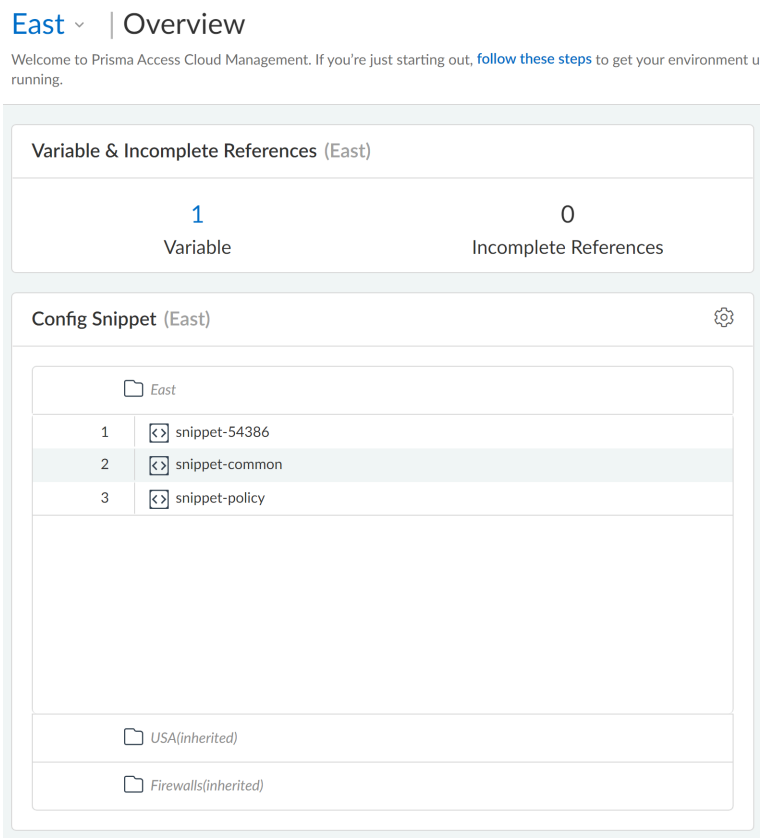
Ein Snippet ist ein Konfigurationsobjekt, das nicht in eine Hierarchie oder Gruppierung von Konfigurationsobjekten passt, die Sie einem Ordner, einer Bereitstellung oder einem Gerät zuordnen können. Snippets werden verwendet, um eine gemeinsame Basiskonfiguration für eine Reihe von Firewalls oder Bereitstellungen zu standardisieren. So können Sie neue Geräte mit einer bekanntermaßen funktionsfähigen Konfiguration schnell integrieren und die Zeit für das Onboarding neuer Geräte reduzieren. Sie können beispielsweise eine neue Firewall in einer Remote-Zweigstelle einbinden. Sie können eine Reihe von Snippets, die alle erforderlichen Netzwerk- und Richtlinienregelkonfigurationen enthalten, dem Ordner zuordnen, zu dem die neue Firewall gehört. Das reduziert die Zeit, die für die nötige Einrichtung der Firewall erforderlich ist, damit sie die Remote-Zweigstelle schützen kann.

Snippet-Zuordnungen haben bei widersprüchlichen Objektwerten eine Priorität von oben nach unten. Regeln mit doppelten Namen sind nicht zulässig und die Validierung schlägt fehl, wenn ein Snippet mit dem gleichen Namen in einem beliebigen Ordner erstellt wird oder wenn ein Snippet einem Ordner zugeordnet wird und ein Snippet mit dem gleichen Namen bereits zugeordnet wurde.

Das heißt, wenn das erste und das letzte zugehörige Snippet unterschiedliche Werte für dasselbe Objekt aufweisen, wird der Wert des ersten Snippets vom Gerät oder der Bereitstellung vererbt. Darüber hinaus können alle von einem Snippet geerbten Konfigurationen auf untergeordneter Ordner-, Bereitstellungs- oder Geräteebene überschrieben werden.

Innerhalb einer Ordnerhierarchie darf ein Snippet nur einmal zugeordnet werden. Das bedeutet, dass ein Snippet nicht sowohl einem Ordner als auch dem darunter liegenden Ordner zugeordnet werden kann. Sie können dasselbe Snippet jedoch mit verschiedenen (unter anderen Ordnern) verschachtelten Ordnern verknüpfen. Snippets, die bereits mit einem Ordner in der Ordnerhierarchie verknüpft sind, sind ausgegraut, sodass sie entsprechend nur einmal verwendet werden können.




## Umfangsübergreifende Referenzierbarkeit von Konfigurationen in Snippets

Mit dieser Funktion können Sie auf alle gängigen Konfigurationen oder Objekte verweisen, die einem globalen Umfang zugeordnet sind, und sie an Prisma Access und NGFWs übertragen. Diese gemeinsamen Objekte und Konfigurationen innerhalb des globalen Umfangs sind für alle Snippets verfügbar. Ein Snippet, das dem globalen Umfang zugeordnet ist, wird als globales Snippet betrachtet. Objekte, die in diesen, an den globalen Umfang angehängten Snippets definiert sind, können in allen Snippets in der Konfiguration referenziert werden.

Sie können beispielsweise ein Snippet mit dem Namen „Globale Variable“ erstellen, um Variablen zu konsolidieren und an einen globalen Umfang anzuhängen. Das gewährleistet eine einfache Referenzierbarkeit und Verfügbarkeit für alle anderen Snippets in der Konfiguration. Ebenso können Sie benutzerdefinierte URL-Kategorien für Zugriffsrichtlinienregeln, Bedrohungsabwehrprofile, Zonen, Adressen und andere Objekte, die Standardnetzwerksegmente darstellen, effektiv verwalten.

## Erstellen eines Snippets

Erstellen Sie ein Snippet und verknüpfen Sie es mit einem Ordner, einer Bereitstellung oder einem Gerät, um eine gemeinsame Basiskonfiguration auf eine Gruppe von Geräten anzuwenden. Sie können einem Ordner, einer Bereitstellung oder einem Gerät beliebig viele Snippets zuordnen.

Snippets können jederzeit nach der Erstellung geändert und mit jedem Ordner, jeder Bereitstellung oder jedem Gerät neu verknüpft werden.

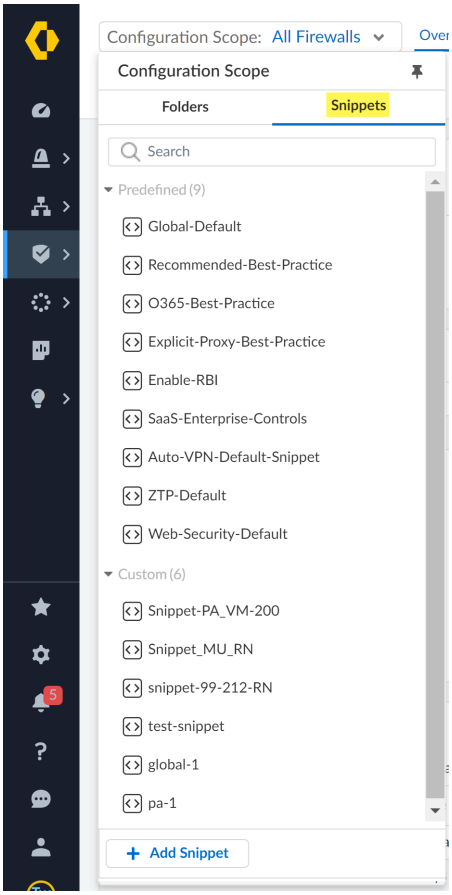
Benutzerdefinierte Snippets, die nicht mehr verwendet werden, können gelöscht werden.

**STEP 1 |** Melden Sie sich bei Strata Cloud Manager an.

**STEP 2 |** Wählen Sie **Verwalten** > **Konfiguration** > **NGFW and Prisma Access** > **Übersicht** aus und erweitern Sie den Konfigurationsumfang, um die **Snippets** anzuzeigen.

**STEP 3 |** Wählen Sie **Snippet hinzufügen**.



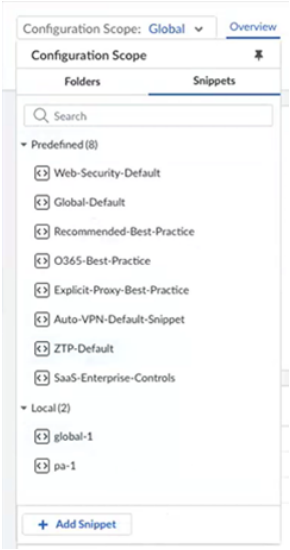

 

**STEP 4 |** Erstellen Sie das Snippet.

1. Geben Sie dem Snippet einen aussagekräftigen **Namen**.
2. (Optional) Geben Sie eine **Beschreibung** für das Snippet ein.
3. (Optional) Weisen Sie ein oder mehrere **Beschriftungen** zu.

   Sie können eine vorhandene Beschriftung auswählen oder eine neue Beschriftung erstellen, indem Sie die Beschriftung eingeben, die Sie erstellen möchten.
4. **Create (Erstellen)**.

   Neu erstellte Snippets werden unter **Lokal** aufgeführt. Nachdem die Snippets veröffentlicht wurden, werden sie zu „Veröffentlicht“ verschoben.




**STEP 5 |** Erstellen Sie Ihre Snippet-Konfiguration.

Sie befinden sich jetzt im Konfigurationsumfang für das Snippet. Alle Konfigurationen, die Sie im Snippet-Umfang erstellen, gelten nur für das Snippet.

Während Sie sich im Snippet-Umfang befinden, können Sie die **Snippet-Übersicht** überprüfen, um detaillierte Informationen zum Snippet zu erhalten. Dazu gehören Informationen wie die Anzahl der Variablen, Informationen über das Snippet, das erstellt und zuletzt aktualisiert wurde, sowie die Liste aller Ordner, Bereitstellungen und Geräte, mit denen das Snippet verknüpft ist.

**STEP 6 |** Verknüpfen Sie ein Snippet.

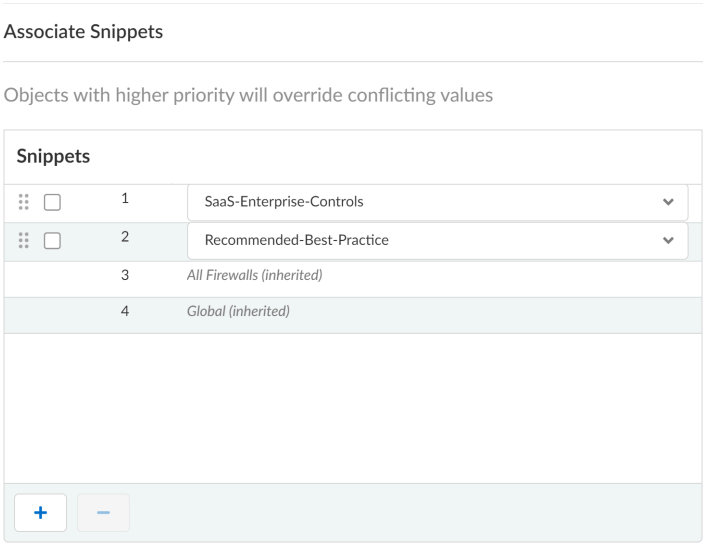
1. Wählen Sie **Verwalten** > **Konfiguration** > **NGFW and Prisma Access** > **Übersicht** aus und erweitern Sie den Konfigurationsumfang, um den **Konfigurationsbaum** anzuzeigen.
2. Wählen Sie den Ordner, die Bereitstellung oder das Gerät aus, dem Sie das Snippet zuordnen möchten.
3. Bearbeiten Sie das **Konfigurations-Snippet**.
4. Fügen Sie die Snippets hinzu, die Sie verknüpfen möchten, und ordnen Sie sie nach Bedarf an.

   Wenn Sie ein Snippet dem globalen Umfang zuordnen, wird es referenzierbar und steht allen anderen Snippets in der Konfiguration zur Verfügung. Alle Snippets können auf

die Objekte verweisen, die in dem Snippet vorhanden sind, das an den globalen Ordner angehängt ist.

5. Wählen Sie **Schließen**.




**STEP 7 |** Wählen Sie **Konfiguration übertragen**, um Ihre Konfigurationsänderungen in Ihr Netzwerk zu übertragen.

## Ändern eines Snippets

Ändern Sie Ihre Snippet-Konfigurationen, -Details und -Zuordnungen.

Benutzerdefinierte Snippets, die nicht mehr mit einem Ordner, einer Bereitstellung oder einem Gerät verknüpft sind, können gelöscht werden.

**STEP 1 |** Melden Sie sich bei Strata Cloud Manager an.

**STEP 2 |** Wählen Sie **Verwalten** > **Konfiguration** > **NGFW and Prisma Access** > **Übersicht** aus und erweitern Sie den Konfigurationsumfang, um die **Snippets** anzuzeigen.

**STEP 3 |** Wählen Sie das Snippet aus, das Sie ändern möchten.

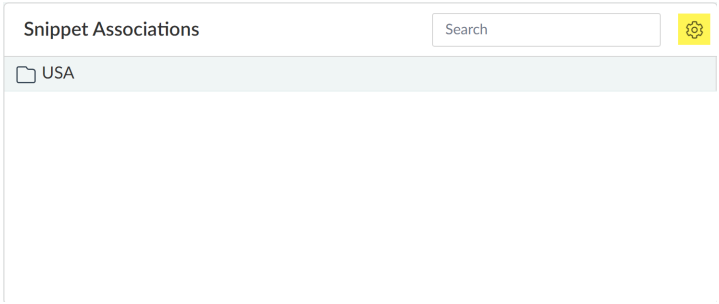
Nachdem Sie ein Snippet ausgewählt haben, werden Sie zur Snippet-**Übersicht** weitergeleitet.

**STEP 4 |** (Optional) Bearbeiten Sie das Snippet, um den **Namen** und die **Beschreibung** zu ändern oder zusätzliche **Beschriftungen** zuzuweisen. Aktivieren oder deaktivieren Sie **Update pausieren**, um die Konfigurationsunterschiede zu sehen und zu entscheiden, ob Sie die Änderung akzeptieren.

**STEP 5 |** Bearbeiten Sie die **Snippet-Zuordnungen**, um das Snippet einem anderen Ordner, einer anderen Bereitstellung oder einem anderen Gerät neu zuzuordnen oder um das Snippet weiteren Ordnern, Bereitstellungen oder Geräten zuzuordnen.

Verlassen Sie den Bildschirm zum erneuten Zuordnen von Snippets, um die Änderungen zu übernehmen.




**STEP 6 |** Nehmen Sie nach Bedarf Änderungen an der Snippet-Konfiguration vor.

**STEP 7 |** Wählen Sie **Konfiguration übertragen** aus.

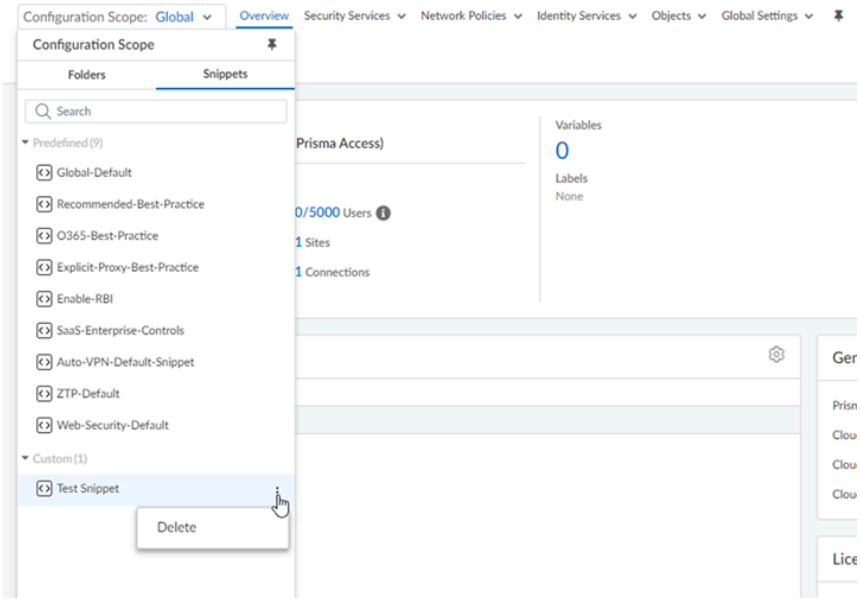
## Löschen eines Snippets

Löschen Sie Ihre benutzerdefinierten Snippets, um Ihre Konfigurationen zu organisieren. Die Verknüpfung von Snippets mit Firewalls, Ordnern oder Bereitstellungen muss aufgehoben werden, bevor sie gelöscht werden können. Das Löschen vordefinierter Snippets wird nicht unterstützt.

**STEP 1 |** Melden Sie sich bei Strata Cloud Manager an.

**STEP 2 |** Wählen Sie **Verwalten** > **Konfiguration** > **NGFW and Prisma Access** > **Übersicht** aus und erweitern Sie den **Konfigurationsumfang**, um die Snippets anzuzeigen.

**STEP 3 |** Klicken Sie auf das Drei-Punkte-Symbol des benutzerdefinierten Snippets, das Sie löschen möchten.



**STEP 4 |** **Löschen** Sie das Snippet.

> *Snippets, die derzeit Ordnern, Bereitstellungen oder Geräten zugeordnet sind, können nicht gelöscht werden. Bearbeiten Sie zunächst die **Snippet-Zuordnungen**, um alle vorhandenen Verknüpfungen zu entfernen, damit das Snippet gelöscht werden kann.*

## Klonen eines Snippets

Wenn Sie ein vorhandenes Snippet als Vorlage für ein neues Snippet verwenden möchten, können Sie es einfach klonen, sodass Sie kein neues Objekt konfigurieren müssen.

Geklonte Snippets sind keinen Geräten, Ordnern oder Bereitstellungen zugeordnet, sodass Sie sie beliebig anpassen können, ohne vor Beginn der Konfiguration die Zuordnung aufheben zu müssen.

**STEP 1 |** Melden Sie sich bei Strata Cloud Manager an.

**STEP 2 |** Wählen Sie **Verwalten** > **Konfiguration** > **NGFW and Prisma Access** > **Übersicht** aus und erweitern Sie den **Konfigurationsumfang**, um die Snippets anzuzeigen.

**STEP 3 |** Klicken Sie auf das Drei-Punkte-Symbol des benutzerdefinierten Snippets, das Sie klonen möchten.

**STEP 4 |** **Klonen** Sie das Snippet.

1. (Optional) Geben Sie dem geklonten Snippet einen neuen Namen.

## Freigeben einer Snippet-Konfiguration

Diese Funktion bietet eine einzigartige und flexible Methode zur gemeinsamen Nutzung gemeinsamer Konfigurationen für alle Mandanten – auch in einer Umgebung mit mehreren Mandanten. Sie können verschiedene Konfigurationen als Snippets speichern und verwalten und sie dann problemlos unter einem Kundenkonto für alle Mandanten freigeben. Diese Funktion bietet erhebliche Flexibilität und Kontrolle bei der Verwaltung gemeinsam genutzter Konfigurationen in verschiedenen Mandantenumgebungen.

Darüber hinaus unterstützt diese Funktion die Zentralisierung des Konfigurationsmanagements für gängige Mandantenszenarien und die Überwachung globaler Konfigurationen in Setups mit mehreren Geschäftseinheiten.

In diesem Framework teilt der Herausgeber-Mandant Snippets mit dem Abonnent-Mandaten und der Abonnent-Mandant empfängt die Snippets vom Herausgeber-Tenant.

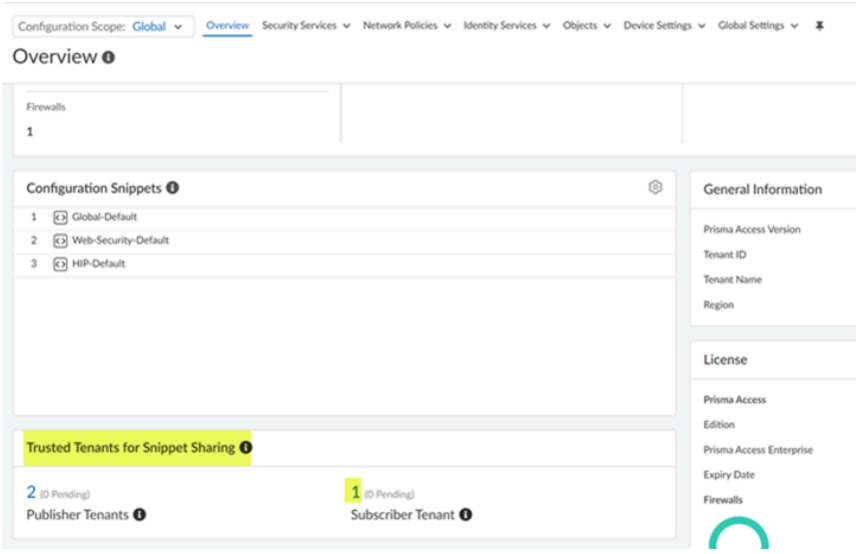
**STEP 1 |** Melden Sie sich bei Strata Cloud Manager an.

**STEP 2 |** Wählen Sie auf dem Herausgeber-Mandanten **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Übersicht** aus und wählen Sie den Konfigurationsumfang **Global** aus.

**STEP 3 |** **Stellen Sie Vertrauen zwischen den Mandanten her**: Stellen Sie eine Verbindung zwischen den Abonnent- und Herausgeber-Mandanten her, um die Freigabe von Snippets zu ermöglichen.

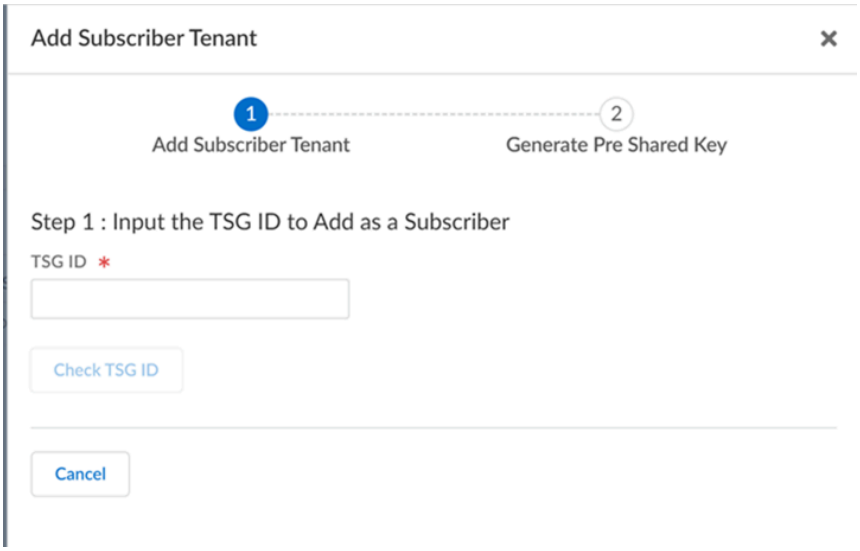
1. Klicken Sie unter **Vertrauenswürdige Mandanten für die Snippet-Freigabe** auf die Option **Abonnent-Mandant**.




2. Wählen Sie **Abonnent-Mandanten hinzufügen** aus.


3. Geben Sie die **TSG-ID** ein, die Sie als Abonnent-Mandant hinzufügen möchten, und wählen Sie **TSG-ID prüfen** aus. So werden Angriffe mit zufällig generierten oder serialisierten TSG-IDs verhindert.

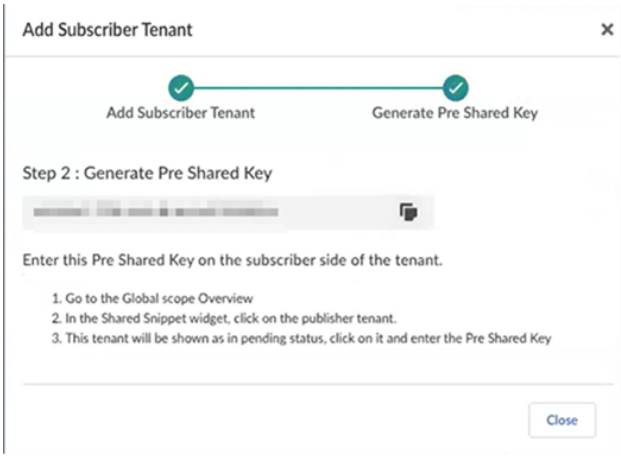
   Nach erfolgreicher Validierung gibt eine Bestätigungsmeldung an, dass die TSD-ID verifiziert wurde.




4. **Nächster Schritt: Generieren Sie den Pre Shared Key**.

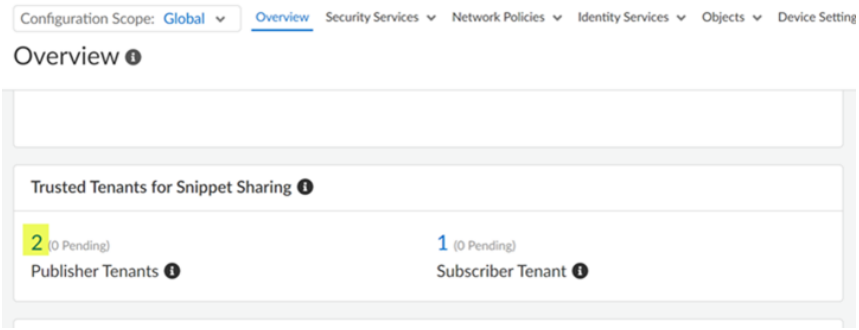
 

Kopieren Sie den generierten PSK. Sie geben diesen PSK ein, wenn Sie den Herausgeber-Mandanten in Schritt 4 validieren.



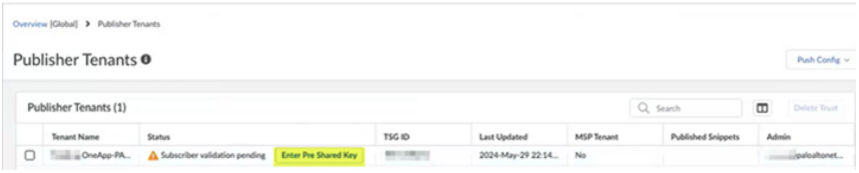

**STEP 4 |** Wählen Sie auf dem Abonnent-Mandanten **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Übersicht** aus und wählen Sie den Konfigurationsumfang **Global** aus.

1. Der **Herausgeber-Mandanten**-Status unter **Vertrauenswürdige Mandanten für die Snippet-Freigabe** wird als **Ausstehend** angezeigt.




2. Klicken Sie auf **Herausgeber-Mandanten**, geben Sie unter **Pre Shared Key eingeben** den im vorherigen Schritt generierten Pre Shared Key ein und **validieren** Sie den Abonnent-Mandanten.

   Nach erfolgreicher Überprüfung bestätigt eine Meldung, dass der Mandant als vertrauenswürdig eingestuft wird, wodurch Vertrauen zwischen den Abonnent- und Herausgeber-Mandanten hergestellt wird.



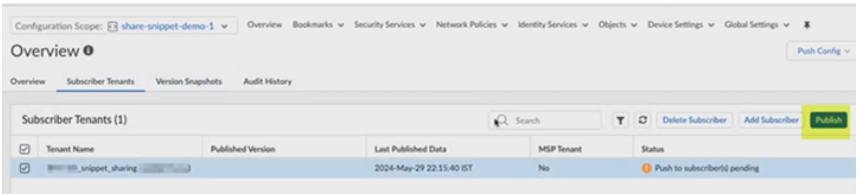
**STEP 5 |** Veröffentlichen Sie ein Snippet für einen Abonnent-Mandanten.

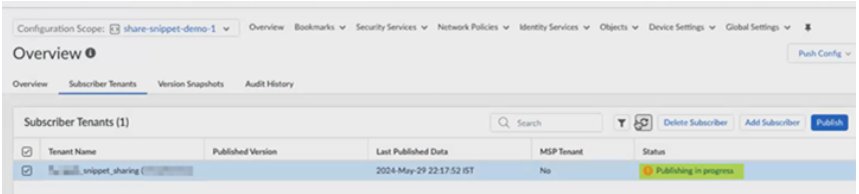
1. Erstellen Sie das Snippet und verknüpfen Sie es mit einem Ordner.

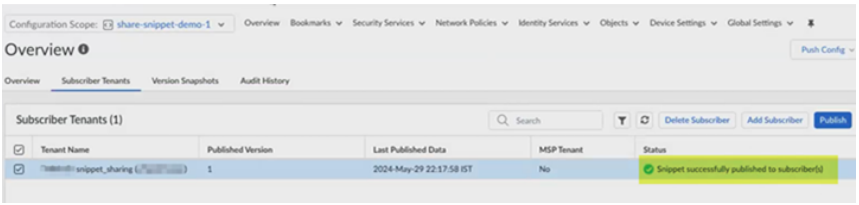
   Neu erstellte Snippets sind unter **Lokal** verfügbar.

   - Auf der Registerkarte **Übersicht** werden Snippet-Details wie Name, Beschreibung, Erstellungszeit (als das Snippet auf Abonnentenseite geladen wurde), Uhrzeit der letzten Aktualisierung sowie Beschriftungsdetails angezeigt.
   - Auf der Registerkarte **Abonnent-Mandanten** werden der Mandantenname, die veröffentlichte Version auf dem Mandanten, das Datum der letzten Veröffentlichung sowie der Veröffentlichungsstatus angezeigt.
     - Klicken Sie auf **Veröffentlichte Version**, um die Konfigurationsänderungen zu überprüfen.
     - Bevor Sie ein Snippet für einen Mandanten veröffentlichen, wählen Sie **Abonnenten hinzufügen** und **speichern** Sie Ihre Eingaben.
   - Die **Versions-Snapshots** enthalten einen Verlauf Ihrer Snippet-Konfiguration. Auf diesem Bildschirm können Sie Konfigurations-Snapshots mit Ihrer Kandidatenkonfiguration vergleichen und den **Versions-Snapshot speichern** oder einen früheren Konfigurations-Snapshot als Ihren Kandidaten **laden**. Klicken Sie auf die Nummer unter **Version**, um die Konfigurationsunterschiede anzuzeigen.
   - Der **Prüfverlauf** bietet einen Prüfpfad für alle Aktionen, die vom Administrator initiiert wurden. Er protokolliert Details wie die veröffentlichte Versionsnummer, vorgenommene Änderungen, den Eigentümer der Änderung, Datum und Uhrzeit der Änderung sowie Einzelheiten zur Änderung.
2. Wählen Sie auf der Registerkarte **Abonnent-Mandant** den Mandantennamen aus und klicken Sie auf **Veröffentlichen**.

   Hierdurch wird die Veröffentlichungsanfrage an den Abonnent-Mandanten gesendet. In der Spalte **Status** wird angegeben, dass das Snippet erfolgreich für den Abonnenten veröffentlicht wurde und das Snippet unter „Veröffentlicht“ verfügbar sein wird.



**STEP 6 |** Überprüfen Sie den Abonnent-Mandanten.

1. Gehen Sie zu **Übersicht** > **Konfigurationsumfang** > **Snippets** und wählen Sie das Snippet unter **Abonniert** aus.

   Sie werden zur Snippet-**Übersicht** weitergeleitet, in der Details wie Name, Beschreibung, TSG-ID, Zeitpunkt der Erstellung des Snippets, Uhrzeit der letzten Aktualisierung sowie Bezeichnungen und Details zum Pausieren der Aktualisierung angezeigt werden.

**STEP 7 |** Löschen Sie die Vertrauensstellung.

*Abonnierte Snippets, die Ordnern oder Firewalls zugeordnet sind, können nur geklont, jedoch nicht gelöscht werden.*

1. Gehen Sie zum Abonnent- oder Herausgeber-Mandanten.
2. Klicken Sie unter **Vertrauenswürdige Mandanten für die Snippet-Freigabe** auf die Option **Abonnent-Mandant**.
3. Wählen Sie den **Mandantennamen** aus und wählen Sie dann **Vertrauensstellung löschen**.

Nach dem Löschen der Vertrauensstellung ist das Snippet nicht mehr mit der Firewall oder dem Ordner verknüpft und wird zu einem lokalen Snippet.

## Snippet-Klassifizierung

- Vordefiniert: Alle Strata Cloud Manager-Benutzer können auf diese Snippets zugreifen, um schnell neue Firewalls und Bereitstellungen mit Best-Practice-Konfigurationen einzurichten.
- Lokal: Diese bearbeitbaren Snippets werden innerhalb des Mandanten erstellt und können nicht mit anderen Abonnent-Mandanten geteilt werden.
- Veröffentlicht: Vertrauenswürdige Abonnent-Mandanten haben Zugriff auf diese geteilten Snippets, die nicht geklont oder bearbeitet werden können.

- Abonniert: Diese Snippets, die vom Herausgeber-Mandanten freigegeben werden, können von Benutzern geklont, jedoch nicht bearbeitet werden.


# Verwalten: Variablen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>☐ Prisma Access<br>☐ AIOps for NGFW Premium<br>☐ Strata Cloud Manager Essentials<br>☐ Strata Cloud Manager Pro<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Verwenden Sie Variablen für Ihre Konfigurationen, um geräte- oder bereitstellungsspezifische Konfigurationsobjekte zu berücksichtigen.

Variablen sind ein erweitertes Tool, mit dem Sie Ihre Konfigurationen standardisieren können. Sie bieten Ihnen die nötige Flexibilität, um einzigartige Konfigurationswerte zu berücksichtigen, die geräte- oder bereitstellungsspezifisch sind. Mit Variablen können Sie die Anzahl der zu verwaltenden Snippets reduzieren und gleichzeitig firewall- oder bereitstellungsspezifische Konfigurationseinstellungen nach Bedarf beibehalten.

Nehmen wir an, Sie verfügen über ein Snippet für die Konfiguration, das Sie mit mehreren verschachtelten Ordnern verknüpfen möchten, wobei jeder verschachtelte Ordner eine Reihe von Firewalls enthält, die für einen geografischen Standort spezifisch sind. Im Snippet haben Sie Richtlinienregeln konfiguriert, um den Zugriff auf geschäftskritische Systeme nur auf spezifische IP-Bereiche zu beschränken. In diesem Szenario können Sie für jeden IP-Bereich, der für jeden verschachtelten Ordner spezifisch ist, eine Variable erstellen und diese Variable in der geerbten Snippet-Konfiguration verwenden. Auf diese Weise können Sie Konfigurationsänderungen verwalten und übertragen und müssen gleichzeitig weniger Snippets verwenden, um geräte- oder bereitstellungsspezifische Konfigurationswerte zu berücksichtigen.

Variablen können auf Ordner-, Bereitstellungs- oder Firewallebene erstellt werden. Wenn Sie eine Variable für einen Ordner erstellen, wird die Variable an alle unter diesem Ordner verschachtelten Ordner vererbt. Im Falle widersprüchlicher Variablen im Konfigurationsumfang eines Ordners erbt die Firewall oder Bereitstellung den Variablenwert aus dem Ordner, der die verschachtelten Ordner enthält. Sie können jedoch eine geerbte Variable auf Ebene des verschachtelten Ordners, der Bereitstellung oder der Firewall überschreiben.

Die folgenden Variablentypen werden unterstützt:

| Variablentyp | Beschreibung |
|---|---|
| **AS-Anzahl** | Autonome Systemnummer zur Verwendung in Ihrer BGP-Konfiguration. |
| **Anzahl** | Anzahl der Ereignisse, die auftreten müssen, um eine Aktion auszulösen. |
| **Geräte-ID** | Zu verwendende Geräte-ID zum Zuweisen eines Gerätepriorität swerts in einer Aktiv/Aktiv-HA-Konfiguration (High Availability, HA). |
| **Gerätepriorität** | Gerätepriorität, um anzugeben, welche Firewall in einer Aktiv/Passiv-HA-Konfiguration die aktive Rolle übernehmen soll. |
| **Ausgang maximal** | Maximaler ausgehender Wert zur Verwendung in der Konfiguration des QoS-Profils (Quality of Service). |
| **FQDN** | Vollqualifizierter Domänenname. |
| **Gruppen-ID** | Hochverfügbarkeits-Gruppen-ID. |
| **IP-Netzmaske** | Statische IP- oder Netzwerkadresse. |
| **IP-Bereich** | Ein IP-Bereich. Beispiel: **`192.168.1.10-192.168.1.20`**. |
| **IP-Platzhalter** | IP-Platzhaltermaske zum Zulassen oder Ablehnen ähnlicher IP-Adressen. Beispiel: `10.0.0.5/255.255.0.255`. |

| Variablentyp | Beschreibung |
|---|---|
| **Link-Tag** | Link-Tag zur Verwendung in Ihrer SD-WAN-Konfiguration. |
| **Prozent** | Prozentsatz zwischen **0** und **99**. |
| **Port** | Quell- oder Zielport. |
| **QoS-Profil** | QoS-Profil zur Verwendung in QoS-Konfigurationen. |
| **Rate** | Rate, um einen Schwellenwert festzulegen, der eine Aktion auslöst. Beispielsweise die `Alarmrate` für ein DoS-Schutzprofil. |
| **Router-ID** | Router-ID, wenn Sie Border Gateway Protocol (BGP) für einen logischen Router konfigurieren. |
| **Timer** | Timer in Sekunden zum Konfigurieren eines Schwellenwerts, der eine Aktion auslöst. |
| **Zone** | Eine Sicherheitszone. |

## Erstellen einer Variablen

*Sie können eine Variable auch inline erstellen, sofern die entsprechende Variable unterstützt wird.*

**STEP 1 |** Melden Sie sich bei Strata Cloud Manager an.

**STEP 2 |** Wählen Sie **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Übersicht** aus und wählen Sie den Konfigurationsumfang aus, in dem Sie die Variable erstellen möchten.

Wählen Sie unter **Ordner** den Ordner oder das Gerät aus, für den bzw. das Sie eine Variable erstellen möchten.

Wählen Sie in den **Snippets** das spezifische Snippet aus, für das Sie eine Variable erstellen möchten.

**STEP 3 |** Klicken Sie im Abschnitt „Variablen“ auf die angezeigte Variablenanzahl.

**STEP 4 |** Wählen Sie **Variable hinzufügen**.

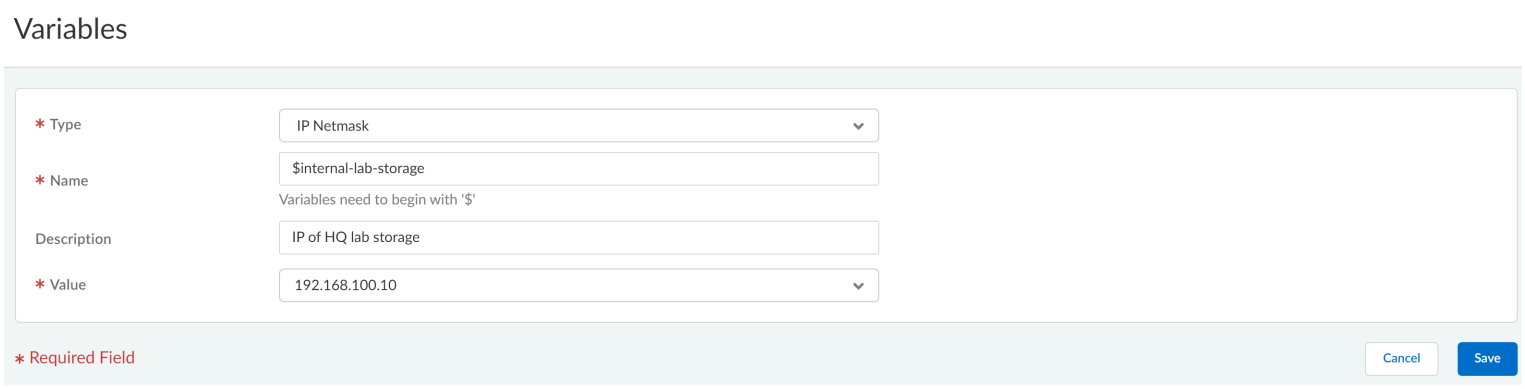
 

**STEP 5 |** Erstellen Sie die Variable.

In diesem Beispiel wird eine `IP-Netzmasken`-Variable zur Verwendung als Adressobjekt für eine kritische interne Ressource erstellt.

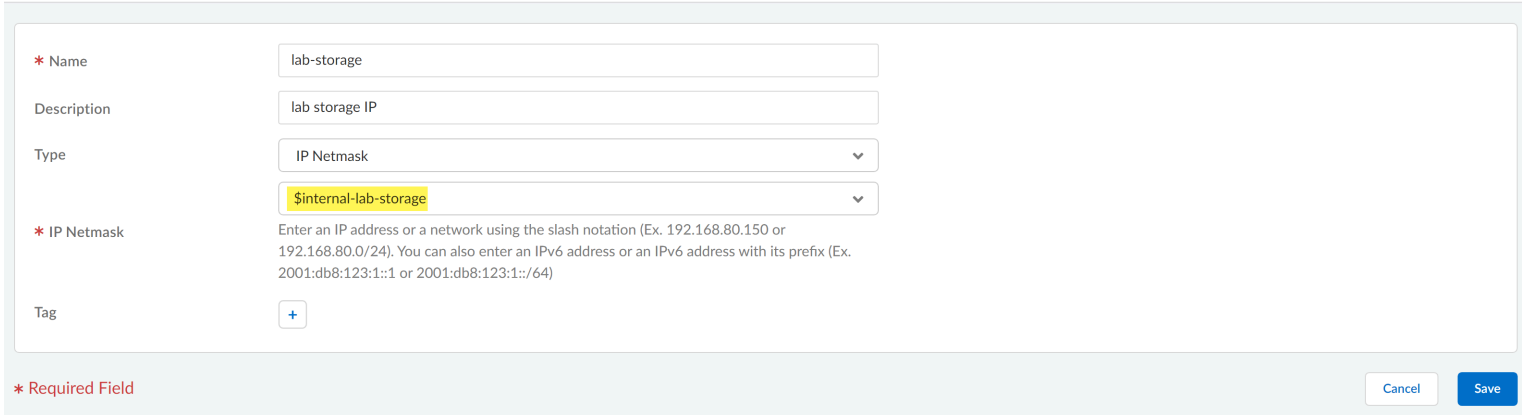
1. Wählen Sie den **Typ** der Variablen aus.
2. Geben Sie der Variablen einen aussagekräftigen **Namen**.

   Alle Variablennamen müssen mit **$** beginnen.
3. (Optional) Geben Sie eine **Beschreibung** für die Variable ein.
4. Geben Sie den **Wert** der Variablen ein.
5. Klicken Sie auf **Speichern**.




**STEP 6 |** Fügen Sie die Variable zu Ihrer Konfiguration hinzu.

In diesem Beispiel wird die im vorherigen Schritt erstellte Variable `$internal-lab-storage` zur Adressobjektkonfiguration hinzugefügt.




**STEP 7 |** Wählen Sie **Konfiguration übertragen**.

## Importieren einer Variablen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Strata Cloud Manager | ❑ AIOps for NGFW Premium-Lizenz |

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| | ❑ Prisma Access-Lizenz |

Importieren Sie Variablen mithilfe einer CSV-Datei in Strata Cloud Manager. Variablenimporte dienen dazu, mehrere Variablen, die die Firewall von der Ordnerhierarchie geerbt hat oder die bereits im Konfigurationsumfang der Firewall konfiguriert sind, mit neuen, firewallspezifischen Werten zu überschreiben.

Die Variable muss bereits aus der Ordnerhierarchie geerbt oder im Konfigurationsumfang der Firewall konfiguriert sein, um durch Variablenimporte überschrieben zu werden. Das Importieren von Variablen zum Erstellen gänzlich neuer Variablen wird nicht unterstützt.

**STEP 1 |** Melden Sie sich bei Strata Cloud Manager an.

**STEP 2 |** Wählen Sie **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Übersicht**.

**STEP 3 |** Klicken Sie im Abschnitt „Variablen“ auf die angezeigte Variablenanzahl.

**STEP 4 |** Wählen Sie **CSV-Export/Import** > **Exportieren** aus, um die Variablen zu exportieren, die Sie überschreiben möchten.

Palo Alto Networks empfiehlt, zunächst die Variablen zu exportieren, die Sie überschreiben möchten. Hierdurch wird sichergestellt, dass die CSV-Datei, die Sie in Strata Cloud Manager hochladen, richtig formatiert ist. So wird auch der Importvorgang beschleunigt, da sichergestellt wird, dass die Zielordner und Firewallvariablen richtig zugeordnet sind.

**STEP 5 |** Ändern Sie die Variablen in der exportierten CSV-Datei.

Beachten Sie Folgendes, wenn Sie Ihre CSV-Datei für den Import ändern.

- Zum Ändern einer exportierten CSV-Datei werden nur einfache Texteditoren wie Notepad unterstützt.
- # bedeutet, dass die Variable in der Ordnerhierarchie erstellt und von der Firewall geerbt wird.

  Entfernen Sie das #, um den geerbten Variablenwert mit einem firewallspezifischen Wert zu überschreiben.

  Ein Variablenwert mit # wird von Strata Cloud Manager beim Import ignoriert, da nur das Überschreiben von Variablenwerten im Konfigurationsumfang der Firewall unterstützt wird.
- `-NA-` bedeutet, dass die Variable in der Firewall-Konfiguration nicht vorhanden ist. Das heißt, dass die Variable außerhalb der Ordnerhierarchie erstellt wurde, zu der die Firewall gehört.

  Das Ändern eines Variablenwerts zu `-NA-` wird nicht unterstützt. Strata Cloud Manager ignoriert alle Variablenwerte, die zu `-NA-` geändert wurden.

  Die Zuweisung eines firewallspezifischen Werts zu einer Variablen mit dem Wert `-NA-` wird nicht unterstützt, da die Variable im Konfigurationsumfang der Firewall nicht vorhanden

ist. Die Variable muss aus der Ordnerhierarchie geerbt oder im Konfigurationsumfang der Firewall konfiguriert worden sein, um durch den Variablenimport überschrieben zu werden.

- Ein Variablenwert von `Keine#` oder `Keine` bedeutet, dass die Variable mit dem **Variablenwert Keine** erstellt wurde.

  Sie können jeden Variablenwert zu `Keine` ändern, um den Wert zu entfernen, die Variable jedoch nicht zu löschen.
- Wenn Sie bei einer Variablen, die im Konfigurationsumfang der Firewall erstellt wurde, einen Variablenwert löschen und ihn leer lassen, wird die Variable gelöscht.

  Wenn Sie bei einer Variablen, die in der Ordnerhierarchie erstellt und von der Firewall geerbt wurde, einen Variablenwert löschen und leer lassen, wird der Variablenwert auf den aus der Ordnerhierarchie geerbten Wert zurückgesetzt.

1. Suchen und öffnen Sie die exportierte CSV-Datei. Das Format der exportierten CSV-Datei lautet:

   `<cloud-management-tenant-name> - Prisma Access_<export-date>_variables`
2. Ändern Sie die Variablen nach Bedarf.

   *Palo Alto Networks rät davon ab, Ordnernamen, Gerätenamen oder Geräteseriennummern zu ändern, da dies zu Importfehlern führen kann.*

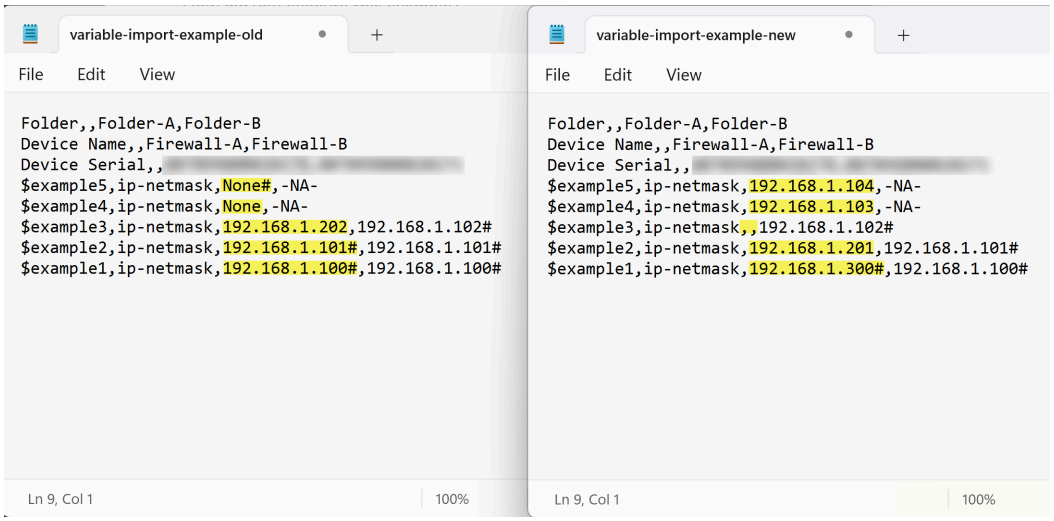
   Im unten stehenden Beispiel wurden die folgenden Änderungen an den Variablenwerten im Konfigurationsumfang `Firewall-A` vorgenommen, um zu veranschaulichen, wie

Variablenimporte verwendet werden können, um mehrere Variablen mit einem Vorgang zu ändern.

- `$example1` – überschreibt den geerbten Wert `None#` mit einem firewallspezifischen Wert.
- `$example2` – überschreibt den firewallspezifischen Wert `None` durch einen firewallspezifischen Wert.
- `$example3` – Wenn die Variable im Konfigurationsumfang der Firewall erstellt wurde, löscht ein leerer Wert die Variable.

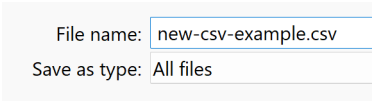
  Wenn die Variable aus der Ordnerhierarchie geerbt und im Konfigurationsumfang der Firewall überschrieben wurde, stellt ein leerer Wert den aus der Ordnerhierarchie geerbten Variablenwert wieder her.
- `$example4` – überschreibt den übernommenen Wert `192.168.1.101` mit einem firewallspezifischen Wert.
- `$example5` – Beispiel einer Variablenänderung, Strata Cloud Manager ignoriert, da # angehängt ist.




**STEP 6 |** Speichern Sie Ihre Änderungen.

Wählen Sie **Datei** > **Speichern** aus, um die an der CSV-Datei vorgenommenen Änderungen zu speichern.

Wählen Sie alternativ **Datei** > **Speichern unter** aus, um Ihre Änderungen in einer neuen CSV-Datei zu speichern. Um eine neue CSV-Datei zu erstellen, müssen Sie **`.csv`** als Dateierweiterung angeben.



**STEP 7 |** Importieren Sie die CSV-Datei in Strata Cloud Manager.

1. Wählen Sie **Verwalten** > **Konfiguration** > **Übersicht** aus.
2. Klicken Sie im Abschnitt „Variablen“ auf die angezeigte Variablenanzahl.
3. Wählen Sie **CSV-Export/Import** > **Importieren** aus.
4. Wählen Sie unter **Datei auswählen** die CSV-Datei mit den von Ihnen geänderten Variablen aus.
5. Wählen Sie **Importieren** aus.

## Exportieren von Variablen

Exportieren Sie Ihren Ordner und Ihre Firewall-Konfigurationsvariablen im CSV-Format auf Ihr lokales Gerät. Das Exportieren Ihrer Variablen ist nützlich, wenn Sie eine große Anzahl von Variablen über mehrere Firewalls hinweg überschreiben wollen.

Das Exportieren von Schnittstellenvariablen, die beim Konfigurieren einer Schnittstelle auf Ordnerebene erstellt werden, wird nicht unterstützt.

**STEP 1 |** Melden Sie sich bei Strata Cloud Manager an.

**STEP 2 |** Wählen Sie **Verwalten** > **NGFW und Prisma Access** > **Konfiguration** > **Übersicht** aus.

**STEP 3 |** Klicken Sie im Abschnitt „Variablen“ auf die angezeigte Variablenanzahl.

**STEP 4 |** Wählen Sie **CSV-Export/Import** > **Exportieren** aus.

**STEP 5 |** Wählen Sie den Ordner und die Firewalls mit den Variablen aus, die Sie exportieren möchten, und klicken Sie auf **Weiter**.

*Wenn Sie alle Variablen exportieren möchten, die in Strata Cloud Manager erstellt wurden, wählen Sie **Alle Firewalls** aus.*

**STEP 6 |** Wählen Sie eine oder mehrere Variablen zum Exportieren aus.

**STEP 7 |** (Optional) Öffnen Sie eine **Vorschau** der ausgewählten Variablen, um weitere Details anzuzeigen.

In der Variablenvorschau können Sie Informationen wie den Variablennamen, den Konfigurationsumfang, in dem die Variable erstellt wurde, sowie den Variablenwert einsehen.

Klicken Sie auf **Abbrechen** und fahren Sie mit dem nächsten Schritt fort oder wählen Sie **CSV herunterladen**, um die CSV-Datei auf Ihr lokales Gerät herunterzuladen.

**STEP 8 |** **Exportieren** Sie die ausgewählten Variablen im CSV-Format.

Die CSV-Datei wird exportiert und lokal auf Ihr Gerät heruntergeladen. Das Format der exportierten CSV-Datei lautet:

```
<cloud-management-tenant-name> - Prisma Access_<export-
date>_variables
```

# Verwalten: Übersicht

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>❑ Prisma Access<br>❑ AIOps for NGFW Premium<br>❑ Strata Cloud Manager Essentials<br>❑ Strata Cloud Manager Pro<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Betrachten Sie die Übersichtsseite als Ihren Einstiegspunkt in NGFW und Prisma Access, sowohl für die Ersteinrichtung als auch für die tägliche Konfigurationsverwaltung (**Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Übersicht**).

- Global
- Prisma Access
- Strata Cloud Manager

## Global

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• NGFW (Managed by Strata Cloud Manager)<br>• NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series, funded with Software NGFW Credits | ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>❑ Prisma Access-Lizenz |

Wenn Sie den Konfigurationsumfang **Global** auswählen, können Sie die folgenden Details anzeigen:

- von Ihnen erstellte globale Ordner und deren Variablen
- Firewalls mit Konfigurationskonflikten
- Firewall-Synchronisierungsstatus und Firewall-Konnektivitätsstatus

- allgemeine Informationen
- Konfigurations-Snippets
- Lizenz
- vertrauenswürdige Mandanten für die Snippet-Freigabe
- Snapshots der Konfigurationsversion

## Konfigurationsübersicht (Prisma Access)

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access-Lizenz |

Wenn Sie gerade erst mit Prisma Access beginnen:

- Die **Grundlagen**-Checkliste zeigt Ihnen, wie Sie mit Prisma Access loslegen können. Führen Sie hier die Aufgaben aus und nutzen Sie die Anleitungen, um mit einer grundlegenden Einrichtung zu beginnen. Testen Sie dann Ihre Umgebung und bauen Sie Ihre Bereitstellung weiter aus.
- Hier erfahren Sie, wie Richtlinien- und Konfigurationsordner funktionieren.
- Hier erfahren Sie, wie Sie Konfigurationsänderungen an Prisma Access übertragen.

**Weitere Informationen zu Ihrer Prisma Access-Umgebung:**

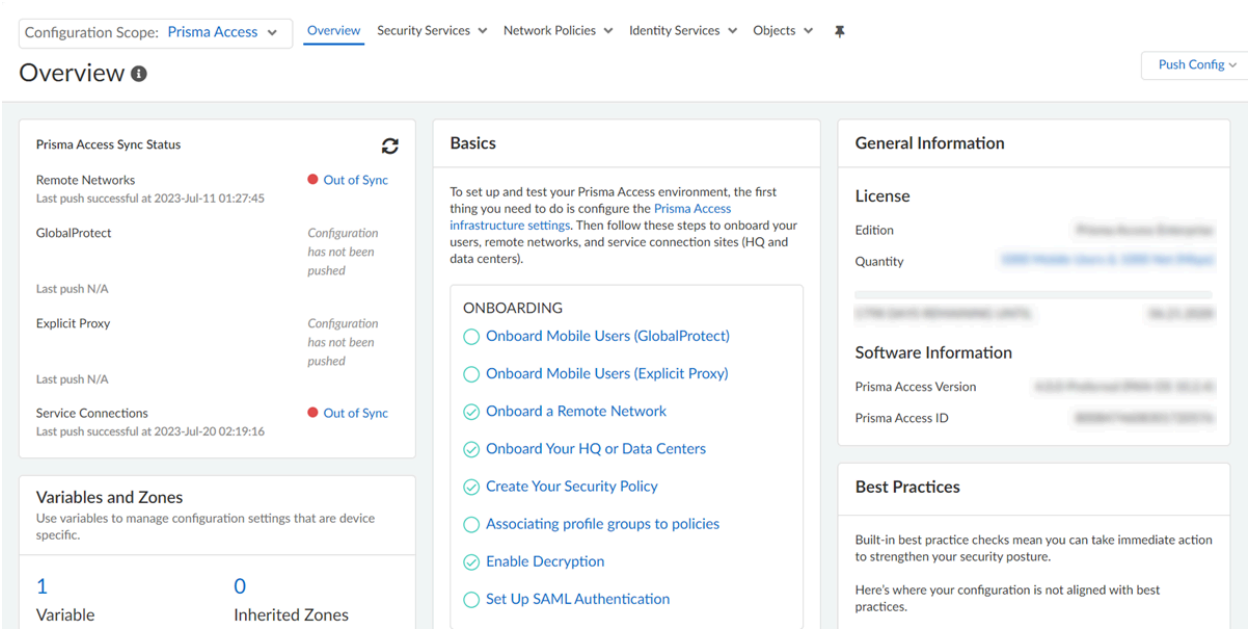
- Überprüfen Sie die **Lizenzdetails**, um zu sehen, was in Ihrem Prisma Access-Abonnement enthalten ist.
- Das **Übersichtsfenster** zeigt die **Software- und Mandanteninformationen** für Ihre Prisma Access-Umgebung an.

**Für das tägliche Konfigurationsmanagement:**

- Sehen Sie den Konfigurationsstatus auf einen Blick.
- Standardisieren Sie eine gemeinsame Basiskonfiguration für eine Gruppe von Prisma Access-Bereitstellungen mithilfe der Konfigurations-Snippets
- Finden Sie Konfigurations-Snapshots – Vergleichen Sie Konfigurationsversionen und stellen Sie eine frühere Version wieder her (oder laden Sie sie), um eine Konfigurationsübertragung mit unbeabsichtigten Auswirkungen auf den Datenfluss rückgängig zu machen oder die Sicherheit wiederherzustellen.
- Optimieren Sie Ihre Konfiguration – Bereinigen Sie nicht verwendete Objekte und Regeln und verschärfen Sie Regeln, die Sicherheitslücken einführen, indem sie Anwendungen zulassen, die Sie nicht verwenden.
- Ermitteln Sie Bereiche, in denen Sie Konfigurationsänderungen vornehmen können, die Ihren Sicherheitsstatus stärken.

- Hier finden Sie auch Details zu Ihrer Prisma Access-Lizenz und dazu, was sie beinhaltet.



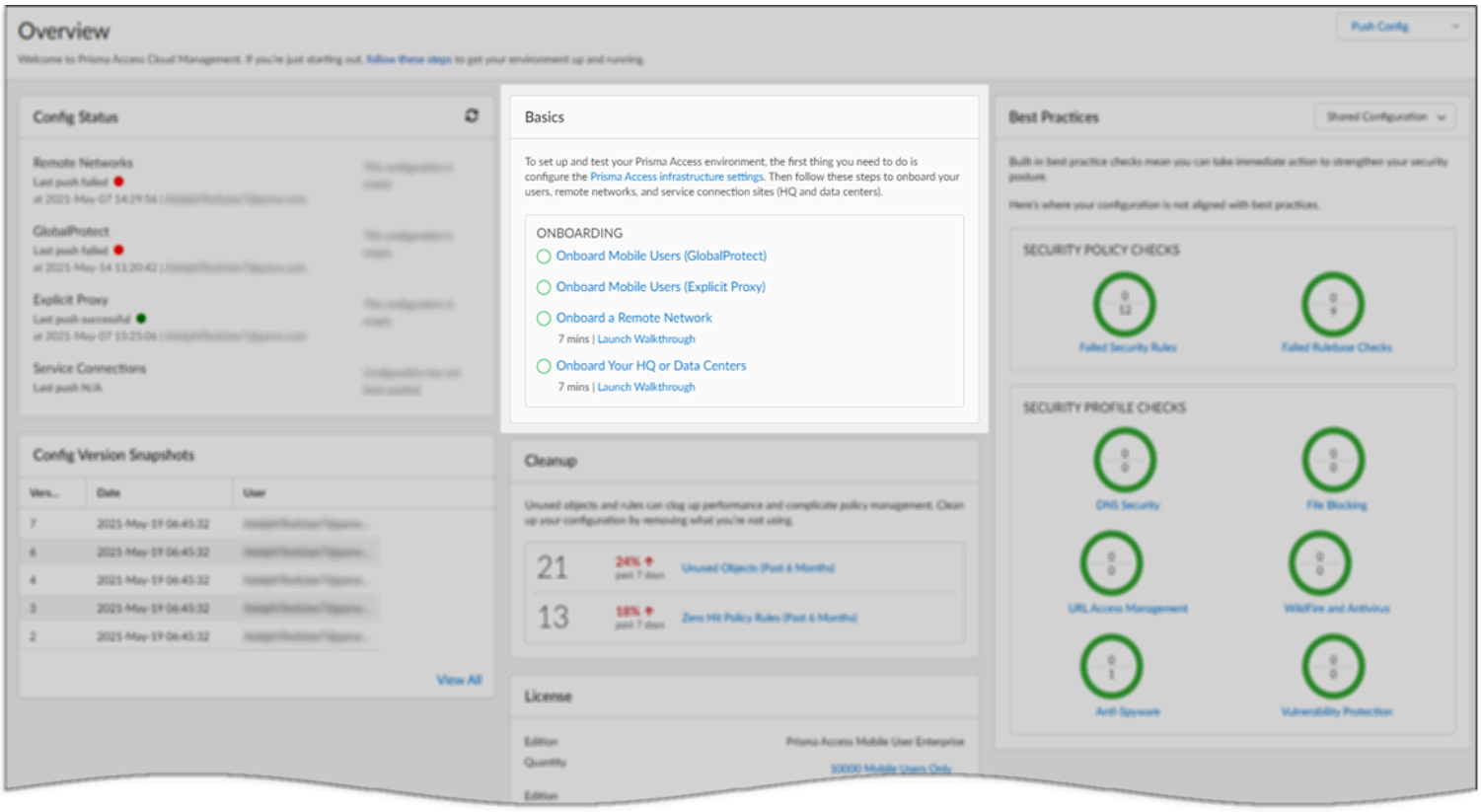

Nach Abschluss der Grundeinrichtung können Sie mit dem Testen Ihrer Umgebung und dem Ausbau Ihrer Bereitstellung beginnen.

## Grundlagen

Prisma Access-Konfiguration – **Grundlagen** zum Einstieg in Prisma Access: Führen Sie die hierin enthaltenen Aufgaben aus, um mit einer grundlegenden Einrichtung zu beginnen, mit der Sie dann Ihre Umgebung testen und Ihre Bereitstellung ausbauen können.

Jede Aufgabe führt Sie zu der Seite, auf der Sie die zugehörige Konfiguration einrichten können; wenn Sie fertig sind, werden Aufgaben auf dieser Liste als abgeschlossen angezeigt. So können Sie Ihre Fortschritte auf einen Blick verfolgen, was besonders hilfreich ist, wenn Sie sich in der Onboarding-Phase befinden.

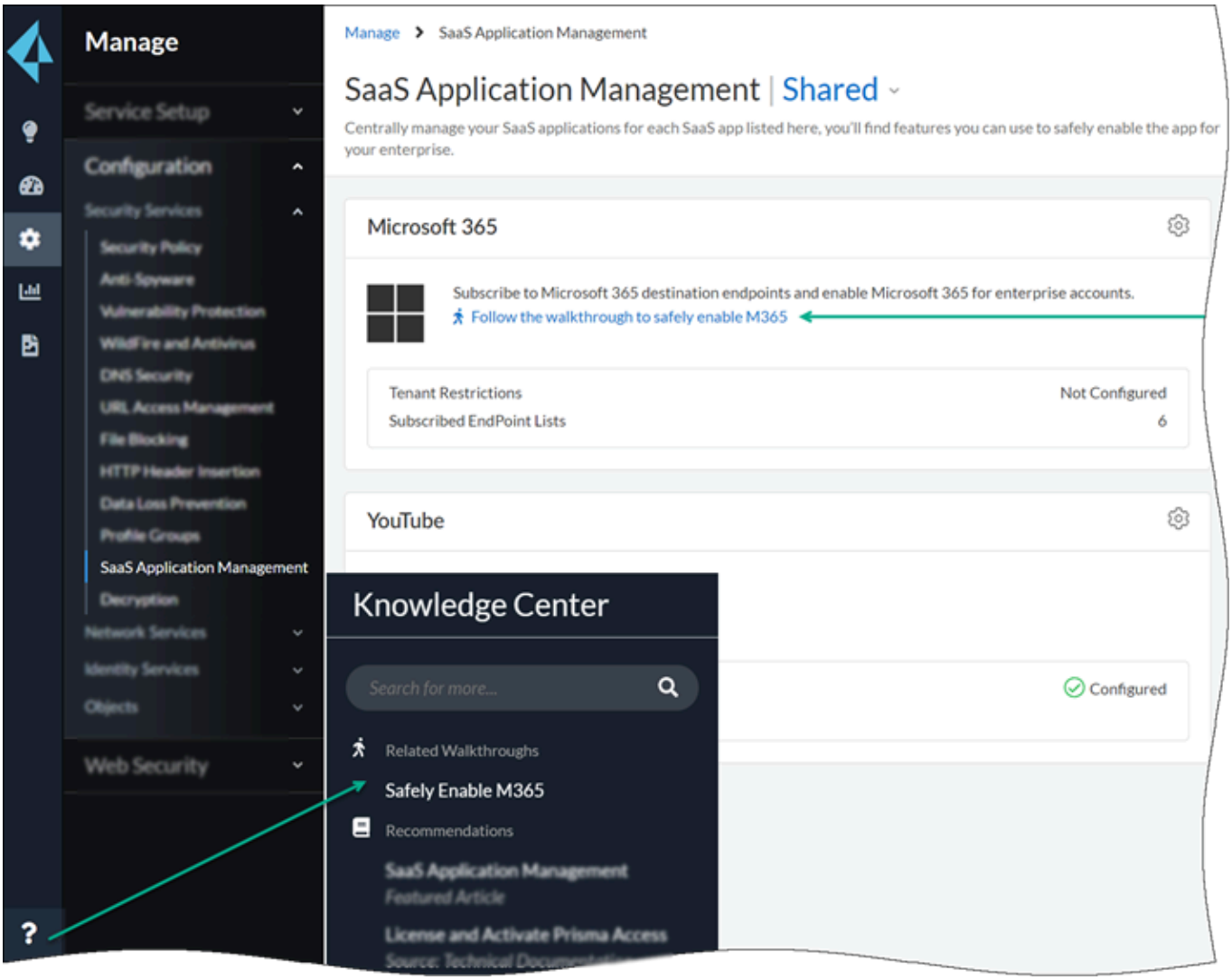



## Schritt-für-Schritt-Anleitungen

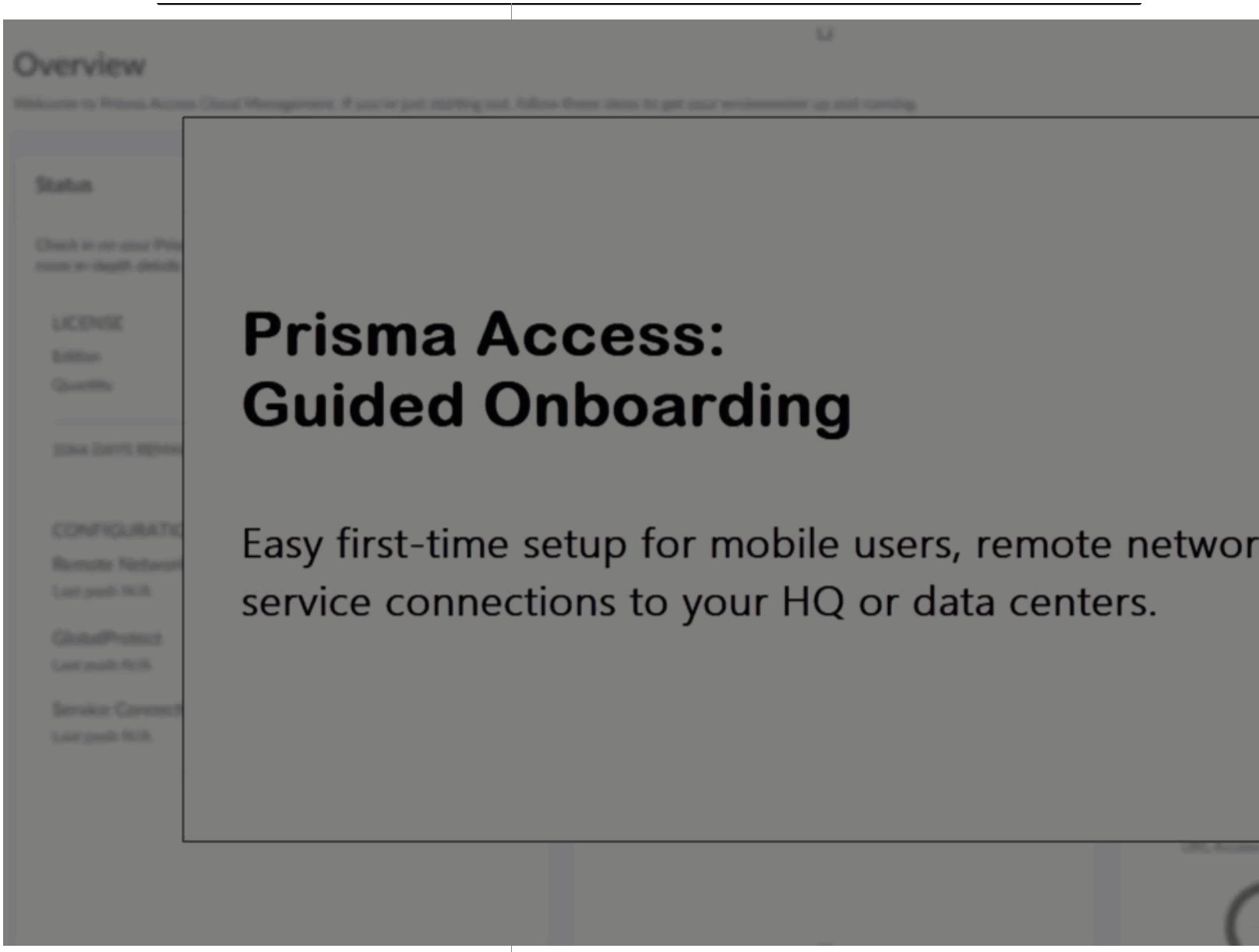
Einige Aufgaben umfassen auch Anleitungen, die Sie durch die grundlegenden, erforderlichen Schritte führen, um Ihre Umgebung betriebsbereit zu machen.

Onboarding-Anleitungen stehen Ihnen im Dashboard **Übersicht** zur Verfügung. Sie können in die Hilfe klicken, um zu sehen, ob es für die Seite, auf der Sie sich befinden, Anleitungen gibt, und nach Anleitungen Ausschau halten, die Sie direkt auf der Seite starten können:






## Prisma Access-Synchronisierungsstatus

Auf der Seite **Übersicht** können Sie den Status Ihrer Prisma Access-Konfigurationen schnell überprüfen. Wenn Sie etwas Unerwartetes sehen, untersuchen Sie die Details, um die betroffene Konfiguration zu identifizieren. Hier sind mögliche Status, die Sie sehen könnten:

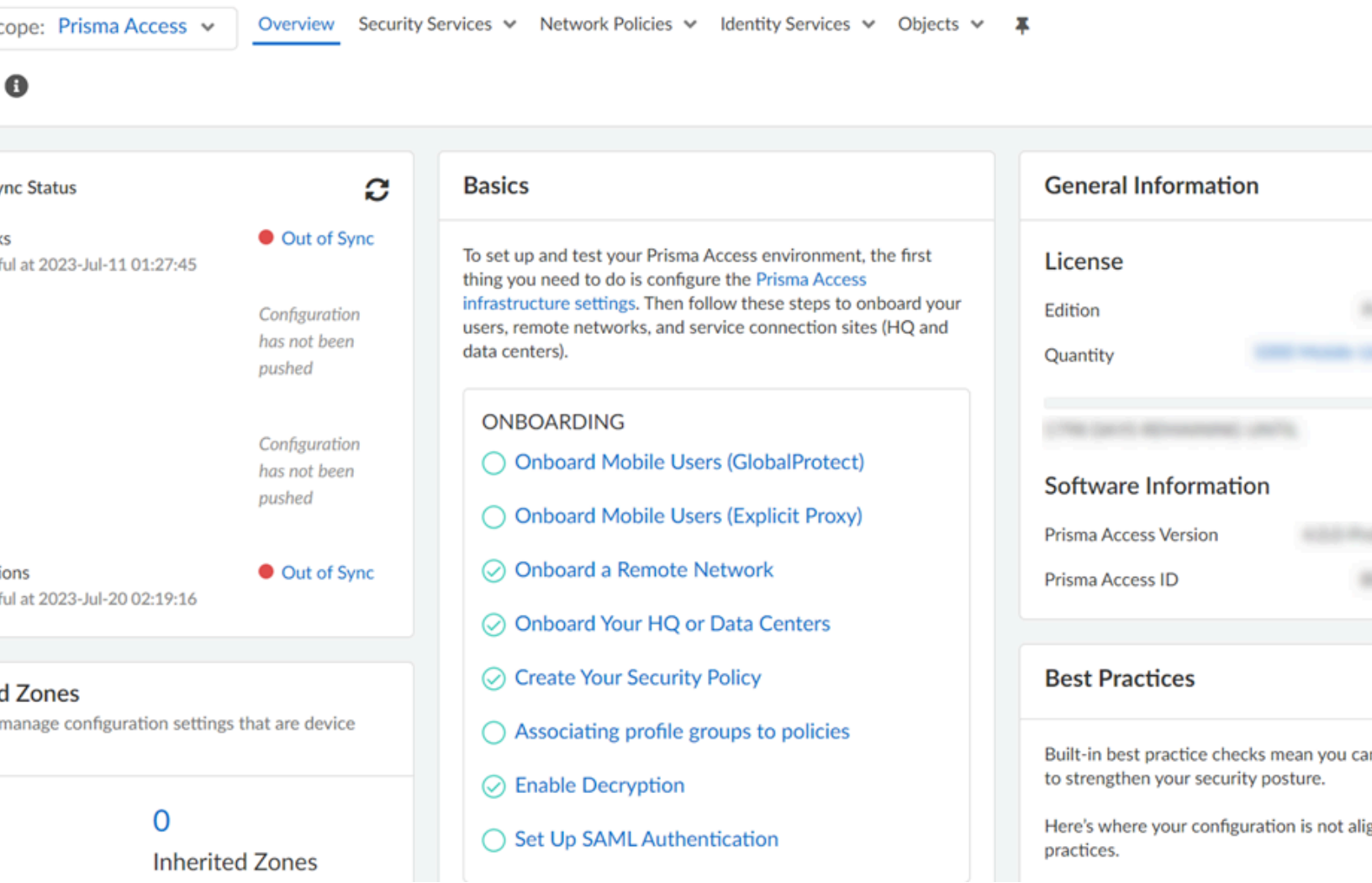
- **Konfiguration wurde nicht per Push übertragen** – Bisher wurde keine Konfiguration an Prisma Access übertragen.
- **Diese Konfiguration ist leer** – Ein Benutzer hat eine leere Konfiguration an Prisma Access übertragen. In diesem Fall war zuvor eine Konfiguration vorhanden, sodass die Übertragung an Prisma Access möglicherweise dafür gedacht war, die Konfiguration zu entfernen. Gehen Sie zu **Konfiguration übertragen** > **Jobs**, um die letzten Änderungen zu überprüfen.
- **Nicht synchron** – Ein Benutzer hat eine Konfiguration an Prisma Access übertragen, aber es gibt einen Fehler oder eine Warnung in Bezug auf die Übertragung. Hierbei kann es sich

um ein Konfigurationsproblem oder ein Problem im Zusammenhang mit der Übertragung an Prisma Access handeln.

- **Synchron** – Die letzte Konfigurationsübertragung an Prisma Access war erfolgreich und es gibt keine Fehler.

Wenn Sie etwas Unerwartetes sehen, klicken Sie auf den Status, um eine Kartenansicht zu öffnen, die die Standorte anzeigt, an denen Sie entweder mobile Benutzer (GlobalProtect oder expliziter Proxy), Remote-Netzwerke oder Dienstverbindungen haben. Sie können dann festlegen, welche Konfiguration überprüft werden muss oder wo Sie ein Update durchführen müssen.



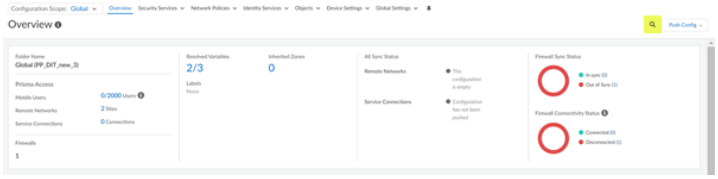

## Globale Suche über Konfigurationssuche

Mit der Konfigurationssuche können Sie spezifische Konfigurationsobjekte und Einstellungen anhand bestimmter Zeichenfolgen finden, wie IP-Adressen, Objektnamen, referenzierte Objekte, doppelte Objekte, Richtliniennamen, Richtlinienregeln, Richtlinien, die für bestimmte CVEs abgedeckt werden, Regel-UUID, vordefinierte Snippets oder Anwendungsnamen.

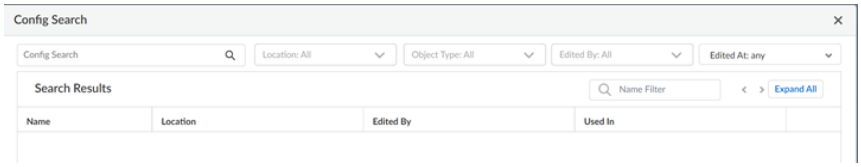
 

1. Um die **Konfigurationssuche** zu starten, klicken Sie auf das

   -Symbol neben **Konfiguration übertragen** oben rechts in der Weboberfläche. Die **Konfigurationssuche** ist auf allen Seiten unter **Verwalten** verfügbar.



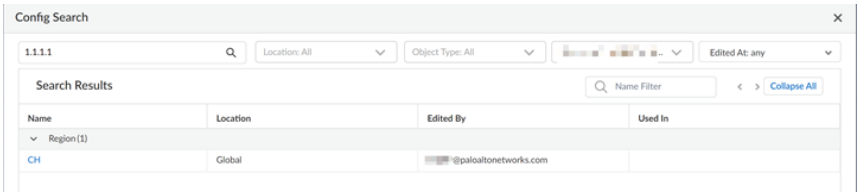

2. Auf dem Bildschirm **Konfigurationssuche** können Sie mithilfe der Felder **Konfigurations-String**, **Standort**, **Objekttyp**, **Bearbeitet von** oder **Ort der Bearbeitung** suchen.




   Suchtipps:

   - Um eine genaue Wortfolge zu finden, setzen Sie sie in Anführungszeichen.
   - Leerzeichen in Suchbegriffen werden als UND-Verknüpfungen behandelt. Wenn Sie z. B. nach [Richtlinie Vertrieb] suchen, enthalten die Suchergebnisse Instanzen, bei denen das Wort „Richtlinie“ und/oder das Wort „Vertrieb“ in der Konfiguration vorhanden ist. Wenn Sie hingegen nach ["Richtlinie Vertrieb"] (in Anführungszeichen) suchen, werden nur Konfigurationen angezeigt, die die Wortfolge „Richtlinie Vertrieb“ enthalten.
   - Um eine vorherige Suche zu wiederholen, klicken Sie auf das Symbol **Konfigurationssuche**, das die letzten 50 Suchen anzeigt. Klicken Sie auf ein beliebiges Element in der Liste, um diese Suche zu wiederholen. Jedes Administratorkonto verfügt über eine individuelle Suchverlaufsliste.
   - Die Konfigurationssuche ist für jedes durchsuchbare Feld verfügbar. Beispielsweise können Sie bei einer Sicherheitsrichtlinie nach folgenden Objekttypen suchen: Tags, Zone, Adresse, Benutzer, HIP-Profil, Anwendung, UUID und Service.
   - Der Standort ist nach Ordnern und Snippets gruppiert. Sie können mehr als einen Standort auswählen. Wenn Sie keinen Standort auswählen, werden standardmäßig **Alle** Standorte ausgewählt.
   - Wenn kein Objekttyp nicht ausgewählt ist, wird **Alle** ausgewählt.

3. Die Suchergebnisse sind kategorisiert und bieten Links zum Konfigurationsort im Strata Cloud Manager, sodass Sie alle Vorkommen und Verweise der gesuchten Zeichenfolge leicht finden können.



# Konfigurationsübersicht (Strata Cloud Manager)

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • NGFW (Managed by Strata Cloud Manager)<br>• NGFW (Managed by PAN-OS or Panorama)<br>• VM-Series, funded with Software NGFW Credits | ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) |

Wenn Sie gerade erst mit NGFW Cloud Management beginnen:

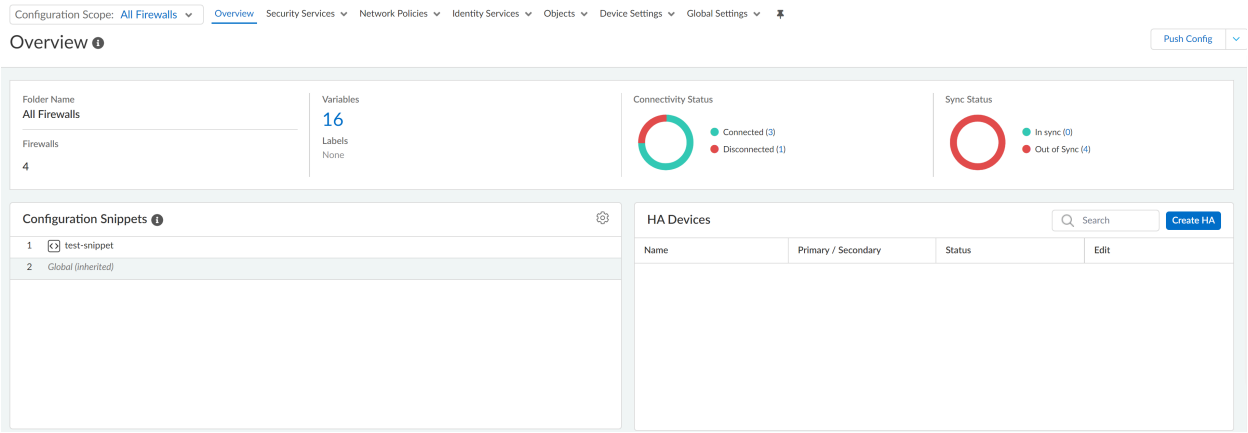
- Hier erfahren Sie, wie Richtlinien- und Konfigurationsordner funktionieren.
- Hier erfahren Sie, wie Sie Konfigurationsänderungen an Firewalls übertragen.

**Für das tägliche Konfigurationsmanagement:**

- Erhalten Sie auf einen Blick eine Übersicht über den aktuellen Ordnernamen, die Anzahl der zum Ordner hinzugefügten Firewalls und die Anzahl der für den Ordner erstellten Variablen.
- Erhalten Sie Einblick in und Kontrolle über lokale Firewallkonfigurationen, ohne dass Sie hierfür zwischen der zentralen Verwaltung und einzelnen Firewalls hin und her wechseln müssen.
  - **Firewalls mit Konfigurationskonflikten** zeigt die Anzahl der Firewalls mit Konflikten. Klicken Sie auf die Zahl, um Konflikte für Firewalls und deren Standort anzuzeigen. Klicken Sie auf eine beliebige Firewall, um Konflikte auf Geräteebene anzuzeigen.
  - **Objekte mit Konfigurationskonflikten** zeigt die Anzahl der Konflikte pro Firewall. Klicken Sie auf die Nummer, um die in Konflikt stehenden Objekte und ihre Typen für eine bestimmte Firewall anzuzeigen. Durch Klicken auf das Objekt werden detaillierte Informationen zum Konflikt angezeigt.
- Standardisieren Sie eine gemeinsame Basiskonfiguration für eine Gruppe verwalteter Firewalls mithilfe der Konfigurations-Snippets.
- Konfigurieren Sie verwaltete Firewalls in einer Konfiguration mit hoher Verfügbarkeit (High Availability, HA), um Redundanz aufzubauen und die Geschäftskontinuität sicherzustellen.
- Überprüfen Sie den **Konnektivitätsstatus** zwischen verwalteten Firewalls und Strata Cloud Manager.

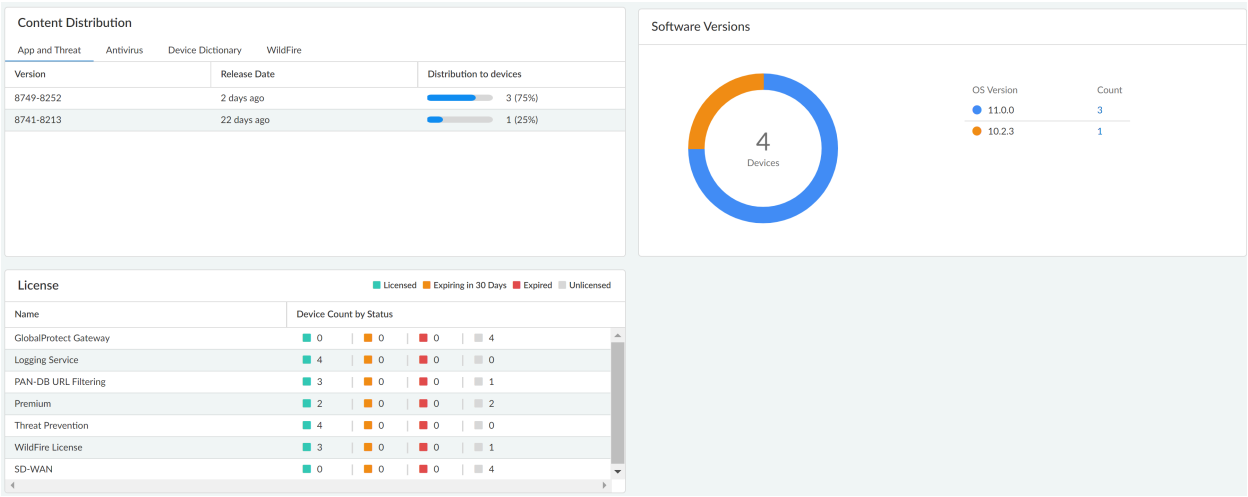
 

- Überprüfen Sie den **Synchronisierungsstatus** der Konfiguration zwischen Strata Cloud Manager und der derzeit ausgeführten Konfiguration auf Ihren verwalteten Firewalls.




**Einzelheiten zu Ihren verwalteten Firewalls:**

- Überprüfen Sie die Details zur **Verteilung von Inhalten** und zu **Softwareversionen**, um zu sehen, welche dynamischen Inhaltsaktualisierungen und PAN-OS-Softwareversionen auf Ihren verwalteten Firewalls ausgeführt werden.
- Überprüfen Sie die **Lizenz**-Details, um zu sehen, welche Lizenzen auf Ihren verwalteten Firewalls aktiviert sind.



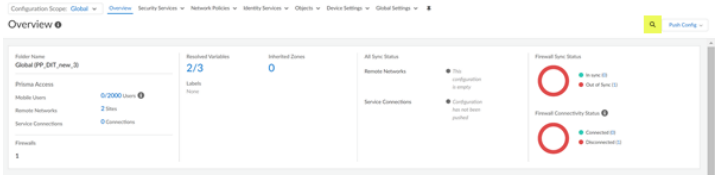

## Globale Suche über Konfigurationssuche

Mit der Konfigurationssuche können Sie spezifische Konfigurationsobjekte und Einstellungen anhand bestimmter Zeichenfolgen finden, wie IP-Adressen, Objektnamen, referenzierte Objekte, doppelte Objekte, Richtliniennamen, Richtlinienregeln, Richtlinien, die für bestimmte CVEs abgedeckt werden, Regel-UUID, vordefinierte Snippets oder Anwendungsnamen.

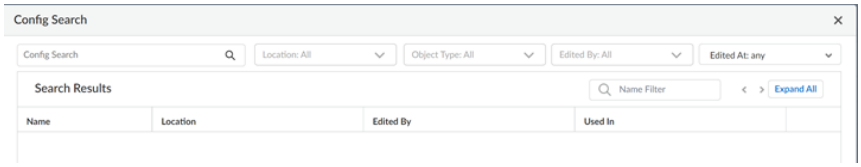
 

1. Um die **Konfigurationssuche** zu starten, klicken Sie auf das

   -Symbol neben **Konfiguration übertragen** oben rechts in der Weboberfläche. Die **Konfigurationssuche** ist auf allen Seiten unter **Verwalten** verfügbar.



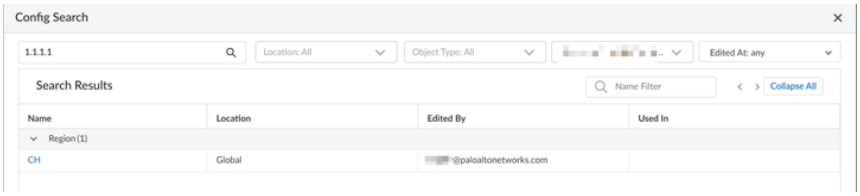

2. Auf dem Bildschirm **Konfigurationssuche** können Sie mithilfe der Felder **Konfigurations-String**, **Standort**, **Objekttyp**, **Bearbeitet von** oder **Ort der Bearbeitung** suchen.




   Suchtipps:

   - Um eine genaue Wortfolge zu finden, setzen Sie sie in Anführungszeichen.
   - Leerzeichen in Suchbegriffen werden als UND-Verknüpfungen behandelt. Wenn Sie z. B. nach [Richtlinie Vertrieb] suchen, enthalten die Suchergebnisse Instanzen, bei denen das Wort „Richtlinie“ und/oder das Wort „Vertrieb“ in der Konfiguration vorhanden ist. Wenn Sie hingegen nach ["Richtlinie Vertrieb"] (in Anführungszeichen) suchen, werden nur Konfigurationen angezeigt, die die Wortfolge „Richtlinie Vertrieb“ enthalten.
   - Um eine vorherige Suche zu wiederholen, klicken Sie auf das Symbol „Konfigurationssuche“, das die letzten 50 Suchen anzeigt. Klicken Sie auf ein beliebiges Element in der Liste, um diese Suche zu wiederholen. Jedes Administratorkonto verfügt über eine individuelle Suchverlaufsliste.
   - Die Konfigurationssuche ist für jedes durchsuchbare Feld verfügbar. Beispielsweise können Sie bei einer Sicherheitsrichtlinie nach folgenden Objekttypen suchen: Tags, Zone, Adresse, Benutzer, HIP-Profil, Anwendung, UUID und Service.
   - Der Standort ist nach Ordnern und Snippets gruppiert. Sie können mehr als einen Standort auswählen. Wenn Sie keinen Standort auswählen, werden standardmäßig **alle** Standorte ausgewählt.
   - Wenn kein Objekttyp ausgewählt ist, wird **Alle** ausgewählt.

3. Die Suchergebnisse sind kategorisiert und bieten Links zum Konfigurationsort im Strata Cloud Manager, sodass Sie alle Vorkommen und Verweise der gesuchten Zeichenfolge leicht finden können.



# Verwalten: Sicherheitsdienste

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>☐ Prisma Access<br>☐ AIOps for NGFW Premium<br>☐ Strata Cloud Manager Essentials<br>☐ Strata Cloud Manager Pro<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Verwalten Sie Ihre Sicherheitsdienste und schützen Sie Ihr Netzwerk, Ihre Systeme und Ihre Benutzer.

Gehen Sie zu **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Sicherheitsdienste**.

Mit Sicherheitsdiensten können Sie Folgendes erreichen:

- Definieren Sie, wie Sie Regeln im Prisma Access-Verkehr mit Verwalten: Sicherheitsrichtlinie durchsetzen möchten.
- Stoppen Sie im verschlüsselten Datenverkehr versteckte Bedrohungen mit Verwalten: Entschlüsselung.

## Verwalten: Sicherheitsrichtlinie

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>☐ Prisma Access<br>☐ AIOps for NGFW Premium<br>☐ Strata Cloud Manager Essentials<br>☐ Strata Cloud Manager Pro<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

In Ihrer Sicherheitsrichtlinie legen Sie fest, wie Sie den Datenverkehr in Ihren Prisma Access- und NGFW-Bereitstellungen kontrollieren wollen. Der gesamte Datenverkehr, der Ihre Strata Cloud Manager-Umgebung durchläuft, wird anhand Ihrer Sicherheitsrichtlinie bewertet und die Regeln werden von oben nach unten angewendet.

Um Ihre Sicherheitsrichtlinie einzurichten, gehen Sie zu **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Sicherheitsdienste** > **Sicherheitsrichtlinie**.

#### Erste Schritte mit Sicherheitsrichtlinien

Hier sind einige Dinge, die Sie jetzt tun können, damit Ihre Sicherheitsrichtlinie optimal funktioniert.

- Erstellen Sie eine Sicherheitsrichtlinienregel – Mit Sicherheitsrichtlinien können Sie Regeln durchsetzen und Maßnahmen ergreifen; sie können so allgemein oder spezifisch sein wie nötig.
- Verfolgen Sie Regeln innerhalb eines Regelsatzes – Jede Regel innerhalb eines Regelsatzes wird automatisch nummeriert; wenn Sie Regeln verschieben oder neu anordnen, ändern sich die Zahlen basierend auf der neuen Reihenfolge.
- Setzen Sie Best Practices für Richtlinienregeln durch – Beim Erstellen oder Ändern von Regeln können Sie eine Regelbeschreibung, ein Tag, einen Auditkommentar usw. verlangen, um sicherzustellen, dass Ihr Richtlinienregelsatz korrekt organisiert und gruppiert ist und um wichtige Regelverläufe für Auditzwecke zu erhalten.
- Testen Sie Richtlinienregeln – Verwenden Sie die Richtlinienregeln für die Richtlinienanalyse.
- Aktivieren Sie ein Sicherheitsprofil – Ein Sicherheitsprofil wird angewendet, um den Datenverkehr zu scannen, nachdem die Anwendung oder Kategorie von der Sicherheitsrichtlinie zugelassen wurde.
- Erstellen Sie eine Sicherheitsprofilgruppe – Eine Sicherheitsprofilgruppe ist ein Satz von Sicherheitsprofilen, die als Einheit behandelt und dann einfach zu Sicherheitsrichtlinien hinzugefügt werden können.
- Richten Sie eine Dateiblockierung ein – Identifizieren Sie bestimmte Dateitypen, die Sie blockieren oder überwachen möchten.
- Erstellen Sie ein Datenfilterprofil – Verhindern Sie, dass sensible Informationen Ihr Netzwerk verlassen.
- Verwalten Sie die Websicherheit – Steuern Sie den Zugriff auf das Internet (allgemeines Browsing) und SaaS-Anwendungen.

## Verwalten: Entschlüsselung

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>❑ Prisma Access<br>❑ AIOps for NGFW Premium<br>❑ Strata Cloud Manager Essentials<br>❑ Strata Cloud Manager Pro |

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| | → Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Aktivieren Sie die Entschlüsselung, um Bedrohungen abzuwehren, die im verschlüsselten Verkehr versteckt sind. Zum Einstieg müssen Sie lediglich Ihre Entschlüsselungszertifikate importieren — für alles andere haben wir Best-Practice-Einstellungen eingebaut, die Sie direkt verwenden können.

Hier erfahren Sie mehr über das Entschlüsseln von Datenverkehr.

Gehen Sie zu **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Sicherheitsdienste** > **Entschlüsselung**.

#### Übersicht über die Entschlüsselung

Die Verschlüsselungsprotokolle Secure Sockets Layer (SSL) und Secure Shell (SSH) sichern den Verkehr zwischen zwei Entitäten, z. B. einem Webserver und einem Client. SSL und SSH kapseln den Datenverkehr und verschlüsseln Daten, sodass sie für andere Entitäten als den Client und den Server mit den Zertifikaten, die das Vertrauen zwischen den Geräten bestätigen, und den Schlüsseln zum Dekodieren der Daten bedeutungslos sind. Entschlüsseln Sie SSL- und SSH-Verkehr, um Folgendes zu erreichen:

- Verhindern Sie, dass Malware, die in verschlüsseltem Datenverkehr verborgen ist, in Ihr Netzwerk gelangt. Beispielsweise kann ein Angreifer eine Website infizieren, die SSL-Verschlüsselung verwendet. Mitarbeiter besuchen diese Website und laden unwissentlich einen Exploit oder eine Malware herunter. Die Malware nutzt dann den infizierten Mitarbeiterendpunkt, um sich lateral durch das Netzwerk zu bewegen und andere Systeme zu gefährden.
- Verhindern Sie, dass vertrauliche Informationen das Netzwerk verlassen.
- Stellen Sie sicher, dass die entsprechenden Anwendungen in einem sicheren Netzwerk ausgeführt werden.
- Entschlüsseln Sie den Datenverkehr selektiv. Erstellen Sie beispielsweise eine Entschlüsselungsrichtlinie und ein Entschlüsselungsprofil, um Finanz- oder Gesundheitsdaten von der Entschlüsselung auszuschließen.

*Die SSH-Proxy-Entschlüsselung wird in Strata Cloud Manager nicht unterstützt.*

#### Entschlüsselungsrichtlinien

Strata Cloud Manager bietet zwei Arten von Regeln für Entschlüsselungsrichtlinien: SSL-Forward-Proxy zur Kontrolle des ausgehenden SSL-Verkehrs und SSL-Eingangsinspektion zur Kontrolle des eingehenden SSL-Verkehrs.

**SSL-Forward-Proxy**

Wenn Sie die Firewall so konfigurieren, dass SSL-Verkehr zu externen Websites entschlüsselt wird, fungiert sie als SSL-Forward-Proxy. Verwenden Sie eine SSL-Forward-Proxy-

Entschlüsselungsrichtlinie, um den SSL-/TLS-Verkehr von internen Benutzern zum Internet zu entschlüsseln und zu überprüfen. Die SSL-Forward-Proxy-Entschlüsselung verhindert, dass Malware, die sich in SSL-verschlüsseltem Datenverkehr verbirgt, in Ihr Unternehmensnetzwerk gelangt. Hierzu wird der Datenverkehr entschlüsselt, damit die Firewall Entschlüsselungsprofile sowie Sicherheitsrichtlinien und -profile auf den Datenverkehr anwenden kann.

**SSL-Eingangsinspektion**

Verwenden Sie die SSL-Eingangsinspektion, um eingehenden SSL-/TLS-Verkehr von einem Client zu einem Zielnetzwerkserver (jeder Server, für den Sie das Zertifikat haben und den Sie in die Firewall importieren können) zu entschlüsseln und zu überprüfen und verdächtige Sitzungen zu blockieren. Nehmen wir zum Beispiel an, ein Cyberkrimineller möchte eine bekannte Sicherheitslücke auf Ihrem Webserver ausnutzen. Die eingehende SSL-/TLS-Entschlüsselung bietet Einblick in den Datenverkehr und ermöglicht es der Firewall, proaktiv auf die Bedrohung zu reagieren.

#### Entschlüsselungsprofile

Sie können ein Entschlüsselungsprofil an eine Richtlinienregel anhängen, um präzise Zugriffseinstellungen auf den Datenverkehr anzuwenden, z. B. Prüfungen auf Serverzertifikate, nicht unterstützte Modi und Fehler.

**SSL-Forward-Proxy-Profile**

Das SSL-Forward-Proxy-Entschlüsselungsprofil steuert die Serverüberprüfung, Sitzungsmodusüberprüfung und Fehlerprüfung für ausgehenden SSL-/TLS-Verkehr, der in den Forward-Proxy-Entschlüsselungsrichtlinien definiert ist, an die Sie das Profil anhängen.

**SSL-Eingangsinspektionsprofile**

Das SSL-Eingangsinspektionsprofil steuert die Sitzungsmodusüberprüfungen und Fehlerprüfungen für eingehenden SSL-/TLS-Verkehr, die in den Eingangsinspektions-Entschlüsselungsrichtlinien definiert sind, an die Sie das Profil anhängen.

**Profil für keine Entschlüsselung**

„Keine Entschlüsselung“-Profile führen Serverüberprüfungen für Datenverkehr durch, den Sie nicht entschlüsseln möchten. Sie fügen ein „Keine Entschlüsselung“-Profil an eine „Keine Entschlüsselung“-Entschlüsselungsrichtlinie an, die den Verkehr definiert, der von der Entschlüsselung ausgeschlossen werden soll. (Verwenden Sie keine Richtlinie, um Datenverkehr auszuschließen, den Sie nicht entschlüsseln können, weil eine Website die Entschlüsselung aus technischen Gründen unterbricht, beispielsweise aufgrund eines angehefteten Zertifikats oder einer gegenseitigen Authentifizierung. Fügen Sie stattdessen den Hostnamen zur Entschlüsselungsausschlussliste hinzu.)

#### Tipps zur Entschlüsselung

- **Verwenden Sie die Best-Practice-Richtlinienregeln als Ausgangspunkt für die Erstellung Ihrer Entschlüsselungsrichtlinie.**

  Diese Regeln – eine, die den Datenverkehr entschlüsselt, und eine, die vertrauliche Inhalte von der Entschlüsselung ausschließt – basieren auf URL-Kategorien.

- **Schließen Sie vertraulichen Inhalt von der Entschlüsselung aus.**

  Schließen Sie vertraulichen Inhalt aus geschäftlichen, rechtlichen oder regulatorischen Gründen von der Entschlüsselung aus.

  - Vordefinierte Entschlüsselungsausschlüsse – Palo Alto Networks verwaltet diese Ausnahmeliste und aktualisiert sie regelmäßig. Diese Liste gilt global und standardmäßig für den gesamten Datenverkehr, den Sie für die Entschlüsselung angeben. Sie können Listeneinträge deaktivieren, um die Liste Ihren Geschäftsanforderungen anzupassen.
  - Benutzerdefinierte Ausschlüsse – schließen Websites oder Anwendungen global von der Entschlüsselung aus.
  - Richtlinienbasierte Ausnahmen – Verwenden Sie URL-Kategorien und externe dynamische Listen, um gezielte, richtlinienbasierte Entschlüsselungsregeln zu erstellen. Legen Sie eine Regelaktion für eine Entschlüsselungsrichtlinie auf **keine Entschlüsselung** fest, um übereinstimmenden Datenverkehr von der Entschlüsselung auszuschließen.

  Platzieren Sie Entschlüsselungsausschlüsse immer ganz oben in Ihren Richtlinienregeln, sodass sie zuerst angewendet werden.

- **Bedenken Sie, dass Sie einige Entschlüsselungseinstellungen global anwenden und andere auf bestimmte Standorte ausrichten können.**

  - Ihre Strata Cloud Manager-Entschlüsselungsrichtlinie wird weltweit auf alle NGFWs und Prisma Access-Standorte angewendet.

    **Verwalten** > **Configuration (Konfiguration)** > **NGFW und Prisma Access** > **Sicherheitsdienste** > **Entschlüsselung**
  - Navigieren Sie zur Entschlüsselungsrichtlinie für jeden Typ, um Richtlinienregeln zu erstellen, die auf bestimmte Firewalls, Standorte mobiler Benutzer, Remote-Netzwerkstandorte oder Dienstverbindungen abzielen.

    **Verwalten** > **Configuration (Konfiguration)** > **NGFW und Prisma Access** > **Konfigurationsumfang** > **Global / Firewalls / Mobile-Benutzer / Remote-Netzwerke / Dienstverbindungen**

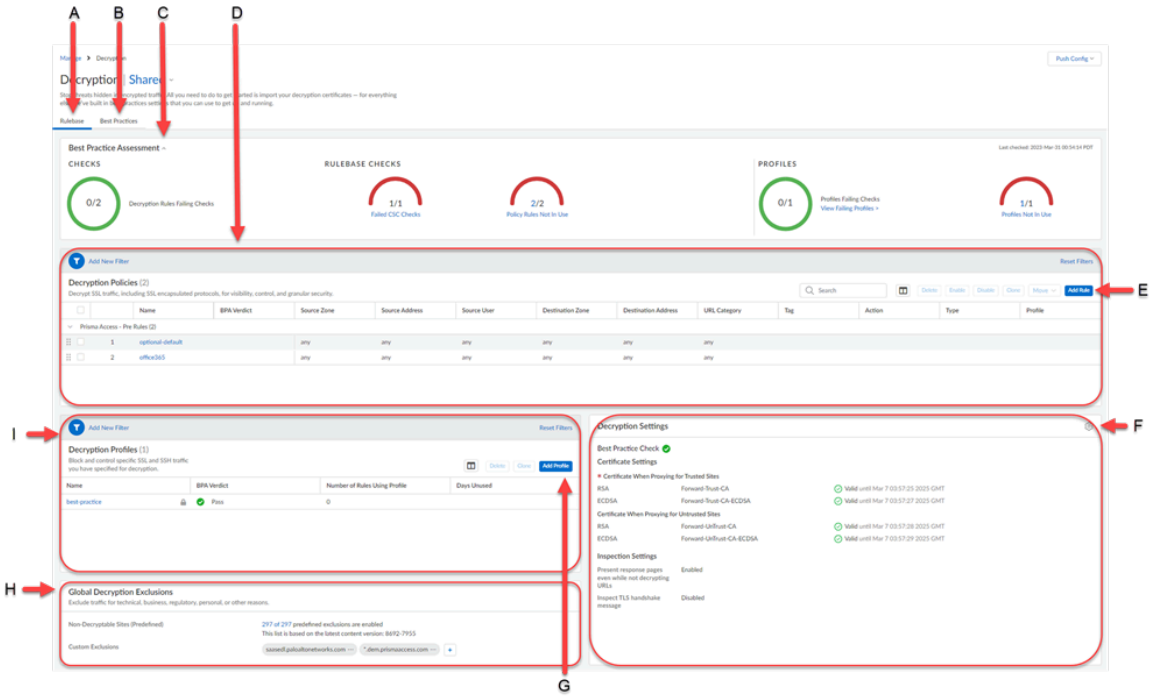
- **Die Reihenfolge der Regeln ist wichtig.**

  Die Regeln der Entschlüsselungsrichtlinie werden von oben nach unten angewendet. Platzieren Sie die Regeln, die durchgesetzt werden sollen, an erster Stelle Ihrer Liste der Entschlüsselungsrichtlinienregeln. Globale Regeln (Vor-Regeln) werden zuerst angewendet und immer vor Regeln aufgeführt, die für mobile Benutzer, Remote-Netzwerke und Dienstverbindungen spezifisch sind.

#### Entschlüsselung auf einen Blick

Auf dem Bildschirm „Entschlüsselung“ können Sie Entschlüsselungsrichtlinien und -profile konfigurieren und Ihre Best-Practice-Bewertungen einsehen.




**A) Regelsatz** – Regelwerküberprüfungen untersuchen, wie die Sicherheitsrichtlinie organisiert und verwaltet wird, einschließlich der Konfigurationseinstellungen, die für mehrere Regeln gelten.

**B) Best Practices** – Hier erhalten Sie einen umfassenden Überblick darüber, inwieweit die Implementierung einer Funktion den Best Practices entspricht. Untersuchen Sie fehlgeschlagene Überprüfungen, um festzustellen, wo Sie Verbesserungen vornehmen können (Sie können auch bestandene Überprüfungen prüfen).

**C) Best-Practice-Bewertung** – Best-Practice-Scores werden im Entschlüsselungs-Dashboard angezeigt. Diese Scores bieten Ihnen einen schnellen Einblick in Ihre Best-Practice-Fortschritte. Sie können auf einen Blick Bereiche erkennen, die einer weiteren Untersuchung bedürfen oder in denen Sie Maßnahmen zur Verbesserung Ihres Sicherheitsstatus ergreifen sollten.

**D) Entschlüsselungsrichtlinien** – Liste der integrierten Entschlüsselungsrichtlinien. Überprüfen Sie die Richtlinienkonfiguration, den Richtlinientyp (*SSL-Forward-Proxy*, *SSL-Eingangsinspektion* oder *SSH-Proxy*), die Richtlinienaktion (*Entschlüsseln* oder *Nicht entschlüsseln*) und das BPA-Urteil.

**E) Regel hinzufügen** – Fügen Sie neue Entschlüsselungsrichtlinien hinzu und konfigurieren Sie sie.

**F) Entschlüsselungseinstellungen** – Greifen Sie auf Zertifikats- und Entschlüsselungseinstellungen zu. Importieren und exportieren Sie Zertifikate.

**G) Profil hinzufügen** – Fügen Sie neue Entschlüsselungsprofile hinzu und konfigurieren Sie sie.

**H) Globale Entschlüsselungsausschlüsse** – Anwendungen, die von der Entschlüsselung ausgeschlossen sind.

**I) Entschlüsselungsprofile** – Liste der integrierten Entschlüsselungsprofile. Überprüfen Sie die Profilkonfiguration, die Richtlinien, die das Profil verwenden, und das BPA-Urteil.

# Verwalten: Netzwerkrichtlinien

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>❑ Prisma Access<br>❑ AIOps for NGFW Premium<br>❑ Strata Cloud Manager Essentials<br>❑ Strata Cloud Manager Pro<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Sie können verschiedene Arten von Netzwerkrichtlinien erstellen, um Ihr Netzwerk vor Bedrohungen und Störungen zu schützen. Das hilft bei der Optimierung der Netzwerkressourcenzuweisung und der Verwaltung Ihrer Netzwerkrichtlinien, um den Datenverkehr zu priorisieren und Anwendungsklassifizierungen zu konfigurieren.

Regeln werden von oben nach unten ausgewertet und wenn der Datenverkehr den definierten Regelkriterien entspricht, werden nachfolgende Regeln nicht ausgewertet. Um die bestmöglichen Übereinstimmungskriterien durchzusetzen, sollten Sie spezifischere Richtlinienregeln oberhalb von allgemeineren platzieren. Für den Datenverkehr, der einer Richtlinienregel entspricht, wird ein Protokoll generiert, wenn die Protokollierung für die Regel aktiviert ist. Protokollierungsoptionen sind für jede Regel konfigurierbar.

Für die meisten Richtlinientypen stehen Best-Practice-Richtlinienregeln zur Verfügung, die Ihnen einen schnellen und sicheren Einstieg ermöglichen. Diese Regeln können zwar nicht bearbeitet werden, um sicherzustellen, dass Ihnen immer ein Mindestmaß an Sicherheit zur Verfügung steht, Sie können sie jedoch klonen, wenn Sie sie als Grundlage für eigene Richtlinien verwenden möchten.

Gehen Sie zu **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Netzwerkrichtlinien**, um zu beginnen.

Mit Netzwerkrichtlinien können Sie Folgendes erreichen:

- Priorisieren Sie den Verkehr, der für Ihren Betrieb mit Verwalten: QoS am wichtigsten ist.
- Verwalten Sie, wie Prisma Access Ihre Anwendungen mit Verwalten: Anwendungsüberschreibung klassifiziert.

# Verwalten: QoS

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager) | Eine der folgenden Komponenten:<br>☐ Prisma Access-Lizenz<br>☐ Strata Cloud Manager Pro<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Mit Quality of Service (QoS) können Sie geschäftskritischen Datenverkehr und wichtige Anwendungen priorisieren, die eine geringe Latenz erfordern (wie VoIP- und Videoanwendungen). Um eine QoS-Richtlinienregel hinzuzufügen oder zu bearbeiten, gehen Sie zu **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Netzwerkrichtlinien** > **QoS**.

#### QoS-Richtlinienregeln

QoS-Richtlinienregeln (Quality of Service) zur Identifizierung von Datenverkehr, der eine bevorzugte Behandlung oder Bandbreitenbegrenzung erfordert. Mithilfe von QoS-Regeln können Sie Anwendungen und Datenverkehr mit hoher Priorität zuverlässig bei begrenzter Netzwerkkapazität ausführen. Sie können die Datenverkehrs-QoS-Behandlung mit Differentiated Services Code Points (DSCP) konfigurieren. Bei diesen Codepunkten handelt es sich um Paket-Headerwerte, die verwendet werden können, um (zum Beispiel) eine Bereitstellung mit hoher Priorität oder eine bestmögliche Bereitstellung anzufordern. Prisma Access erzwingt nicht nur DSCP-Werte für eingehenden Datenverkehr, sondern markiert Sitzungen auch mit einem DSCP-Wert, wenn Sitzungsverkehr die Firewall verlässt. Das bedeutet, dass der gesamte eingehende und ausgehende Datenverkehr für eine Sitzung eine kontinuierliche QoS-Behandlung erhält. Sie können die Datenverkehrs-QoS-Behandlung mithilfe der folgenden Codepunkte konfigurieren:

- **Expedited Forwarding (EF)** – wird verwendet, um geringe Paketverluste, geringe Latenz und garantierte Bandbreite für den Datenverkehr anzufordern.

  Pakete mit EF-Codepunkt-Werten werden typischerweise mit höchster Priorität ausgeliefert.
- **Assured Forwarding (AF)** – wird verwendet, um eine zuverlässige Bereitstellung für Anwendungen zu gewährleisten.

  -

  Pakete mit AF-Codepunkten weisen darauf hin, dass Datenverkehr eine Behandlung mit höherer Priorität erhalten muss als der bestmögliche Dienst. Pakete mit EF-Codepunkt haben Vorrang vor Paketen mit AF-Codepunkt.
- **Class Selector (CS)** – wird verwendet, um Abwärtskompatibilität mit Netzwerk-IP-Adressen bereitzustellen, die das Feld „IP-Präzedenz“ verwenden, um vorrangigen Datenverkehr zu markieren.
- **IP-Präzedenz (ToS)** – wird von älteren Netzwerk-IP-Adressen verwendet, um vorrangigen Datenverkehr zu markieren.

- **Benutzerdefinierter Codepunkt** – Erstellen Sie einen benutzerdefinierten Codepunkt, der dem Datenverkehr entspricht, indem Sie einen Codepunktnamen und Binärwert eingeben.

  Beispielsweise können Sie eine QoS-Richtlinienregel erstellen, um Sprachkommunikation wie Voice over IP (VoIP) zu priorisieren und so eine einheitliche Paketübertragung sicherzustellen. So wird eine einheitliche Sprachkommunikation gewährleistet.

# Verwalten: Anwendungsüberschreibung

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>❑ Prisma Access<br>❑ AIOps for NGFW Premium<br>❑ Strata Cloud Manager Essentials<br>❑ Strata Cloud Manager Pro<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Erstellen Sie eine Richtlinie zur Anwendungsüberschreibung, um festzulegen, dass Anwendungen mit der Fast-Path-Layer-4-Inspektion verarbeitet werden, anstatt die Anwendungs-ID für die Layer-7-Inspektion zu verwenden. Dadurch wird der Sicherheitsdurchsetzungsknoten gezwungen, die Sitzung als reguläre Statusprüfung zu behandeln, was die Anwendungsverarbeitungszeiten reduziert. Sie können eine Richtlinienregel zur Anwendungsüberschreibung erstellen, wenn Sie keine Datenverkehrsprüfung für benutzerdefinierte Anwendungen zwischen bekannten IP-Adressen wünschen. Nehmen wir an, Sie haben eine benutzerdefinierte Anwendung an einem nicht standardmäßigen Port, von dem Sie wissen, dass die Benutzer, die auf die Anwendung zugreifen, sanktioniert sind. Darüber hinaus befinden sich beide in der Vertrauenszone. In solchen Fällen können Sie die Anwendungsprüfungsanforderungen für die vertrauenswürdigen Benutzer, die auf die benutzerdefinierte Anwendung zugreifen, überschreiben.

Um die Klassifizierung von Anwendungen durch Prisma Access zu ändern, gehen Sie zu **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Netzwerkrichtlinien** > **Anwendungsüberschreibung** und erstellen Sie dann Ihre Richtlinienregel zur Anwendungsüberschreibung.

#### Tipps zur Anwendungsüberschreibung

Bedenken Sie, dass Sie durch das Erstellen einer Anwendungsüberschreibungsrichtlinienregel die Anwendungs-ID daran hindern, den Datenverkehr Ihrer Bereitstellung zu klassifizieren und basierend auf dieser Anwendungsidentifikation eine Bedrohungsüberprüfung durchzuführen. Zur Unterstützung interner, eigens entwickelter Anwendungen lohnt es sich, die Erstellung einer benutzerdefinierten Anwendung in Betracht zu ziehen (anstelle einer Anwendungsüberschreibungsregel), die die Anwendungssignatur enthält, sodass Strata Cloud Manager eine Layer-7-Inspektion durchführt und den Anwendungsverkehr auf Bedrohungen

scannt. Um eine benutzerdefinierte Anwendung zu erstellen, gehen Sie zu **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Objekte** > **Anwendungen**.

#### Anwendungsüberschreibungsrichtlinien

Verwenden Sie die folgenden Abschnitte, um eine Anwendungsüberschreibungsregel zu konfigurieren:

- **Quelle**
  - **Zonen** – **Hinzufügen** von Quellzonen
  - **Adressen** – **Hinzufügen** von Quelladressen, Adressgruppen oder Regionen und Festlegen der Einstellungen.
- **Ziel**
  - **Zonen** – **Hinzufügen** von Zielzonen.
  - **Adressen** – **Hinzufügen** von Quelladressen, Adressgruppen oder Regionen und Festlegen der Einstellungen.
- **Anwendung**
  - **Anwendung** – Auswahl der Überschreibungsanwendung für Datenverkehrsflüsse, die den oben genannten Regelkriterien entsprechen. Beim Überschreiben einer benutzerdefinierten Anwendung wird keine Bedrohungsprüfung durchgeführt. Die Ausnahme bilden Fälle, in denen Sie zu einer vordefinierten Anwendung wechseln, die die Bedrohungsprüfung unterstützt.

    Um neue Anwendungen zu definieren, gehen Sie zu **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Objekte** > **Anwendungen**.
- **Protokoll**
  - **Protokoll** – Auswahl des Protokolls (**TCP** oder **UDP**), für das eine Anwendungsüberschreibung zugelassen werden soll.
  - **Port** – Eingabe der Portnummer (0 bis 65535) oder des Portnummernbereichs (Port1–Port2) für die angegebenen Zieladressen. Mehrere Ports oder Bereiche müssen durch Kommas getrennt werden.

# Verwalten: Richtlinienbasierte Weiterleitung

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>❑ Prisma Access<br>❑ AIOps for NGFW Premium<br>❑ Strata Cloud Manager Essentials<br>❑ Strata Cloud Manager Pro<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung |

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| | stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Richtlinienbasierte Weiterleitungsregeln ermöglichen es dem Datenverkehr, einen alternativen Pfad vom nächsten in der Routentabelle angegebenen Hop zu nehmen. Sie werden normalerweise verwendet, um aus Sicherheits- oder Leistungsgründen eine Ausgangsschnittstelle anzugeben.

Gehen Sie zu **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Netzwerkrichtlinien** > **Richtlinienbasierte Weiterleitung**, um zu beginnen.

Verwenden Sie eine richtlinienbasierte Weiterleitungsregel, um den Datenverkehr an eine bestimmte Ausgangsschnittstelle zu leiten und den Standardpfad für den Datenverkehr zu überschreiben. Bevor Sie eine richtlinienbasierte Weiterleitungsregel erstellen, beachten Sie, dass der Satz von IPv4-Adressen als Teilmenge des Satzes von IPv6-Adressen behandelt wird.

Verwenden Sie die folgenden Abschnitte, um eine richtlinienbasierte Weiterleitungsregel zu konfigurieren:

- **Quelle**
  - **Zonen** – **Hinzufügen** von Quellzonen
  - **Schnittstelle** – **Hinzufügen** von Quellschnittstellen.
  - **Adressen** – **Hinzufügen** von Quelladressen, Adressgruppen oder Regionen und Festlegen der Einstellungen.
  - **Benutzer** – **Hinzufügen** der Benutzer und Benutzergruppen, für die die Richtlinie gilt.
- **Ziel**
  - **Adressen** – **Hinzufügen** von Quelladressen, Adressgruppen oder Regionen und Festlegen der Einstellungen.
- **Anwendung und Dienste**
  - **Anwendungsentitäten** – Wählen Sie die Anwendungen aus, die Sie über alternative Pfade weiterleiten möchten.

    Eine richtlinienbasierte Weiterleitungsregel kann angewendet werden, bevor die Firewall über genügend Informationen verfügt, um die Anwendung zu bestimmen. Daher werden anwendungsspezifische Regeln für die Verwendung mit richtlinienbasierter Weiterleitung nicht empfohlen. Wann immer möglich, verwenden Sie ein Serviceobjekt.

    *Sie können keine benutzerdefinierten Anwendungen, Anwendungsfilter oder Anwendungsgruppen in richtlinienbasierten Weiterleitungsregeln verwenden.*
  - **Dienstentitäten** – Wählen Sie die Dienste und Dienstgruppen aus, die Sie über alternative Pfade weiterleiten möchten.

- **Weiterleitung**
  - **Aktion** – Sie können die Aktion festlegen, die beim Abgleich eines Pakets ausgeführt werden soll, indem Sie aus Folgendem wählen:
    - **Weiterleiten** – leitet das Paket an die angegebene **Ausgangsschnittstelle** weiter.
    - **Verwerfen** – verwirft das Paket.
    - **Keine PBF** – schließt Pakete aus, die den in der Regel definierten Kriterien für Quelle, Ziel, Anwendung oder Dienst entsprechen. Passende Pakete verwenden die Routentabelle anstelle von PBF.
  - **Ausgangsschnittstelle** – Wählen Sie die Netzwerkinformationen aus, an die Sie den Datenverkehr weiterleiten möchten, der Ihrer richtlinienbasierten Weiterleitungsregel entspricht.
  - **Nächster Hop**
    - **IP-Adresse** – Geben Sie eine IP-Adresse ein oder wählen Sie ein Adressobjekt vom Typ „IP-Netzmaske“ aus, an das passende Pakete weitergeleitet werden sollen.
    - **FQDN** – Geben Sie einen FQDN ein (oder wählen oder erstellen Sie ein Adressobjekt vom Typ „FQDN“), an den passende Pakete weitergeleitet werden sollen.
    - **Kein** – Kein nächster Hop bedeutet, dass die Ziel-IP-Adresse des Pakets als nächster Hop verwendet wird. Die Weiterleitung schlägt fehl, wenn die Ziel-IP-Adresse nicht im selben Subnetz wie die Ausgangsschnittstelle liegt.
  - **Überwachen** – Aktivieren Sie die Überwachung, um die Konnektivität mit einer Ziel-IP-Adresse oder mit der Next-Hop-IP-Adresse zu überprüfen, wenn keine IP-Adresse angegeben ist.

# Verwalten: NAT

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>☐ Prisma Access<br>☐ AIOps for NGFW Premium<br>☐ Strata Cloud Manager Essentials<br>☐ Strata Cloud Manager Pro<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Mit NAT können Sie private, nicht routbare IPv4-Adressen in eine oder mehrere global routbare IPv4-Adressen übersetzen und so die routbaren IP-Adressen einer Organisation beibehalten. NAT ermöglicht es außerdem, die tatsächlichen IP-Adressen von Hosts, die Zugriff auf öffentliche Adressen benötigen, nicht preiszugeben und den Datenverkehr durch Portweiterleitung zu

verwalten. Mit NAT können Sie Herausforderungen im Netzwerkdesign lösen und es Netzwerken mit identischen IP-Subnetzen ermöglichen, miteinander zu kommunizieren.

Sie konfigurieren eine NAT-Richtlinienregel, die mindestens die Quellzone und Zielzone eines Pakets abgleicht. Zusätzlich zu den Zonen können Sie Übereinstimmungskriterien basierend auf der Zielschnittstelle, der Quell- und Zieladresse und dem Dienst des Pakets konfigurieren. Sie können mehrere NAT-Regeln konfigurieren.

Gehen Sie zu **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Netzwerkdienste** > **NAT**, um zu beginnen.

**Behebung** *von Konnektivitätsproblemen – erhalten Sie einen Gesamtüberblick über Ihre Routing- und Tunnelzustände und gehen Sie ins Detail, um Anomalien und problematische Konfigurationen zu finden.*

# Verwalten: SD-WAN

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • SD-WAN | ❑ SD-WAN-Lizenz |

In einer SD-WAN-Richtlinienregel werden Anwendungen und/oder Dienste sowie ein Datenverkehrsverteilungsprofil festgelegt, um zu bestimmen, wie die Firewall den bevorzugten Pfad für ein eingehendes Paket auswählt, das nicht zu einer vorhandenen Sitzung gehört und alle anderen Kriterien erfüllt, wie Quell- und Zielzonen, Quell- und Ziel-IP-Adressen und Quellbenutzer. Die SD-WAN-Richtlinienregel legt auch ein Pfadqualitätsprofil von Schwellenwerten für Latenz, Jitter und Paketverlust fest. Bei Überschreitung eines der Schwellenwerte wählt die Firewall einen neuen Pfad für die Anwendungen und/oder Dienste aus.

Um eine SD-WAN-Richtlinie zu konfigurieren, wählen Sie **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Netzwerkrichtlinien** > **SD-WAN**.

## Regeln

Sie können Vor-Regeln und Nach-Regeln in einem Freigabekontext, als freigegebene Richtlinien für alle verwalteten Firewalls oder in einem Gerätegruppenkontext definieren, um die Regeln spezifisch für eine Gerätegruppe zu machen:

- **Vor-Regeln** – Regeln, die am Anfang der Regelreihenfolge hinzugefügt und zuerst ausgewertet werden. Sie können Vor-Regeln verwenden, um die Nutzungsrichtlinie für eine Organisation durchzusetzen. Beispielsweise können Sie den Zugriff auf bestimmte URL-Kategorien blockieren oder DNS-Verkehr für alle Benutzer zulassen.
- **Nach-Regeln** – Regeln, die am Ende der Regelreihenfolge hinzugefügt und nach den Vor-Regeln und den lokal in einer Firewall definierten Regeln ausgewertet werden. Nach-Regeln enthalten für gewöhnlich Regeln, um den Zugriff auf Datenverkehr basierend auf **App-ID™**, **User-ID™** oder **Dienst** zu verweigern.

## Profile

Erstellen Sie Profile, die auf Sätze von Anwendungen und Diensten angewendet werden, die in SD-WAN-Richtlinienregeln festgelegt sind.

**Pfadqualität**

Mit SD-WAN können Sie ein Pfadqualitätsprofil für jeden Satz von Anwendungen, Anwendungsfiltern, Anwendungsgruppen, Diensten, Dienstobjekten und Dienstgruppenobjekten erstellen, die individuelle Netzwerkqualitätsanforderungen haben, und das Profil dann in einer SD-WAN-Richtlinienregel nutzen. Im Profil legen Sie maximale Schwellenwerte für drei Parameter fest: Latenz, Jitter und Paketverlust. Wenn eine SD-WAN-Verbindung einen der Schwellenwerte überschreitet, wählt die Firewall einen neuen besten Pfad für Pakete aus, die der SD-WAN-Regel entsprechen, in der Sie dieses Profil anwenden.

**SaaS-Qualität**

Mit SD-WAN können Sie SaaS-Qualitätsprofile (Software-as-a-Service) erstellen, um die Pfadzustandsqualität zwischen Ihrer Hub- oder Zweigstellen-Firewall und den serverseitigen SaaS-Anwendungen zu messen. So können Sie die Zuverlässigkeit von SaaS-Anwendungen genau überwachen und Pfade austauschen, falls sich die Pfadzustandsqualität verschlechtert. Dadurch kann die Firewall genau bestimmen, wann ein Failover auf eine andere DIA-Verbindung (Direct Internet Access, direkter Internetzugang) durchgeführt werden soll.

Das SaaS-Qualitätsprofil ermöglicht es Ihnen, die zu überwachende SaaS-Anwendung mit einem adaptiven Lernalgorithmus anzugeben, der die Anwendungsaktivität überwacht. Alternativ können Sie eine SaaS-Anwendung mit der IP-Adresse, dem FQDN oder der URL der Anwendung angeben.

**Verkehrsverteilung**

Wählen Sie für dieses Datenverkehrsverteilungsprofil die Methode aus, die die Firewall verwendet, um Sitzungen zu verteilen und bei Verschlechterung der Pfadqualität einen Failover auf einen besseren Pfad durchzuführen. Fügen Sie die Link-Tags hinzu, die die Firewall berücksichtigt, wenn sie die Verbindung bestimmt, über die sie SD-WAN-Datenverkehr weiterleitet. Sie wenden ein Datenverkehrsverteilungsprofil auf jede von Ihnen erstellte SD-WAN-Richtlinienregel an.

**Fehlerkorrektur**

Wenn Ihr SD-WAN-Datenverkehr eine Anwendung enthält, die empfindlich auf Paketverlust oder -beschädigung reagiert (beispielsweise Audio-, VoIP- oder Videokonferenzen), können Sie entweder Forward Error Correction (FEC) oder Paketduplizierung zur Fehlerkorrektur anwenden. Mit FEC kann die empfangende Firewall (Decoder) verlorene oder beschädigte Pakete wiederherstellen, indem Paritätsbits verwendet werden, die der Encoder in einen Anwendungsfluss einbettet. Paketduplizierung ist eine alternative Methode zur Fehlerkorrektur, bei der eine Anwendungssitzung von einem Tunnel in einem zweiten Tunnel dupliziert wird. Um eine dieser Methoden zu verwenden, erstellen Sie ein Fehlerkorrekturprofil und verweisen Sie innerhalb einer SD-WAN-Richtlinienregel für spezifische Anwendungen auf dieses Profil.

(Sie müssen auch angeben, welche Schnittstellen für die Firewall zur Fehlerkorrektur verfügbar sind, indem Sie in einem SD-WAN-Schnittstellenprofil angeben, dass Schnittstellen „Berechtigt für die Auswahl der Fehlerkorrekturprofilschnittstelle“ sind.)

**SD-WAN-Schnittstelle**

Erstellen Sie ein SD-WAN-Schnittstellenprofil, um die Eigenschaften von ISP-Verbindungen zu definieren und die Geschwindigkeit von Verbindungen sowie die Häufigkeit der Verbindungsüberwachung durch die Firewall festzulegen, und geben Sie ein Link-Tag für die Verbindung an. Wenn Sie dasselbe Link-Tag für mehrere Verbindungen angeben, gruppieren

(bündeln) Sie diese physischen Verbindungen zu einer gebündelten Verbindung (Fat Pipe). Sie müssen ein SD-WAN-Schnittstellenprofil konfigurieren und es für eine mit SD-WAN aktivierte Ethernet-Schnittstelle angeben, bevor Sie die Ethernet-Schnittstelle speichern können.

## Link-Tags

Erstellen Sie ein Link-Tag, um eine oder mehrere physische Verbindungen zu identifizieren, die Anwendungen und Dienste bei der SD-WAN-Verkehrsverteilung bzw. beim Failover in einer bestimmten Reihenfolge verwenden sollen. Die Gruppierung mehrerer physischer Verbindungen ermöglicht es Ihnen, die Anwendungs- und Servicequalität zu maximieren, wenn sich der Zustand der physischen Verbindung verschlechtert.

Wenn Sie überlegen, wie Sie Ihre Verbindungen gruppieren können, berücksichtigen Sie die Verwendung oder den Zweck der Verbindungen und gruppieren Sie sie entsprechend. Wenn Sie beispielsweise Verbindungen für kostengünstigen oder nicht geschäftskritischen Datenverkehr konfigurieren, erstellen Sie ein Link-Tag und gruppieren Sie diese Schnittstellen, um sicherzustellen, dass der beabsichtigte Datenverkehr hauptsächlich über diese Verbindungen geleitet wird – und nicht über teurere Verbindungen, die geschäftskritische Anwendungen oder Dienste beeinträchtigen könnten.

# Verwalten: Identitätsdienste

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>❑ Prisma Access<br>❑ AIOps for NGFW Premium<br>❑ Strata Cloud Manager Essentials<br>❑ Strata Cloud Manager Pro<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Erfahren Sie, wie Sie Ihre Identitätsdienste verwalten und sicherstellen, dass nur bestimmte Benutzer auf die richtigen Daten in Ihrem Netzwerk zugreifen können.

Gehen Sie zu **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Identitätsdienste**, um zu beginnen.

Mit Identitätsdiensten können Sie Folgendes:

- Ermöglichen Sie nur legitimen Benutzern den Zugriff auf Ihr Netzwerk, indem Sie Prisma Access mit Ihrem Identitätsanbieter (IdP) verbinden und in Verwalten: Authentifizierung die gewünschte Authentifizierungsmethode auswählen.
- Geben Sie Prisma Access schreibgeschützten Zugriff auf Ihre Active Directory-Informationen über die Verwalten: Cloud Identity Engine.
- Setzen Sie Ihre Sicherheitsrichtlinien einheitlich durch und teilen Sie per Verwalten: Identitätsweitergabe Identitätsdaten mit lokalen Geräten an Remote-Netzwerk- oder Dienstverbindungsstandorten (Hauptsitz und Rechenzentren).

# Verwalten: Authentifizierung

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>❑ Prisma Access<br>❑ AIOps for NGFW Premium<br>❑ Strata Cloud Manager Essentials<br>❑ Strata Cloud Manager Pro |

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| | → Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Um sicherzustellen, dass nur legitime Benutzer auf Ihre am besten geschützten Ressourcen zugreifen können, unterstützt Prisma Access verschiedene Authentifizierungstypen, darunter SAML, TACACS+, RADIUS, LDAP, Kerberos, MFA, lokale Datenbankauthentifizierung und SSO.

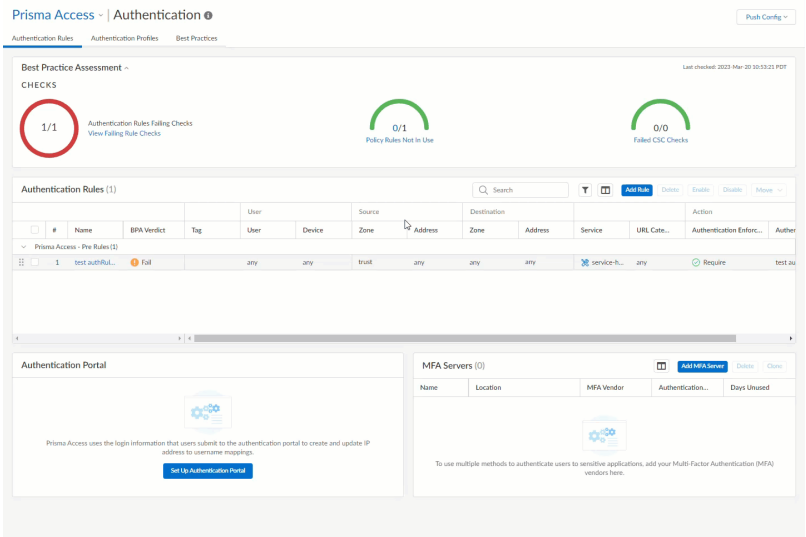
Um Ihre Authentifizierungsrichtlinien einzurichten, gehen Sie zu **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Identitätsdienste** > **Authentifizierung**.

Hier finden Sie nicht nur die Dienste, die Prisma Access integrieren kann, um die Authentifizierung bereitzustellen, sondern auch Funktionen, die Sie bei der Planung Ihrer Authentifizierungseinrichtung berücksichtigen sollten:

## Authentifizierungsunterstützung

| | |
|---|---|
| **SAML** | Wenn Ihre Benutzer auf Dienste und Anwendungen zugreifen, die sich außerhalb Ihres Netzwerks befinden, können Sie SAML verwenden, um einen Identitätsanbieter (Identity Provider, IdP) in Prisma Access zu integrieren, der den Zugriff auf externe und interne Dienste und Anwendungen steuert. SAML Single Sign-on (SSO) ermöglicht eine einzige Anmeldung für den Zugriff auf mehrere Anwendungen. Das ist in Umgebungen hilfreich, in denen jeder Benutzer auf viele Anwendungen zugreifen muss, weil hier eine separate Authentifizierung pro Anwendung die Benutzerproduktivität beeinträchtigen würde. In diesem Fall ermöglicht SAML Single Sign-on (SSO) eine einzige Anmeldung für den Zugriff auf mehrere Anwendungen. Ebenso können Benutzer über SAML Single Logout (SLO) Sitzungen für mehrere Anwendungen beenden, indem sie sich von nur einer Sitzung abmelden. SSO funktioniert für mobile Benutzer, die über die GlobalProtect-App auf Anwendungen zugreifen, oder für Benutzer in Remote-Netzwerken, die über das Authentifizierungsportal auf Anwendungen zugreifen. SLO steht Benutzern der GlobalProtect-App zur Verfügung.<br><br>*Sie können SAML-Authentifizierungsprofile nicht in Authentifizierungssequenzen verwenden.* |
| **TACACS+** | Terminal Access Controller Access-Control System Plus (TACACS+) ist eine Protokollfamilie, die die Authentifizierung und Autorisierung über einen zentralen Server ermöglicht. TACACS+ verschlüsselt Benutzernamen und Passwörter und ist damit sicherer als RADIUS, das nur Passwörter |

| | |
|---|---|
| | verschlüsselt. TACACS+ ist auch zuverlässiger, da es TCP verwendet, während RADIUS UDP verwendet. |
| **RADIUS** | Der Remote Authentication Dial-In User Service (RADIUS) ist ein breit unterstütztes Netzwerkprotokoll, das eine zentrale Authentifizierung und Autorisierung ermöglicht. Sie können Prisma Access auch einen RADIUS-Server hinzufügen, um Multi-Faktor-Authentifizierung zu implementieren. |
| **LDAP** | Lightweight Directory Access Protocol (LDAP) ist ein Standardprotokoll für den Zugriff auf Informationsverzeichnisse. Sie können LDAP verwenden, um Benutzer zu authentifizieren, die über das Authentifizierungsportal auf Anwendungen oder Dienste zugreifen. |
| **Kerberos** | Kerberos ist ein Authentifizierungsprotokoll, das einen sicheren Informationsaustausch zwischen Parteien ermöglicht, indem eindeutige Schlüssel (sogenannte Tickets) verwendet werden, um die Parteien zu identifizieren. Mit Kerberos können Sie Benutzer authentifizieren, die über das Authentifizierungsportal auf Anwendungen zugreifen. Wenn Kerberos SSO aktiviert ist, müssen sich Benutzer nur beim ersten Zugriff auf Ihr Netzwerk anmelden (z. B. eine Anmeldung bei Microsoft Windows). Nach dieser ersten Anmeldung können sie auf jeden browserbasierten Dienst im Netzwerk zugreifen, ohne sich erneut anmelden zu müssen, bis die SSO-Sitzung abläuft.<br><br>Um Kerberos verwenden zu können, benötigen Sie zunächst ein Kerberos-Konto für Prisma Access, das Benutzer authentifiziert. Ein Konto ist erforderlich, um ein Kerberos-Keytab zu erstellen. Dabei handelt es sich um eine Datei, die den Prinzipalnamen und das gehashte Passwort der Firewall bzw. von Panorama enthält. Für den SSO-Vorgang ist das Keytab erforderlich.<br><br>Kerberos SSO ist nur für Dienste und Anwendungen verfügbar, die in Ihrer Kerberos-Umgebung intern sind. Verwenden Sie SAML, um SSO für externe Dienste und Anwendungen zu aktivieren. |
| **Cloud Identity Engine** | Die Cloud Identity Engine (CIE) bietet sowohl Benutzeridentifikation als auch Benutzerauthentifizierung für mobile Benutzer in einer Prisma Access-Bereitstellung mit explizitem Proxy. Die Cloud Identity Engine ist in den Authentication Cache Service (ACS) des expliziten Proxys integriert und verwendet SAML-Identitätsanbieter (IdPs), um die Authentifizierung für mobile Benutzer des expliziten Proxys bereitzustellen. |

| | |
|---|---|
| **MFA** | Multi-Faktor-Authentifizierung (MFA) bietet Ihnen die Möglichkeit, mehrere Authentifizierungsmethoden verschiedener Art (sogenannte *Faktoren*) zu implementieren, um Ihre vertraulichsten Dienste und Anwendungen zu schützen. Beispielsweise möchten Sie möglicherweise für wichtige Finanzdokumente eine stärkere Authentifizierung als für Suchmaschinen.<br><br>Prisma Access verfügt über eine integrierte Liste der unterstützten MFA-Anbieter, die automatisch aktualisiert wird, wenn neue Anbieter hinzugefügt werden:<br><br>  |
| **Lokale Datenbankauthentifizierung** | Erstellen Sie eine Datenbank, die lokal in Prisma Access läuft und Benutzerkonten (Benutzernamen und Passwörter oder gehashte Passwörter) enthält. Diese Art der Authentifizierung ist nützlich, um in Fällen, in denen Sie nur die gehashten Passwörter, aber nicht die Klartext-Passwörter kennen, Benutzerkonten zu erstellen, die die Anmeldeinformationen vorhandener Unix-Konten wiederverwenden. Für Konten, die Klartext-Passwörter verwenden, können Sie auch Passwortkomplexität und Ablaufeinstellungen definieren. Diese Authentifizierungsmethode steht Benutzern zur Verfügung, die über das Authentifizierungsportal oder die GlobalProtect-App auf Dienste und Anwendungen zugreifen. |

## Highlights der Authentifizierungsfunktion

| | |
|---|---|
| **SSO** | Wenn Sie SAML oder Kerberos verwenden, können Sie Single Sign-on (SSO) implementieren, damit sich Benutzer nur einmal authentifizieren müssen, um auf mehrere Dienste und Anwendungen zuzugreifen. SAML und Kerberos unterstützen SSO. |

| | |
|---|---|
| **Authentifizierungsportal** | Leiten Sie Webanfragen, die einer Authentifizierungsregel entsprechen, an eine Prisma Access-Anmeldeseite weiter, auf der sie zur Authentifizierung aufgefordert werden. Prisma Access verwendet die Informationen, die der Benutzer an dieses Authentifizierungsportal übermittelt, um Zuordnungen von IP-Adressen zu Benutzernamen zu erstellen oder zu aktualisieren.<br><br>Dies ist besonders für Remote-Netzwerke nützlich, wo Datenverkehrsüberwachung und Richtliniendurchsetzung weiterhin auf Grundlage eines Benutzers (oder einer Gruppe) durchgeführt werden müssen. Wenn ein Benutzer Webdatenverkehr (HTTP oder HTTPS) initiiert, der einer Authentifizierungsregel entspricht, fordert Prisma Access den Benutzer auf, sich über das Authentifizierungsportal zu authentifizieren. Prisma Access erstellt oder aktualisiert die Zuordnung der IP-Adresse zum Benutzernamen auf Grundlage der Informationen, die der Benutzer an das Portal übermittelt. Dies stellt sicher, dass Sie genau wissen, wer an einem Remote-Netzwerkstandort auf Ihre sensibelsten Anwendungen und Daten zugreift. |
| **Authentifizierungssequenz** | Wenn Sie mehrere Arten der Authentifizierung für unterschiedliche Zwecke verwenden, können Sie eine Authentifizierungssequenz festlegen, um Ihre Profile in eine Rangfolge zu bringen. Prisma Access überprüft jedes Profil auf der Basis Ihrer Rangfolge, bis eines den Benutzer erfolgreich authentifiziert. |

### So funktioniert die Authentifizierung

Nachdem Sie die Authentifizierungsdienste Ihres Unternehmens zu Prisma Access hinzugefügt haben (hier erfahren Sie, wie das funktioniert), authentifiziert Prisma Access Benutzer an mehreren Stellen:

- **Wenn sie eine Verbindung zu Prisma Access herstellen**

  So definieren Sie, wie sich mobile Benutzer bei Prisma Access authentifizieren sollen. Sie müssen keine Authentifizierungseinstellungen für Benutzer in Remote-Netzwerken definieren, um eine Verbindung zu Prisma Access herzustellen, da der Remote-Netzwerkverkehr durch sichere VPN-Tunnel geleitet wird.

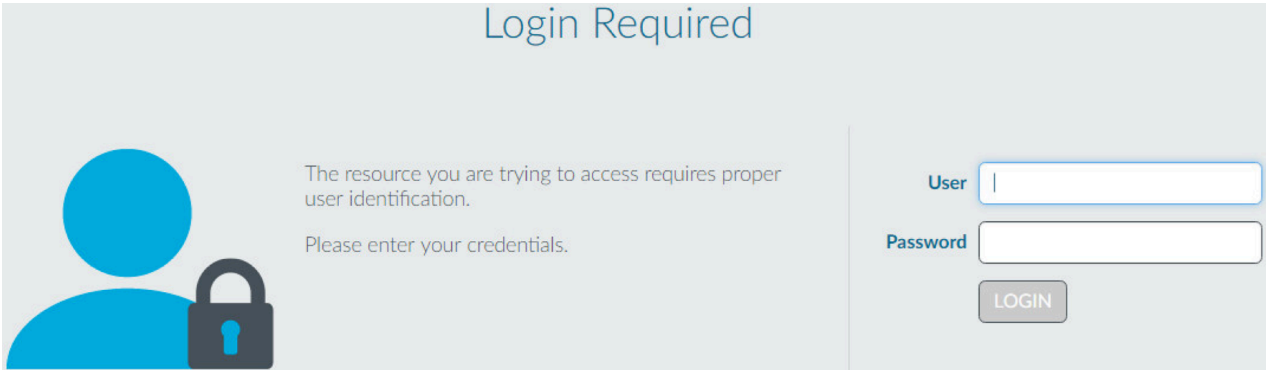
- **Wenn der Benutzerdatenverkehr Ihre Anforderungen für eine zusätzliche Authentifizierung erfüllt**

  So fordern Sie Benutzer auf, sich zu authentifizieren (mit einer oder mehreren Methoden), um auf Unternehmensanwendungen und geschützte Netzwerkressourcen zuzugreifen.

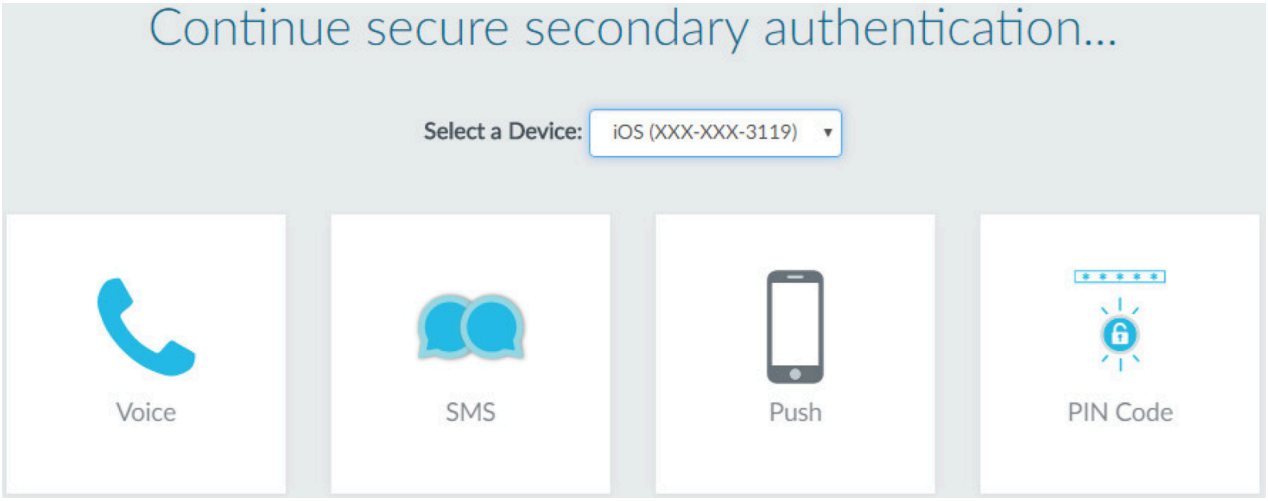
*Wenn Benutzer Webdatenverkehr generieren, der Ihren Authentifizierungsanforderungen entspricht, überprüft Prisma Access, ob die Benutzer legitim sind, indem es sie auffordert, sich mit einer oder mehreren Methoden (Faktoren) zu authentifizieren, z. B. mit Benutzername und Passwort oder per Sprach-, SMS-, Push- oder OTP-Authentifizierung (One-Time Password, Einmalpasswort). Die Faktoren,*

*die Prisma Access verwendet, basieren alle auf dem Authentifizierungsdienst und den Einstellungen, die Sie in Ihren Authentifizierungsprofilen angeben.* Beim ersten Faktor (Benutzername und Passwort) authentifizieren sich Benutzer über das Authentifizierungsportal.




Bei den anderen Faktoren authentifizieren sich Benutzer dann über eine MFA-Anmeldeseite.




Nach der Authentifizierung der Benutzer bewertet Prisma Access Ihre Sicherheitsregeln, um festzustellen, ob der Zugriff auf die Anwendung zulässig ist. Prisma Access protokolliert alle Aktivitäten, bei denen Benutzer versuchen, auf Anwendungen, Dienste oder Ressourcen zuzugreifen, für die Sie sicheren Zugriff vorgesehen haben.

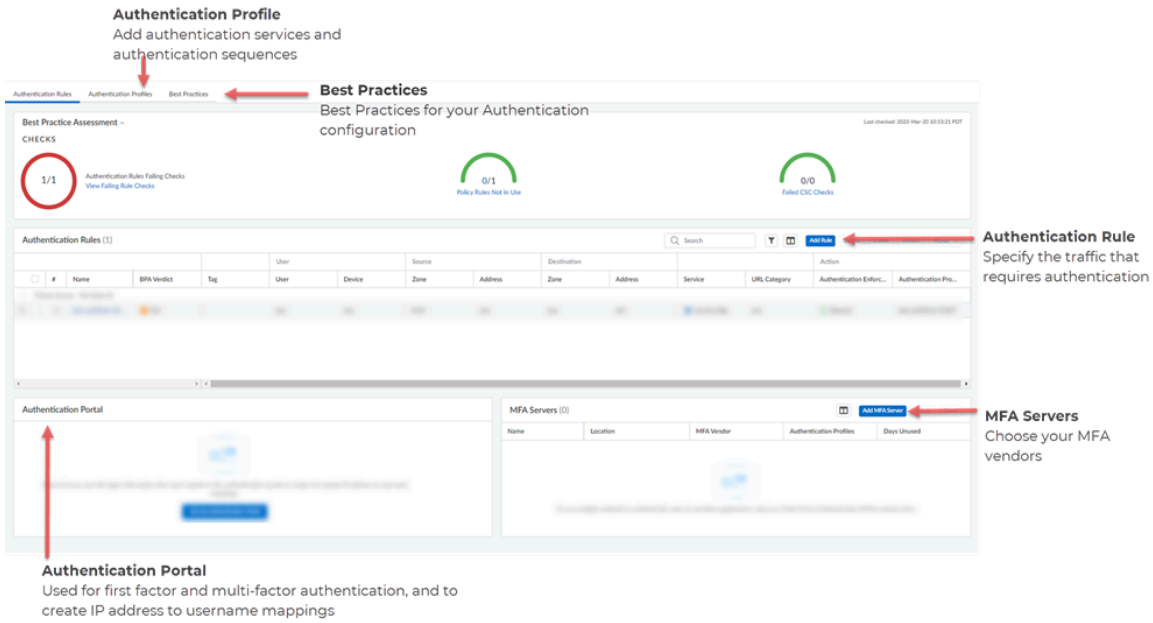
## Verwalten: Authentifizierungseinrichtung

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager) | Eine der folgenden Komponenten:<br>❑ Prisma Access-Lizenz<br>❑ Strata Cloud Manager Pro<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Um die Authentifizierung mit Prisma Access in Strata Cloud Manager einzurichten, fügen Sie zunächst Ihre Authentifizierungsdienste zu Prisma Access hinzu. Geben Sie dann den Datenverkehr an, für den eine Authentifizierung erforderlich sein soll. Bauen Sie auf diesen Einstellungen auf, um weitere Authentifizierungsfunktionen wie MFA und Authentifizierungssequenzen hinzuzufügen, oder richten Sie Prisma Access so ein, dass es Zuordnungen von IP-Adressen zu Benutzernamen erstellt und aktualisiert.

So können Sie loslegen – alle Einstellungen, die Sie zum Aktivieren der Authentifizierung mit Prisma Access benötigen, befinden sich an einem Ort: **Verwalten** > **Identitätsdienste** > **Authentifizierung**.



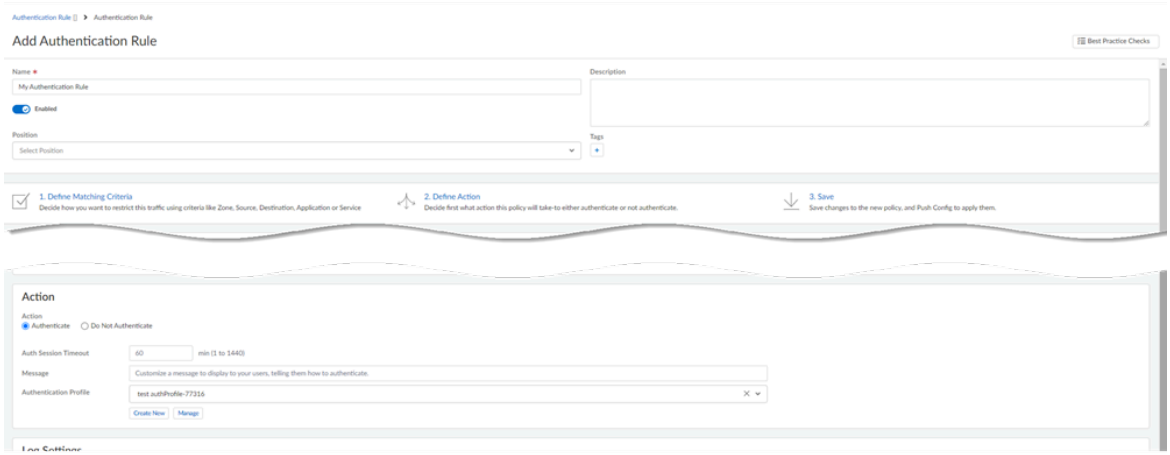

- **Authentifizierungsregeln:** Hier geben Sie den Datenverkehr an, für den eine Authentifizierung erforderlich sein soll.

  Zum Einrichten einer Authentifizierungsregel gehört auch das Hinzufügen eines Authentifizierungsprofils zur Regel. Wenn Prisma Access Datenverkehr erkennt, der einer Authentifizierungsregel entspricht, wendet es die im Authentifizierungsprofil definierten Authentifizierungsmethoden und -einstellungen auf den entsprechenden Datenverkehr an. Das Profil definiert, wie sich die Benutzer authentifizieren müssen.

  1. Gehen Sie zu **Verwalten** > **Identitäts- und Zugriffsdienste** > , **Authentifizierung** > **Authentifizierungsregel** und wählen Sie **Authentifizierungsregel hinzufügen** aus.
  2. Definieren Sie die Benutzer, Dienste und URL-Kategorien, die eine Authentifizierung erfordern.

3. Legen Sie die Regelaktion auf **Authentifizieren** fest und wählen Sie das **Profil** aus, das die Authentifizierungsmethode für Datenverkehr definiert, der dieser Regel entspricht.




- **Authentifizierungsprofil:** Fügen Sie hier Ihre Authentifizierungsdienste hinzu und definieren Sie die Authentifizierungseinstellungen.

  Verbinden Sie Prisma Access mit den Diensten, die Sie zur Benutzerauthentifizierung verwenden möchten – SAML, TACACS+, RADIUS, LDAP oder Kerberos –, und definieren Sie Authentifizierungseinstellungen (legen Sie beispielsweise ein Limit für fehlgeschlagene Anmeldeversuche fest).

  *Wenn Sie einen lokalen Authentifizierungsdienst verwenden, müssen Sie zuerst eine Dienstverbindung erstellen, um den lokalen Authentifizierungsdienst mit Prisma Access zu verbinden. Kehren Sie dann hierher zurück, um Ihr Authentifizierungsprofil einzurichten.*

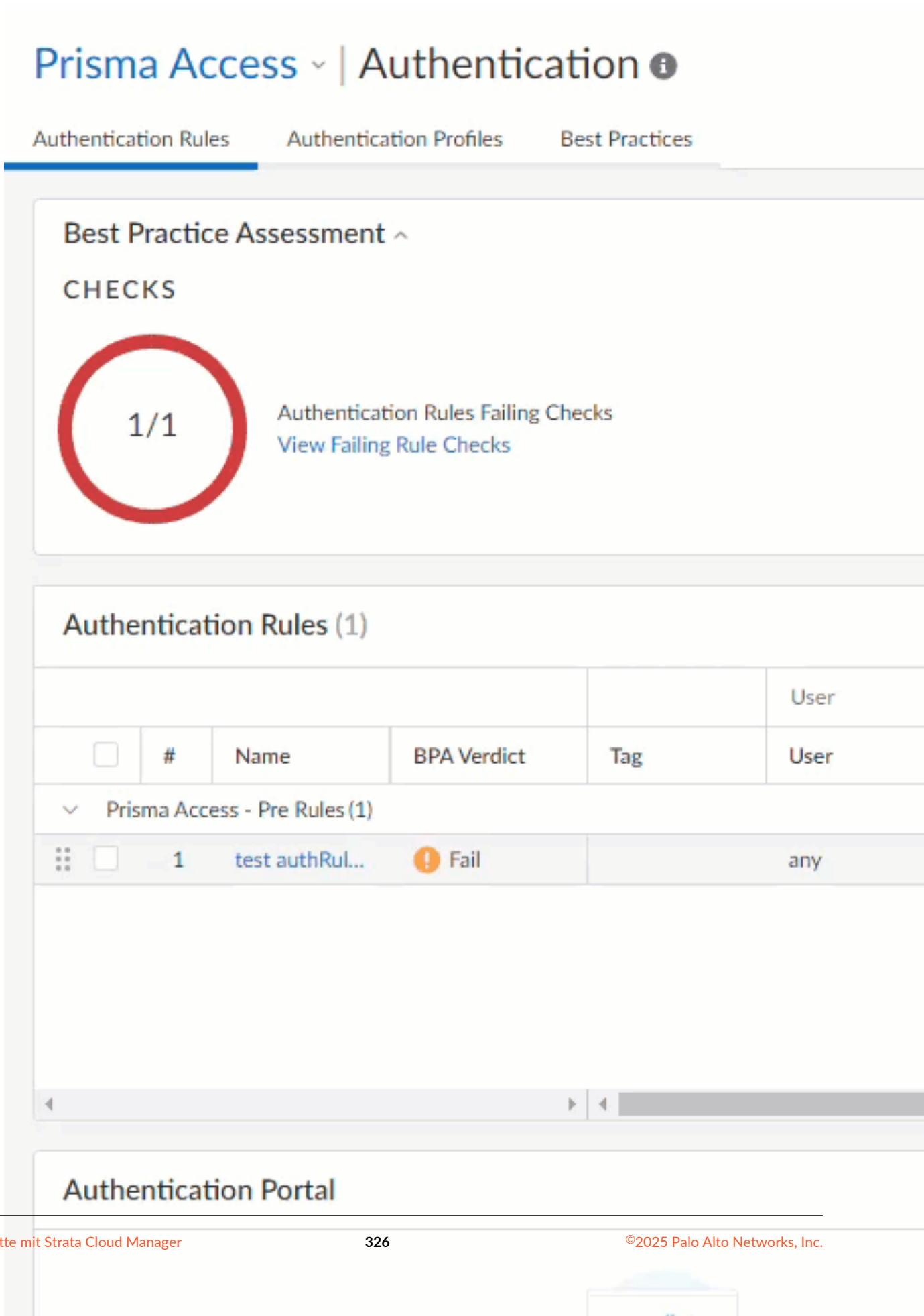
  Gehen Sie zu **Verwalten** > **Identitäts- und Zugriffsdienste** > **Authentifizierung** > **Authentifizierungsprofil** > **Profil hinzufügen** und legen Sie zunächst den **Authentifizierungstyp** für das Profil fest:

  Sie werden aufgefordert, Details zu dem von Ihnen ausgewählten Authentifizierungsdienst hinzuzufügen, der es Prisma Access ermöglicht, eine Verbindung mit dem Dienst herzustellen und Benutzeranmeldedaten und Rollenberechtigungen zu lesen. Im Profil werden zusätzliche Einstellungen zum Anpassen der Authentifizierung bereitgestellt, die je nach Art der eingerichteten Authentifizierung variieren können.

- **MFA-Server:** Geben Sie den von Ihnen verwendeten MFA-Anbieter an.

  Um bei vertraulichen Anwendungen mehrere Methoden zur Benutzerauthentifizierung zu verwenden, fügen Sie zunächst die MFA-Anbieter hinzu, die Sie verwenden möchten (**MFA-Server hinzufügen**). Prisma Access stellt Ihnen eine Liste von MFA-Anbietern zur Auswahl.



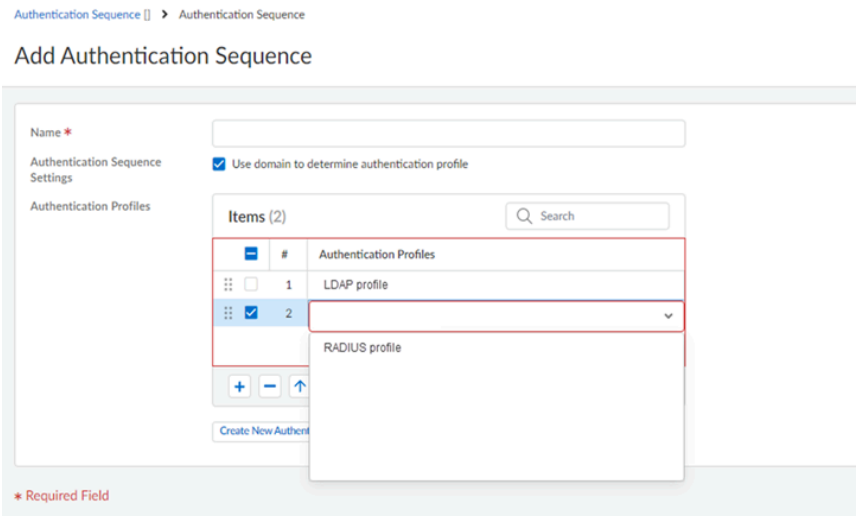
- **Authentifizierungsportal:** Richten Sie das Authentifizierungsportal (auch *Captive Portal* genannt) für Benutzer an Remote-Netzwerkstandorten ein und ermöglichen Sie es Prisma Access, Zuordnungen von IP-Adressen zu Benutzernamen zu erstellen.

  Bei der Authentifizierung mit dem ersten Faktor (Benutzername und Kennwort) müssen sich Benutzer an Remote-Netzwerkstandorten über das Authentifizierungsportal authentifizieren. Wenn die Authentifizierung erfolgreich ist, zeigt Prisma Access für jeden zusätzlichen erforderlichen Authentifizierungsfaktor eine MFA-Anmeldeseite an. Prisma Access verwendet die von Benutzern übermittelten Anmeldeinformationen, um Zuordnungen von IP-Adressen zu Benutzernamen zu erstellen und zu aktualisieren. Das bedeutet, dass Sie immer wissen, wer an einem Remote-Netzwerkstandort auf Webinhalte und Unternehmensanwendungen zugreift.

- 

- **Authentifizierungsreihenfolge:** Ordnen Sie die Authentifizierungsprofile in der Reihenfolge, in der Prisma Access sie anwenden soll.

  Wählen Sie **Verwalten** > **Identitäts- und Zugriffsdienste** > **Authentifizierung** > **Authentifizierungsprofil** und wählen Sie **Authentifizierungssequenz hinzufügen** aus, um Ihre Authentifizierungsprofile anzuordnen. Prisma Access überprüft sie alle der Reihe nach, bis eines der Profile den Benutzer erfolgreich authentifiziert.




## Verwalten: Authentifizierungsprofile

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager) | Eine der folgenden Komponenten:<br>☐ Prisma Access-Lizenz<br>☐ Strata Cloud Manager Pro<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung |

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| | stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Ein Authentifizierungsprofil definiert den Authentifizierungsdienst, der die Anmeldeinformationen von Administratoren validiert, die auf die Firewall-Weboberfläche zugreifen, sowie von Endbenutzern, die über Captive Portal oder GlobalProtect auf Anwendungen zugreifen. Das Authentifizierungsprofil definiert auch Optionen wie Single Sign-on (SSO).

- Kerberos
- Cloud Identity Engine

**Cloud Identity Engine**

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access-Lizenz |

Die Cloud Identity Engine (CIE) bietet sowohl Benutzeridentifikation als auch Benutzerauthentifizierung für mobile Benutzer in einer Prisma Access-Bereitstellung mit explizitem Proxy. Die Cloud Identity Engine ist in den Authentication Cache Service (ACS) des expliziten Proxys integriert und verwendet SAML-Identitätsanbieter (IdPs), um die Authentifizierung für mobile Benutzer des expliziten Proxys bereitzustellen.

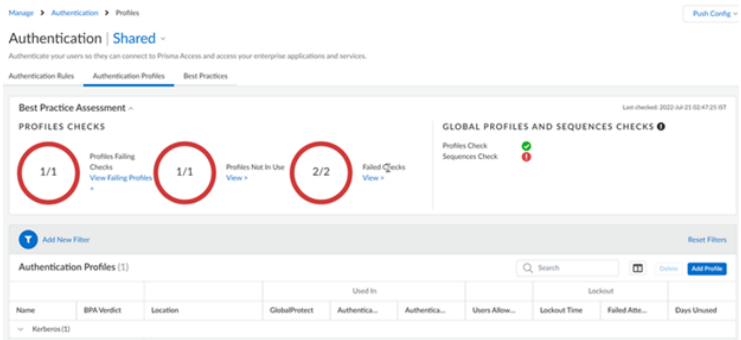
Konfigurieren Sie ein Authentifizierungsprofil, um Benutzer mit der Cloud Identity Engine zu authentifizieren.

Die SAML-/CIE-Authentifizierungsmethode wird nur angezeigt, wenn der Cloud Authentication Service (CAS) aktiviert ist. Wenn die CIE-Authentifizierung oder CAS auf Ihrem Prisma Access-Mandanten nicht unterstützt wird, wird nur die SAML-Authentifizierungsmethode angezeigt.

Bevor Sie beginnen:

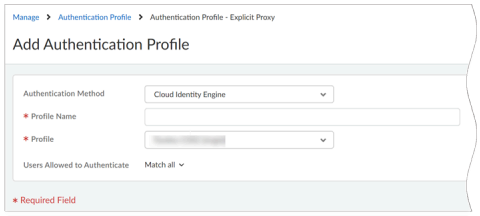
- Lesen Sie die Richtlinien für explizite Proxys.
- Richten Sie ein Authentifizierungsprofil in der Cloud Identity Engine ein.

**STEP 1 |** Gehen Sie zu **Verwalten** > **Konfiguration** > **Identitätsdienste** > **Authentifizierung**, legen Sie den Konfigurationsumfang auf **Expliziter Proxy** fest und wählen Sie unter **Authentifizierungsprofile** die Option **Profil hinzufügen** aus, um ein Profil hinzuzufügen.



**STEP 2 |** Wählen Sie die **Authentifizierungsmethode** aus: **Cloud Identity Engine**.




**STEP 3 |** Geben Sie einen eindeutigen **Profilnamen** ein.

**STEP 4 |** Wählen Sie unter **Profil** das Cloud Identity Engine-Authentifizierungsprofil aus, das Sie in der Cloud Identity Engine konfiguriert haben.

**STEP 5 |** **Save (Speichern)** Sie Ihre Änderungen.

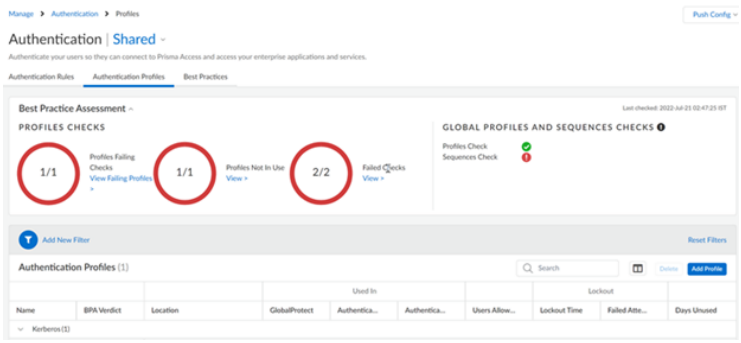
### Kerberos

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access-Lizenz |

Kerberos ist ein Authentifizierungsprotokoll für Computernetzwerke. Es verwendet Tickets, damit sich Knoten, die über ein unsicheres Netzwerk kommunizieren, auf sichere Weise gegenseitig ihre Identität mitteilen können.

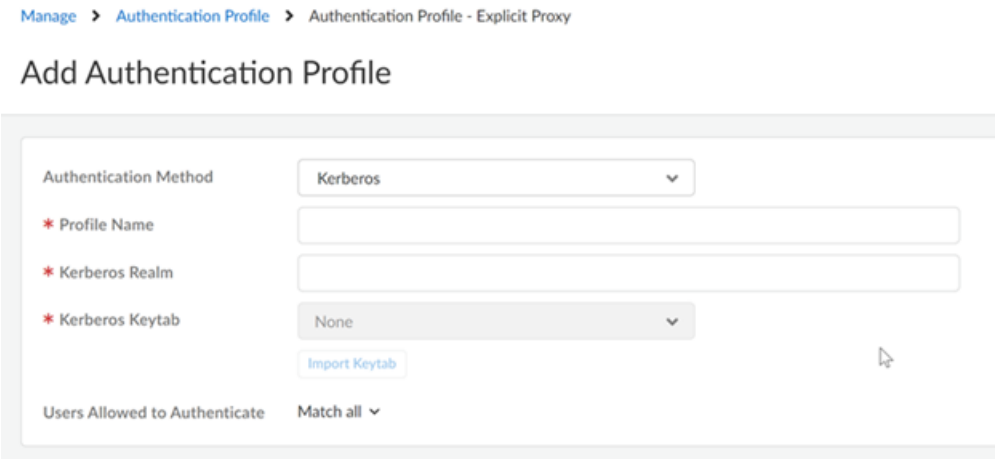
Das Authentifizierungsprofil gibt das Serverprofil an, das vom Portal oder den Gateways zur Benutzerauthentifizierung verwendet wird. Befolgen Sie diese Schritte, um ein Kerberos-Authentifizierungsprofil für mobile Benutzer des expliziten Proxys einzurichten, damit sie eine Verbindung mit Prisma Access herstellen können.

**STEP 1 |** Gehen Sie zu **Verwalten** > **Konfiguration** > **Identitätsdienste** > **Authentifizierung** > **Authentifizierungsprofile** und wählen Sie **Profil hinzufügen** aus.



**STEP 2 |** Wählen Sie die **Authentifizierungsmethode** aus: **Kerberos**.




**STEP 3 |** Geben Sie einen eindeutigen **Profilnamen** ein, um das Profil zu identifizieren. Das Authentifizierungsprofil gibt das Serverprofil an, das vom Portal oder den Gateways zur Benutzerauthentifizierung verwendet wird.

**STEP 4 |** Geben Sie den **Kerberos-Bereich** (bis zu 127 Zeichen) ein, um den Hostnamen-Teil des Benutzer-Anmeldenamens anzugeben. Beispielsweise weist der Benutzerkontoname „user@EXAMPLE.LOCAL“ den Bereich „EXAMPLE.LOCAL“ auf.

**STEP 5 |** **Importieren** Sie eine **Kerberos-Keytab**-Datei, die die Kerberos-Kontoinformationen enthält. Suchen Sie bei der entsprechenden Eingabeaufforderung nach der Keytab-Datei und klicken Sie dann auf **Speichern**. Während der Authentifizierung versucht der Endpunkt zunächst, SSO mithilfe des Keytabs durchzuführen.

**STEP 6 |** Wählen Sie das **Kerberos-Keytab**.

**STEP 7 |** Klicken Sie auf **Save (Speichern)**.

# Verwalten: Cloud Identity Engine

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>❑ Prisma Access<br>❑ AIOps for NGFW Premium<br>❑ Strata Cloud Manager Essentials<br>❑ Strata Cloud Manager Pro<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Cloud Identity Engine (Directory Sync) gewährt Prisma Access schreibgeschützten Zugriff auf Ihre Active Directory-Informationen, sodass Sie Sicherheits- und Entschlüsselungsrichtlinien für Benutzer und Gruppen einfach einrichten und verwalten können.

Cloud Identity Engine funktioniert sowohl mit lokalem Active Directory als auch mit Azure Active Directory.

Um Cloud Identity Engine mit Prisma Access einzurichten, gehen Sie zunächst zum Hub, um Cloud Identity Engine zu aktivieren und zu Prisma Access hinzuzufügen. Gehen Sie dann zu Prisma Access, um zu überprüfen, ob Prisma Access auf Verzeichnisdaten zugreifen kann.

**STEP 1 |** Aktivierung von Cloud Identity Engine

Die Cloud Identity Engine kann Active Directory-Informationen mit jeder unterstützten Anwendung im Hub teilen. Sie ist kostenlos und erfordert zum Einstieg keinen Authentifizierungscode. Zur Einrichtung der Cloud Identity Engine gehört das Aktivieren der Cloud Identity Engine-Anwendung im Hub, das Konfigurieren des Cloud Identity Engine-Agents zum Erfassen von Active Directory-Zuordnungen sowie die Konfiguration der gegenseitigen Authentifizierung zwischen Cloud Identity Engine und dem Agent.

Stellen Sie sicher, dass die Cloud Identity Engine-Instanz in derselben Region bereitgestellt wird, in der Sie Prisma Access und Strata Logging Service bereitgestellt haben.

**STEP 2 |** Aktivieren Sie die Cloud Identity Engine für Prisma Access.

Sie können Prisma Access bei Ihrer ersten Prisma Access-Aktivierung oder zu einem beliebigen späteren Zeitpunkt mit der Cloud Identity Engine verknüpfen:

- **Bei der Prisma Access-Aktivierung:** Wenn Sie Cloud-verwaltetes Prisma Access zum ersten Mal aktivieren, können Sie eine Cloud Identity Engine-Instanz für die Verwendung durch Prisma Access auswählen. Stellen Sie sicher, dass Sie eine Instanz auswählen, die in derselben Region wie Prisma Access bereitgestellt wird.
- **Nach der Prisma Access-Aktivierung:** Um die Cloud Identity Engine für eine vorhandene Prisma Access-Instanz zu aktivieren, melden Sie sich beim Hub an. Wählen Sie im Dropdown-Menü der Hub-Einstellungen (siehe Zahnrad in der oberen Menüleiste) die Option **Apps verwalten** aus. Suchen Sie die Prisma Access-Instanz, die Sie aktualisieren möchten, und wählen Sie die Cloud Identity Engine-Instanz aus, die Prisma Access verwenden soll.

**STEP 3 |** Bestätigen Sie, dass Prisma Access mit der Cloud Identity Engine verbunden ist und dass Cloud Identity Engine Verzeichnisinformationen mit Prisma Access teilt.

- Überprüfen Sie, ob Sie Ihre Verzeichnisse in Prisma Access sehen können.

  Gehen Sie zu **Verwalten** > **Konfiguration** > **Identitätsdienste** > **Cloud Identity Engine**:
- Überprüfen Sie, ob Sie einer Richtlinienregel Benutzer und Gruppen hinzufügen können.

  Wählen Sie **Verwalten** > **Sicherheitsdienste** > **Sicherheit** oder **Entschlüsselung** aus. Überprüfen Sie in einer Sicherheits- oder Entschlüsselungsrichtlinienregel, ob in der Dropdown-Liste **Benutzer** Ihre Active Directory-Benutzer- und -Gruppeneinträge

angezeigt werden. Jetzt können Sie damit beginnen, diese Benutzer und Gruppen zu Ihren Sicherheits- und Entschlüsselungsrichtlinienregeln hinzuzufügen.

**Beheben Sie Probleme** *mit Datenverkehr, bei dem Regeln nicht wie erwartet durchgesetzt werden. Überprüfen Sie den Status bestimmter Firewalls, um festzustellen, ob eine Nichtübereinstimmung zwischen den erwarteten Richtlinien (wie konfiguriert) und den durchgesetzten Richtlinien besteht.*

# Verwalten: Identitätsweitergabe

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>☐ Prisma Access<br>☐ AIOps for NGFW Premium<br>☐ Strata Cloud Manager Essentials<br>☐ Strata Cloud Manager Pro<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Verwenden Sie Strata Cloud Manager, um die Identitätsweitergabe für NGFWs und Prisma Access einzurichten und zu verwalten.

- Prisma Access
- NGFW

## Identitätsweitergabe (Prisma Access)

Damit Sie Ihre Sicherheitsrichtlinien einheitlich durchsetzen können, teilt Prisma Access Identitätsdaten, die GlobalProtect entdeckt, lokal in Ihrer gesamten Prisma Access-Umgebung. Prisma Access kann auch Identitätsdaten mit lokalen Geräten an Remote-Netzwerk- oder Dienstverbindungsstandorten (Hauptsitz und Rechenzentren) teilen.

Für Prisma Access Cloud Management haben wir standardmäßig einige Weitergaben von Identitätsdaten aktiviert – und für die übrigen Daten haben wir die Konfiguration zur Aktivierung der Weitergabe sehr einfach gemacht (wählen Sie einfach ein Kontrollkästchen aus, um auszuwählen, welche Daten Sie teilen möchten).

Im Dashboard „Identitätsweitergabe“ können Sie sehen, wie Identitätsdaten gemeinsam genutzt werden, und die Datenweitergabe verwalten (**Verwalten** > **Konfiguration** > **Identitätsdienste** > **Identitätsweitergabe**).

Zu den Identitätsdaten, die Sie weitergeben können, gehören:

- HIP-Daten
- IP-Adresse-zu-Tag-Zuordnungen

- IP-Adresse-zu-Benutzer-Zuordnungen
- Benutzer-zu-Tag-Zuordnungen
- Geräte in Quarantäne

Erste Schritte mit der Identitätsweitergabe:

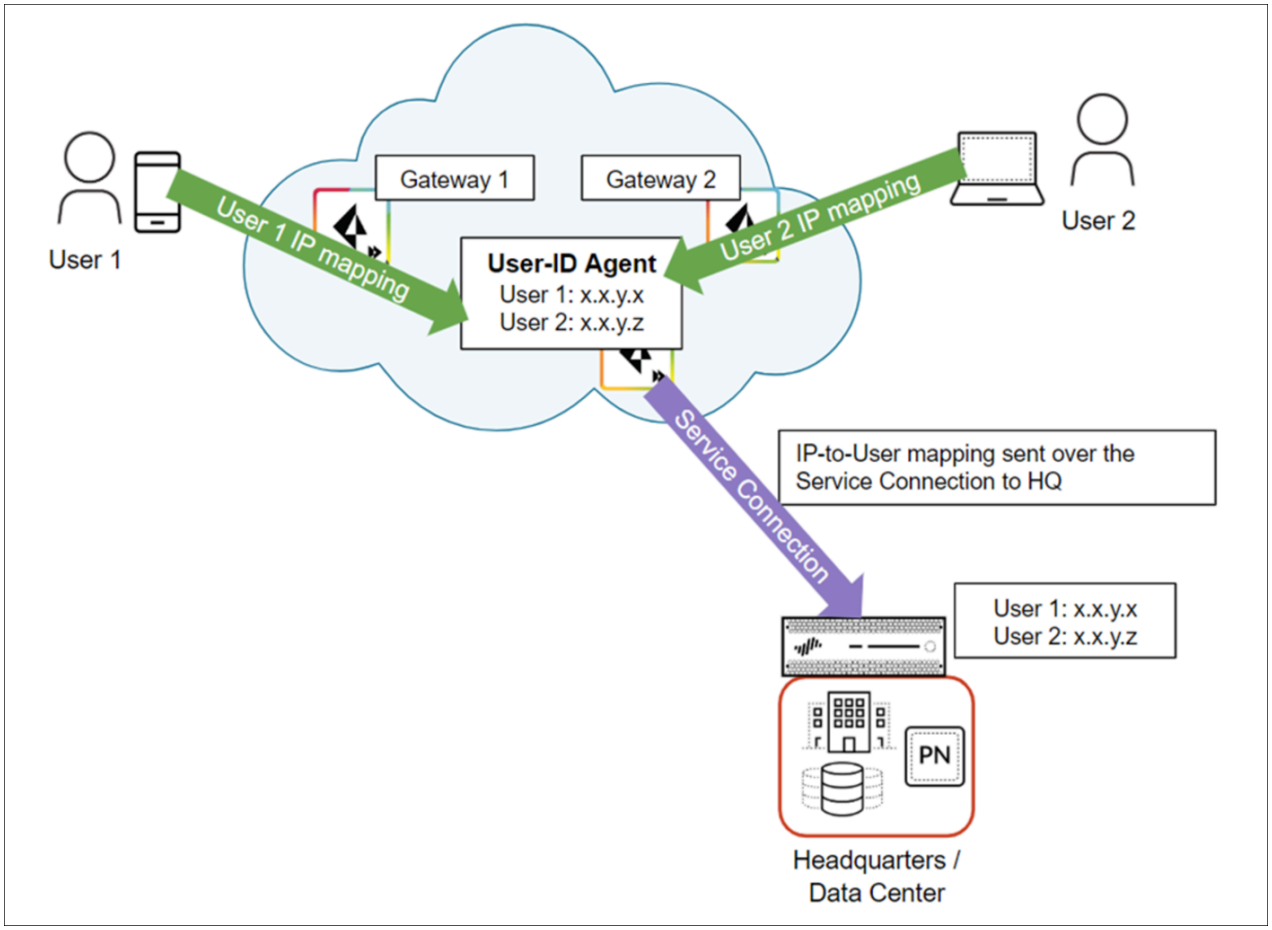
### So funktioniert die Identitätsweitergabe

Damit mobile Benutzer auf eine Ressource an einem Remote-Netzwerkstandort oder in einem Hauptsitz/Rechenzentrum zugreifen können, der/das durch ein Gerät mit benutzerbasierten Richtlinien gesichert ist, müssen Sie die Identitätsdaten der mobilen Prisma Access-Benutzer und der Remote-Netzwerk-Benutzer an dieses On-Premises-Gerät weitergeben.

Wenn Benutzer eine Verbindung zu Prisma Access herstellen, erfasst Prisma Access ihre Identitätsdaten und speichert sie.

Das folgende Beispiel zeigt zwei mobile Benutzer, für die eine IP-Adresse-zu-Benutzername-Zuordnung in Prisma Access besteht. Prisma Access gibt diese Zuordnung dann über eine Dienstverbindung an die lokalen Geräte weiter, die den Hauptsitz / das Rechenzentrum sichern.

Prisma Access Cloud Management ermöglicht es automatisch, dass Dienstverbindungen als Agents für die Identitätsweitergabe fungieren (sie werden auch als „User-ID-Agents“ bezeichnet).



### Einrichten der Identitätsweitergabe

- Bestätigen Sie die Einrichtung Ihrer Dienstverbindung:

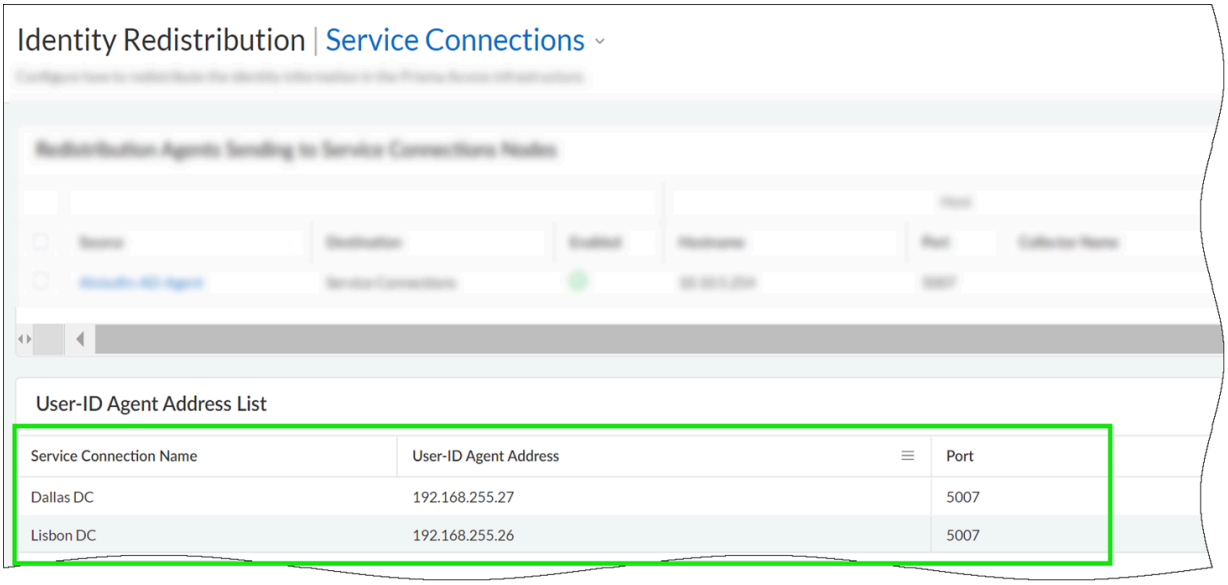
  Wenn Sie noch keine Dienstverbindung für Ihren Hauptsitz oder Ihre Rechenzentren eingerichtet haben, konfigurieren Sie zunächst eine Dienstverbindung. Eine Dienstverbindung ist erforderlich, damit Prisma Access Identitätsdaten in Ihrer gesamten Umgebung austauschen kann. Prisma Access ermöglicht automatisch, dass Dienstverbindungen als Weitergabe-Agents fungieren. Ein neu erstellter Dienstverbindungsstandort ist bereit zur Verwendung als Weitergabe-Agent, wenn Sie sehen, dass ihm eine User-ID-Agent-Adresse zugewiesen wurde (Prisma Access erledigt dies automatisch, es dauert nur einige Minuten). Gehen Sie zu **Verwalten** > **Konfiguration** > **Identitätsdienste** > **Identitätsweitergabe** und legen Sie den Konfigurationsumfang auf **Dienstverbindungen** fest, um die Details des User-ID-Agents für die Dienstverbindung zu überprüfen.

- Senden Sie Identitätsdaten von Prisma Access an lokale -Geräte

  Die User-ID-Agent-Informationen der Dienstverbindung sind alles, was Sie benötigen, um Prisma Access so zu konfigurieren, dass Identitätsdaten an lokale Geräte weitergegeben werden.

  Gehen Sie zu **Verwalten** > **Konfiguration** > **Identitätsdienste** > **Identitätsweitergabe** und legen Sie den Konfigurationsumfang auf **Dienstverbindungen** fest, um die Details des User-ID-Agents für die Dienstverbindung abzurufen.

  Verwenden Sie diese Details, um Prisma Access in Panorama oder einer NGFW als Datenweitergabe-Agent zu konfigurieren.



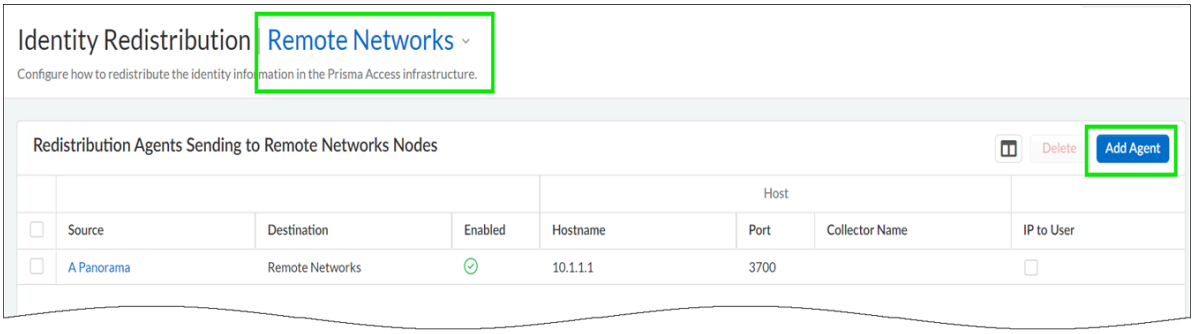

 

- Senden Sie Identitätsdaten von lokalen Geräten an Prisma Access:

  Fügen Sie lokale Geräte als Weitergabe-Agents zu Prisma Access hinzu. Die Geräte, die Sie hinzufügen, können Identitätsdaten an Prisma Access weitergeben.

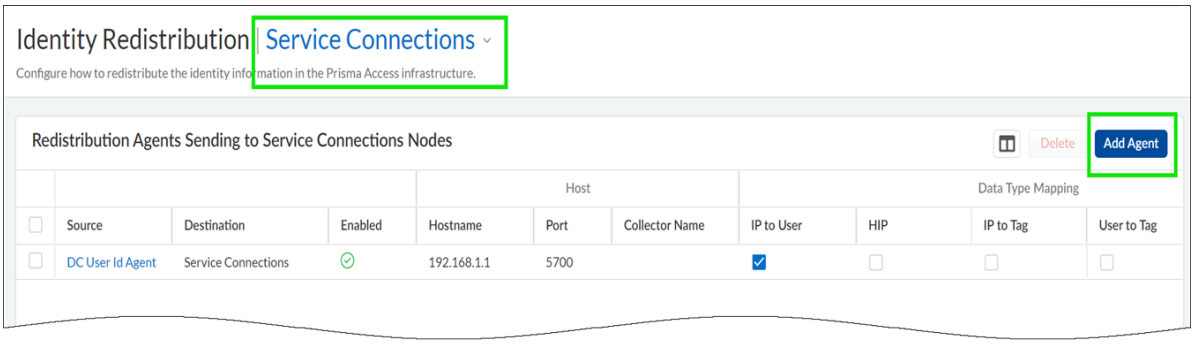
  - **Über Geräte an Remote-Netzwerkstandorten:**

    Gehen Sie zum Dashboard zur **Identitätsweitergabe**, legen Sie den Konfigurationsumfang auf **Remote-Netzwerke** fest und wählen Sie **Agent hinzufügen** aus. Wählen Sie zusätzlich zur Angabe der Hostdetails den Datentyp aus, den das Gerät mit Prisma Access teilt. Zu den optionalen Einstellungen gehören der Name und ein Pre-Shared Key für das Gerät.

  - **Über Geräte an Dienstverbindungsstandorten:**

    Gehen Sie zum Dashboard für **Identitätsweitergabe**, legen Sie den Konfigurationsumfang auf **Dienstverbindungen** fest und wählen Sie **Agent hinzufügen** aus. Wählen Sie zusätzlich zur Angabe der Hostdetails den Datentyp aus, den das Gerät mit Prisma Access teilt. Zu den optionalen Einstellungen gehören der Name und ein Pre-Shared Key für das Gerät.

- Konfigurieren Sie den Terminalserver-Agent für die Benutzerzuordnung:

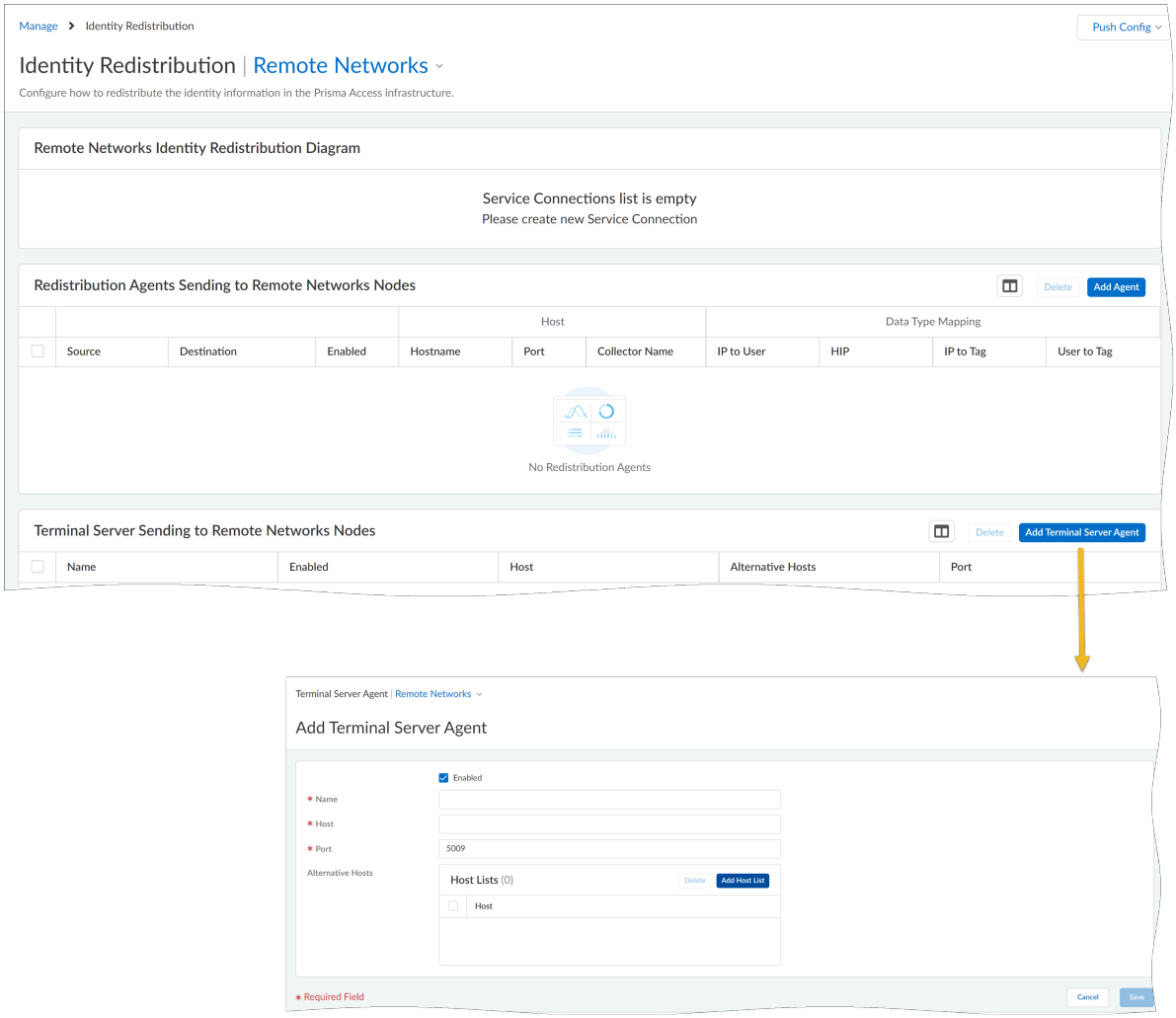
  Der Terminalserver-Agent (oder „TS-Agent“) weist jedem Benutzer einen Portbereich zu, um bestimmte Benutzer auf Windows-basierten Terminalservern zu identifizieren. Der TS-Agent

benachrichtigt Prisma Access über die zugewiesenen Portbereiche, sodass Prisma Access Richtlinien auf der Grundlage von Benutzern und Benutzergruppen durchsetzen kann.

Stellen Sie im Dashboard zur **Identitätsweitergabe** den Konfigurationsumfang auf **Remote-Netzwerke** ein und nutzen Sie **Terminalserver-Agent hinzufügen**, um unter **Terminalserver, die an Remote-Netzwerk-Knoten senden** einen TS-Agent hinzuzufügen.

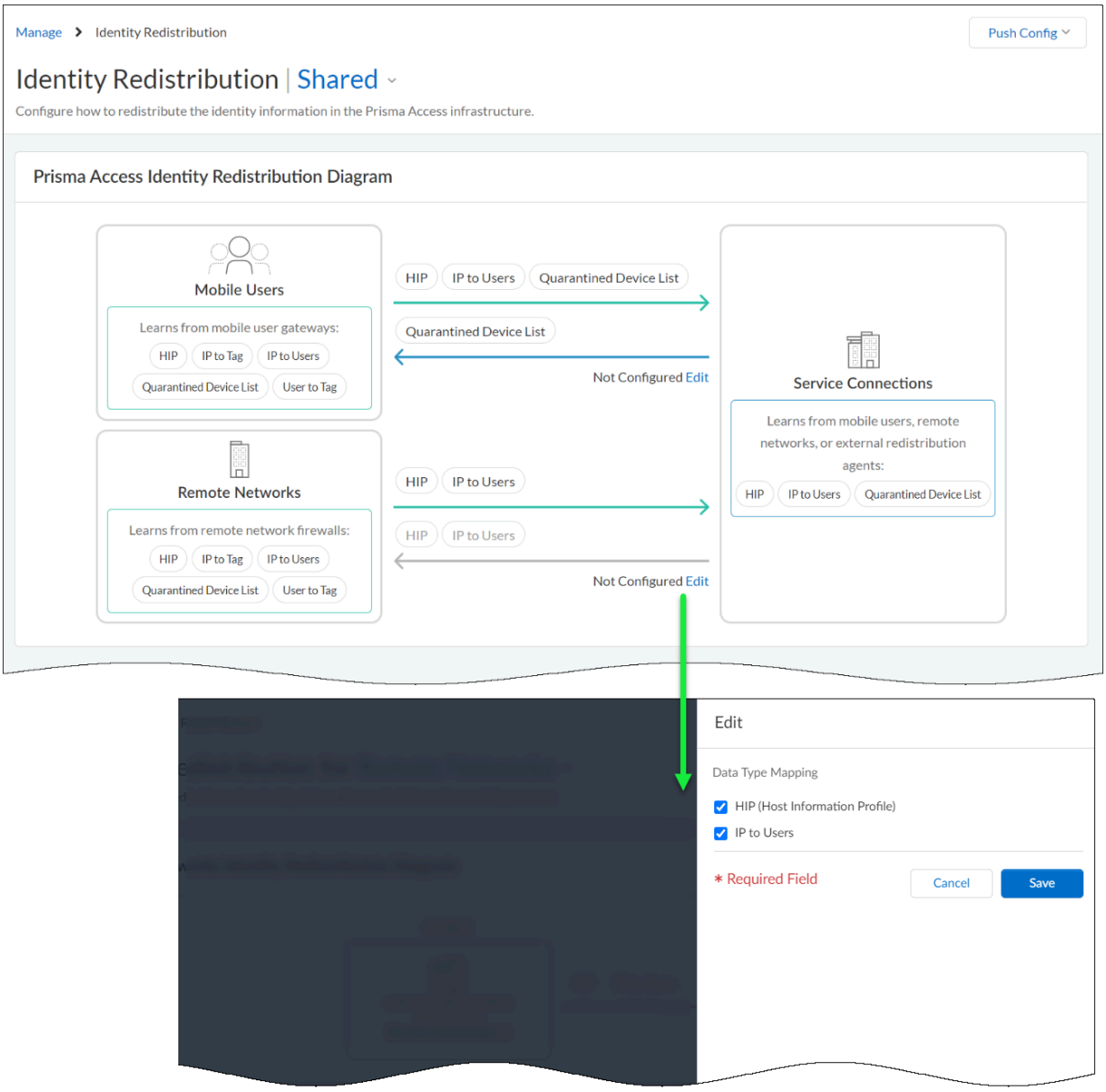
- Die Konfiguration ist standardmäßig **aktiviert**.
- Geben Sie einen **Namen** für den TS-Agent ein.
- Geben Sie die IP des **Windows-Hosts** ein, auf dem der TS-Agent installiert ist.
- Geben Sie die Nummer des **Ports** ein, an dem der Agent auf Benutzerzuordnungsanfragen wartet. Der Port ist standardmäßig auf 5009 festgelegt.
- **Save (Speichern)** Sie Ihre Änderungen.



- Verteilen Sie Identitätsdaten in Ihrer Prisma Access-Umgebung:

  **Bearbeiten** Sie im Dashboard zur **Identitätsweitergabe** das Diagramm, um die Identitätsdaten anzugeben, die Sie aus jeder Quelle sammeln und in Prisma Access teilen möchten.




- Um Ihre Änderungen zu aktivieren, übertragen Sie die Konfiguration an Prisma Access.

## Identitätsweitergabe (NGFW)

Bei einem großen Netzwerk können Sie die Ressourcennutzung optimieren, indem Sie nicht alle Firewalls so konfigurieren, dass die Zuordnungsinformationsquellen direkt abgefragt werden, sondern einige Firewalls so konfigurieren, dass sie die Zuordnungsinformationen über die Weitergabe erfassen. Durch die Weitergabe der Daten ist außerdem eine höhere Präzision möglich, wodurch Sie nur die von Ihnen angegebenen Informationstypen und nur die von Ihnen ausgewählten Geräte weitergeben können. Sie können die IP-Benutzerzuordnungen oder IP-Tag-

Zuordnungen auch mithilfe von Subnetzen und Bereichen filtern, um sicherzustellen, dass die Firewalls nur die Zuordnungen erfassen, die sie zum Durchsetzen der Richtlinienregeln benötigen.

Zur Weitergabe der Daten können Sie die folgenden Architekturtypen verwenden:

- **Hub-and-Spoke-Architektur für eine einzelne Region:**

  Um Daten zwischen Firewalls weiterzugeben, empfiehlt sich die Verwendung einer Hub-and-Spoke-Architektur. In dieser Konfiguration sammelt eine Hub-Firewall die Daten aus Quellen wie Windows User-ID-Agenten, Syslog-Servern, Domänencontrollern oder anderen Firewalls. Konfigurieren Sie die Weitergabe-Client-Firewalls so, dass sie die Daten von der Hub-Firewall erfassen.
- **Multi-Hub-and-Spoke-Architektur für mehrere Regionen:**

  Wenn Sie Firewalls in mehreren Regionen bereitgestellt haben und die Daten an die Firewalls in allen diesen Regionen weitergeben möchten – sodass Sie Richtlinienregeln einheitlich durchsetzen können, unabhängig davon, wo sich der Benutzer anmeldet –, dann können Sie eine Multi-Hub-and-Spoke-Architektur für mehrere Regionen verwenden.
- **Hierarchische Architektur:**

  Zur Weitergabe von Daten können Sie auch eine hierarchische Architektur verwenden. Um beispielsweise Daten wie Benutzer-ID-Informationen weiterzugeben, organisieren Sie die Weitergabesequenz in Ebenen, wobei jede Ebene über eine oder mehrere Firewalls verfügt. Auf der untersten Ebene ordnen PAN-OS-integrierte User-ID-Agents, die auf Firewalls laufen, und Windows-basierte User-ID-Agents, die auf Windows-Servern laufen, IP-Adressen Benutzernamen zu. Jede höhere Ebene verfügt über Firewalls, die die Zuordnungsinformationen und Authentifizierungszeitstempel von bis zu 100 Weitergabepunkten in der darunter liegenden Ebene empfangen. Die Firewalls der obersten Ebene aggregieren die Zuordnungen und Zeitstempel aus allen Ebenen. Diese Bereitstellung bietet die Möglichkeit, separate Richtlinienregeln zu konfigurieren: einerseits Richtlinienregeln für alle Benutzer in Firewalls der obersten Ebene und andererseits regions- oder funktionsspezifische Richtlinienregeln für eine Teilmenge von Benutzern in den entsprechenden Domänen, die von Firewalls der unteren Ebenen bedient werden.

*Wenn Regeln im Datenverkehr nicht wie erwartet durchgesetzt werden, überprüfen Sie mithilfe der* **Fehlerbehebung** *den Datenebenenstatus bestimmter Firewalls, um festzustellen, ob eine Nichtübereinstimmung zwischen den erwarteten Richtlinien (wie konfiguriert) und den durchgesetzten Richtlinien besteht.*

**STEP 1 |** Melden Sie sich bei Strata Cloud Manager an.

**STEP 2 |** Stellen Sie sicher, dass Ihre Strata Cloud Manager-Bereitstellung die Anforderungen zum Konfigurieren der Identitätsweitergabe erfüllt.

1. Konfigurieren und aktivieren Sie die Cloud Identity Engine (CIE) für Ihren Strata Cloud Manager-Mandanten.

   Das ist erforderlich, um die Identitätsweitergabe zu verwenden.

   1. Aktivieren Sie die Cloud Identity Engine.
   2. Richten Sie die Cloud Identity Engine ein.

2. Wählen Sie **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Objekte** > **Adressgruppen** und fügen Sie über **Hinzufügen** eine dynamische Adressgruppe mit den erforderlichen IP-Adress-zu-Tag-Zuordnungen hinzu.

   Wählen Sie für den Adressgruppentyp die Option **Dynamisch** aus. Konfigurieren Sie die dynamische Adressgruppe nach Bedarf und wählen Sie **Speichern**.

3. Wählen Sie **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Objekte** > **Dynamische Benutzergruppen** aus und fügen Sie über **Hinzufügen** eine dynamische Benutzergruppe mit den erforderlichen Benutzernamen-Tag-Zuordnungen hinzu.

   Konfigurieren Sie die dynamische Benutzergruppe nach Bedarf und wählen Sie **Speichern**.

**STEP 3 |** Wählen Sie **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Identitätsdienste** > **Identitätsweitergabe** und wählen Sie den Konfigurationsumfang aus, in dem Sie die Identitätsweitergabe konfigurieren möchten.

Sie können einen Ordner oder eine Firewall aus Ihren **Ordnern** auswählen oder **Snippets** auswählen, um die Identitätsweitergabe in einem Snippet zu konfigurieren.

**STEP 4 |** **Fügen Sie Agents hinzu**.

**STEP 5 |** Geben Sie einen aussagekräftigen **Namen** für den Agent ein.

**STEP 6 |** Geben Sie die **Host**-IP-Adresse ein.

**STEP 7 |** Geben Sie den **Port** ein (Bereich ist 1–65535).

**STEP 8 |** Wählen Sie die **Datentypzuordnung** aus.

- **IP zu Benutzer** – Zuordnung von IP-Adresse zu Benutzername für die Benutzer-ID.
- **Host Information Profile (HIP)** – IP-Adress-Tag-Zuordnungen für dynamische Adressgruppen.
- **IP zu Tag** – Benutzername-zu-Tag-Zuordnungen für dynamische Benutzergruppen.
- **Benutzer zu Tag** – HIP-Daten von GlobalProtect, die HIP-Objekte und -Profile enthalten.
- **Liste der Quarantäne-Geräte** – Geräte, die GlobalProtect als „unter Quarantäne gestellt“ identifiziert.

**STEP 9 |** Klicken Sie auf **Speichern**.

**STEP 10 |** (Nur NGFW Cloud Management) Aktivieren Sie die Identitätsweitergabe für Firewalls.

1. Wählen Sie **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Geräteeinstellungen** > **Geräteeinrichtung** > **Verwaltung** und wählen Sie **Anpassen** aus, um eine Serviceroute für den **UID-Agent**-Dienst zu konfigurieren.

   Wählen Sie den Konfigurationsumfang aus, in dem Sie die Serviceroute erstellen möchten. Sie können einen Ordner oder eine Firewall aus Ihren **Ordnern** auswählen oder **Snippets** auswählen, um die Serviceroute in einem Snippet zu konfigurieren.
2. Aktivieren Sie die Firewall, damit sie reagiert, wenn andere Firewalls Daten zur Weitergabe von ihr anfordern.

   1. Wählen Sie **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Geräteeinstellungen** > **Geräteeinrichtung** > **Verwaltung** aus und aktivieren Sie den **User-ID**-Netzwerkdienst.
   2. Wählen Sie **Verwalten** > **„Konfiguration** > **NGFW- und Prisma Access** > **Geräteeinstellungen** > **Schnittstellen** aus, um eine Layer-3-Schnittstelle zu erstellen oder auszuwählen.

      Erweitern Sie die **erweiterten Einstellungen**. Erstellen oder bearbeiten Sie unter **Sonstiges** das Verwaltungsprofil, um **User-ID** zu aktivieren.

   - Auswählen

**STEP 11 |** Wählen Sie Konfiguration übertragen aus.

# Verwalten: Lokale Benutzer und Gruppen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>❑ Prisma Access<br>❑ AIOps for NGFW Premium<br>❑ Strata Cloud Manager Essentials<br>❑ Strata Cloud Manager Pro<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Speichern Sie Authentifizierungsinformationen für Administratoren und Endbenutzer lokal. Sie können Authentifizierungsinformationen von Administratoren und Endbenutzern speichern, die sich mit GlobalProtect oder dem Authentifizierungsportal authentifizieren.

Um die lokale Datenbankauthentifizierung zu konfigurieren, erstellen Sie eine Datenbank, die lokal auf der Firewall ausgeführt wird und Benutzerkonten (Benutzernamen und Passwörter oder gehashte Passwörter) enthält. Sie können eine lokale Benutzerdatenbank für die Firewall konfigurieren, um Administratoren zu authentifizieren, die auf die Firewall-Weboberfläche

zugreifen, und um Endbenutzer zu authentifizieren, die über das Authentifizierungsportal oder GlobalProtect auf Anwendungen zugreifen.

Die lokale Datenbankauthentifizierung kann mit einem Authentifizierungsprofil verknüpft werden, sodass sie für Bereitstellungen geeignet ist, bei denen unterschiedliche Benutzergruppen unterschiedliche Authentifizierungseinstellungen benötigen, z. B. Kerberos Single Sign-on (SSO) oder Multi-Faktor-Authentifizierung (MFA). Für Administratorkonten, die ein Authentifizierungsprofil verwenden, werden Passwortkomplexität und Ablaufeinstellungen nicht angewendet. Diese Authentifizierungsmethode steht Administratoren zur Verfügung, die auf die Firewall zugreifen, und Endbenutzern, die über das Authentifizierungsportal oder GlobalProtect auf Dienste und Anwendungen zugreifen.

Gehen Sie zu **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Identitätsdienste** > **Lokale Benutzer und Gruppen**, um mit der Erfassung von Authentifizierungsdaten zu beginnen.

## Erstellen lokaler Benutzer

**STEP 1 |** Melden Sie sich bei Strata Cloud Manager an.

**STEP 2 |** Wählen Sie **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Identitätsdienste** > **Lokale Benutzer und Gruppen** > **Lokale Benutzer** und wählen Sie den Konfigurationsumfang aus, in dem Sie einen lokalen Benutzer erstellen möchten.

Sie können einen Ordner oder eine Firewall aus Ihren **Ordnern** auswählen oder **Snippets** auswählen, um einen lokalen Benutzer in einem Snippet zu konfigurieren.

**STEP 3 |** Wählen Sie **Lokalen Benutzer hinzufügen** aus.

**STEP 4 |** Geben Sie einen **Namen** für den Benutzer ein.

**STEP 5 |** Stellen Sie sicher, dass der lokale Benutzer **aktiviert** ist.

*Anstatt einen lokalen Benutzer zur Authentifizierung aus der lokalen Firewall-Datenbank zu löschen, können Sie das Häkchen entfernen (deaktivieren), sodass der Benutzer nicht mehr für die Authentifizierung aktiviert ist.*

**STEP 6 |** Geben Sie ein **Passwort** ein und bestätigen Sie es unter **Passwort bestätigen**.

**STEP 7 |** Klicken Sie auf **Speichern**.

**STEP 8 |** Wählen Sie **Konfiguration übertragen**.

## Erstellen lokaler Benutzergruppen

Gruppieren Sie mehrere lokale Benutzer in einer einzigen lokalen Gruppe, um Gruppeninformationen zur lokalen Firewall-Datenbank hinzuzufügen. Sie können eine lokale Benutzergruppe erstellen, um mehrere lokale Benutzer zu verwalten, die dieselben Authentifizierungsanforderungen haben.

**STEP 1 |** Melden Sie sich bei Strata Cloud Manager an.

**STEP 2 |** Wählen Sie **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Identitätsdienste** > **Lokale Benutzer und Gruppen** > **Lokale Benutzergruppen** und wählen Sie den Konfigurationsumfang aus, in dem Sie eine lokale Benutzergruppe erstellen möchten.

Sie können einen Ordner oder eine Firewall aus Ihren **Ordnern** auswählen oder **Snippets** auswählen, um eine lokale Benutzergruppe in einem Snippet zu konfigurieren.

**STEP 3 |** Wählen Sie **Lokale Benutzergruppe hinzufügen** aus.

**STEP 4 |** Geben Sie einen **Namen** für die lokale Benutzergruppe ein.

**STEP 5 |** Fügen Sie die **lokalen Benutzer** hinzu, die Sie im vorherigen Schritt erstellt haben.

**STEP 6 |** Klicken Sie auf **Speichern**.

**STEP 7 |** Wählen Sie **Konfiguration übertragen**.

# Verwalten: Geräteeinstellungen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | ❑ Strata Cloud Manager Essentials<br>❑ AIOps for NGFW Premium oder Strata Cloud Manager Pro<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

In den **Geräteeinstellungen** können Sie die folgenden Einstellungen für Ihre Cloud-verwalteten Firewalls konfigurieren:

| Einstellung | Beschreibung |
|---|---|
| Schnittstellen | Konfigurieren Sie Oberflächen, damit Ihre Firewall in mehreren Bereitstellungen gleichzeitig ausgeführt werden kann.<br>Verwenden Sie auf der Registerkarte **„Ethernet** “ die **Option „Lokale Gerätekonfigurationen anzeigen“,** um die verschiedenen Konfigurationen der lokalen Firewall und des Strata Cloud Managers anzuzeigen. |
| Routing | Konfigurieren Sie Routingprofile, einen logischen Router und eine statische Route für Ihre Firewalls. |
| IPSec-Tunnel | Konfigurieren Sie IPSec-Tunnel, um IP-Pakete beim Durchqueren des Tunnels zu authentifizieren und zu verschlüsseln. |
| DHCP | Konfigurieren Sie DHCP, um TCP/IP- und Link-Layer-Konfigurationsparameter bereitzustellen und dynamisch konfigurierten Hosts in einem TCP/IP-Netzwerk Netzwerkadressen bereitzustellen. |
| Zonen | Konfigurieren Sie Zonen, um Ihr Netzwerk in funktionale und organisatorische Zonen zu segmentieren und so Ihre Angriffsfläche zu reduzieren. |
| DNS-Proxy | Konfigurieren Sie einen DNS-Proxy, um die Firewall so zu konfigurieren, dass sie als Vermittler zwischen DNS-Clients und -Servern fungiert. |

| Einstellung | Beschreibung |
|---|---|
| Geräteeinrichtung | Richten Sie Ihre Geräte ein, um Dienstrouten, Verbindungseinstellungen, zulässige Dienste und Einstellungen für den Administratorzugriff für die Verwaltungs- und Hilfsschnittstellen für Ihre Firewalls zu konfigurieren. |
| Proxy | Konfigurieren Sie einen Webproxy, um Proxy- und Firewall-Funktionen auf einem Gerät zu konsolidieren.<br><br>*Ein Webproxy für Strata Cloud Manager erfordert den Legacy-Router-Stack. Wenn Sie dies aktivieren möchten, wenden Sie sich bitte an Ihr Account-Team.* |
| Virtueller Draht | Konfigurieren Sie einen virtuellen Draht, um eine Firewall-Schnittstelle in eine Topologie zu integrieren, sodass die beiden verbundenen Schnittstellen auf der Firewall weder Switching noch Routing durchführen müssen. |
| GlobalProtect | Aktivieren Sie Ihre Cloud-verwalteten NGFWs als GlobalProtect-Gateways und -Portale, um Benutzern überall flexiblen, sicheren Remote-Zugriff zu ermöglichen. |

# Verwalten: Global Settings (Globale Einstellungen)

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama or Strata Cloud Manager) | Eine der folgenden Komponenten:<br>☐ Prisma Access-Lizenz<br>☐ Strata Cloud Manager Pro<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Überprüfen und konfigurieren Sie die globalen Einstellungen in Strata Cloud Manager **(Verwalten > Konfiguration > NGFW und Prisma Access > Globale Einstellungen)**

| Objekt | Beschreibung |
|---|---|
| SaaS-App-Verwaltung | Verwalten Sie Ihre SaaS-Anwendungen zentral. Die SaaS-App-Verwaltung bietet Funktionen, mit denen Sie Apps sicher für Ihr Unternehmen aktivieren können. |
| Vorlage für Benutzer-Coaching-Benachrichtigungen | Verwalten Sie zentral die Benachrichtigungsvorlagen für Endbenutzer, um Benutzer über AI-Powered ADEM zu benachrichtigen, wenn der Benutzer einen Enterprise Data Loss Prevention (E-DLP)-Vorfall erzeugt, bei dem Datenverkehr mit vertraulichen Daten überprüft und blockiert wird. |
| Auto-VPN | Die manuelle Konfiguration von Netzwerkgeräten und Einrichtung von VPN-Tunneln ist ein langwieriger Prozess und anfällig für Fehlkonfigurationen. Auto-VPN erstellt automatisch den VPN-Tunnel zwischen den Netzwerkgeräten. Mit Auto-VPN können Sie einen VPN-Cluster erstellen, um mehrere Local Area Networks (LANs) zu verbinden. SD-WAN mit Auto-VPN erleichtert die Bereitstellung und Verwaltung der SD-WAN-Bereitstellungen. |

# Vorlage für Benutzer-Coaching-Benachrichtigungen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ GlobalProtect app Version 6.3 oder höher<br>❑ Enterprise Data Loss Prevention (E-DLP)-Lizenz<br>❑ Prisma Access-Mobile-Benutzer-Lizenz<br>❑ Prisma Access-Lizenz<br>Oder eine der folgenden Lizenzen, die die Enterprise DLP-Lizenz enthalten:<br>❑ Prisma Access-CASB-Lizenz<br>❑ Next-Generation CASB for Prisma Access and NGFW (CASB-X)-Lizenz |

Mit der Vorlage für Benutzer-Coaching-Benachrichtigungen können Sie die Benachrichtigung konfigurieren, die Ihren Benutzern in der Access Experience-Benutzeroberfläche angezeigt wird, wenn sie einen Enterprise Data Loss Prevention (E-DLP)-Vorfall generieren. Ein Enterprise DLP-Vorfall wird generiert, wenn eine Datei mit sensiblen Daten heruntergeladen oder hochgeladen wird oder wenn nicht dateibasierter Datenverkehr mit sensiblen Daten an ein Webformular gesendet wird.

Um zu ermitteln, was als sensible Daten gilt, fügen Sie eine oder mehrere **Inline-DLP-Regeln** hinzu. DLP-Regeln enthalten Kriterien für den Verkehrsabgleich, die definieren, was als sensible Daten gilt. Die DLP-Regel wird aus dem gleichnamigen Enterprise DLP-Datenprofil abgeleitet. Darüber hinaus können Sie benutzerdefinierte Nachrichten konfigurieren, wenn ein **dateibasierter** oder **nicht dateibasierter** Enterprise DLP-Vorfall generiert wird. Nachdem ein Enterprise DLP-Vorfall erzeugt wurde, kann der Benutzer, der den Vorfall generiert hat, die Datensicherheitsbenachrichtigung anzeigen, um weitere Informationen über die sensiblen Daten zu erhalten, die hochgeladen, heruntergeladen oder veröffentlicht wurden.

Es wird nur eine Benachrichtigung pro Vorfall in einem Zeitraum von 30 Sekunden angezeigt, unabhängig davon, wie oft der Benutzer den gleichen Vorfall generiert. Hierzu ein Beispiel: Ein Benutzer versucht, eine Datei mit sensiblen Daten in die Box-Webanwendung hochzuladen, und Enterprise Data Loss Prevention (E-DLP) blockiert den Upload. Der Benutzer versucht dann sofort, dieselbe Datei fünf weitere Male hochzuladen, wird aber jedes Mal blockiert. In diesem Fall wird nur eine Access Experience-Benachrichtigung generiert, obwohl der Benutzer insgesamt sechsmal daran gehindert wurde, eine Datei mit sensiblen Daten in die Box-Webanwendung hochzuladen.

**STEP 1 |** Wenden Sie sich an Ihren Palo Alto Networks-Ansprechpartner, um Endbenutzer-Coaching für Ihren Mandanten zu aktivieren.

**STEP 2 |** Installieren Sie GlobalProtect app Version 6.3 oder höher unter Windows oder macOS.

**STEP 3 |** Melden Sie sich bei Strata Cloud Manager an.

**STEP 4 |** Aktivieren Sie Autonomous DEM.

Öffnen Sie Strata Cloud Manager und wählen Sie **Workflows** > **Einrichtung Prisma Access** > **GlobalProtect** > **GlobalProtect-App** und dann **App-Einstellungen hinzufügen** aus. Sie müssen diese erforderlichen Einstellungen so konfigurieren, dass Ihren Benutzern Benachrichtigungen in der Access Experience-Benutzeroberfläche angezeigt werden, wenn diese einen DLP-Vorfall generieren.

- Aktivieren Sie die **Autonomous DEM- und GlobalProtect-Protokollerfassung für die Fehlersuche**.
- **DEM für Prisma Access (nur Windows und Mac)** – Wählen Sie **„Installieren“ und „Benutzer kann DEM nicht aktivieren oder deaktivieren“** aus.
- **DEM für Prisma Access ab Version 6.3 (nur Windows und Mac)** – Wählen Sie **Agent installieren** aus.

**STEP 5 |** (Nur MacOS) Wählen Sie in der Access Experience-Benutzeroberfläche **Einstellungen** > **Benachrichtigungen** aus und aktivieren Sie **Benachrichtigungen zulassen**.

Diese Einstellung muss in der Access Experience-Benutzeroberfläche für jeden Benutzer aktiviert sein und ist erforderlich, um Benachrichtigungen auf dem Desktop des Benutzers anzuzeigen. Konfigurieren Sie den Rest der Access Experience-Benachrichtigungseinstellungen nach Bedarf.

**STEP 6 |** Konfigurieren Sie Enterprise DLP.

1. Erstellen Sie ein Entschlüsselungsprofil und eine Richtlinienregel.

   Diese werden benötigt, damit Enterprise DLP den Datenverkehr entschlüsseln und auf sensible Daten prüfen kann.
2. Erstellen Sie benutzerdefinierte Datenmuster, um Ihre Übereinstimmungskriterien zu definieren.

   Alternativ können Sie die vordefinierten Datenmuster verwenden, anstatt benutzerdefinierte Datenmuster zu erstellen.
3. Erstellen Sie ein Datenprofil und fügen Sie Ihre Datenmuster hinzu.

   Es werden nur benutzerdefinierte Datenprofile unterstützt. Standardmäßig sind alle vordefinierten **Aktionen** der DLP-Regeln auf **Benachrichtigen** gesetzt. Sofern erforderlich, klonen Sie das vordefinierte Datenprofil, um die DLP-Regel-**Aktion** zu bearbeiten.
4. Ändern Sie die DLP-Regel.

   - Wenn Sie die DLP-Regel ändern, müssen Sie die **Aktion** auf **Blockieren** setzen. Das ist erforderlich, um Benachrichtigungen in der Access Experience-Benutzeroberfläche zu generieren. Es werden keine Benachrichtigungen angezeigt, wenn die **Aktion** auf **Benachrichtigen** eingestellt ist.
   - Fügen Sie die DLP-Regel einer Profilgruppe hinzu und fügen Sie die Profilgruppe einer Sicherheitsrichtlinienregel hinzu. Das ist erforderlich, damit Enterprise DLP einen DLP-Vorfall generiert, der dann eine Benachrichtigung in der Access Experience-Benutzeroberfläche erzeugt.

**STEP 7 |** Wählen Sie **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Globale Einstellungen** > **Vorlage für Benutzer-Coaching-Benachrichtigungen** und dann **Benachrichtigungsvorlage hinzufügen** aus.

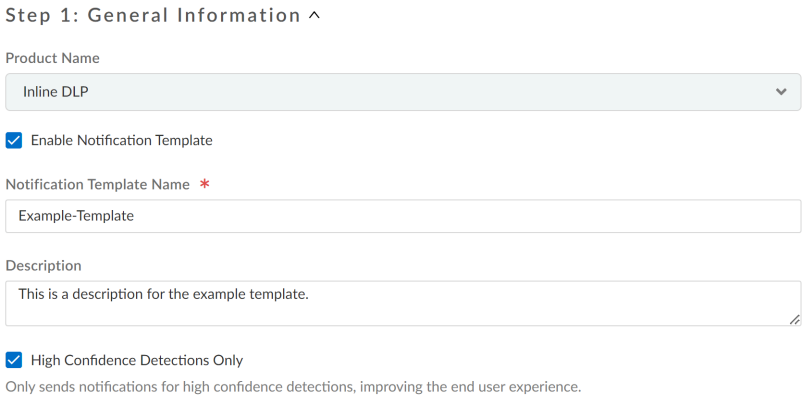
**STEP 8 |** Konfigurieren Sie die **allgemeinen Informationen**.

1. Stellen Sie sicher, dass **Inline-DLP** als **Produktname** festgelegt ist.

   Dies ist die Standardeinstellung und kann nicht geändert werden.
2. Wählen Sie **Benachrichtigungsvorlage aktivieren**, um die Vorlage nach dem Speichern zu aktivieren.

   Diese Einstellung ist standardmäßig aktiviert.
3. Geben Sie einen aussagekräftigen **Namen der Benachrichtigungsvorlage** ein.
4. (Optional) Geben Sie eine **Beschreibung** für die Benachrichtigungsvorlage ein.
5. (Optional) Wählen Sie **Nur Erkennungen mit hoher Zuverlässigkeit** aus, um nur Access Experience-Benachrichtigungen für Verkehrsübereinstimmungen mit hoher Zuverlässigkeit zu generieren.

   Übereinstimmungen mit hoher Konfidenz spiegeln wider, wie sicher sich Enterprise DLP bei der Erkennung des übereinstimmenden Verkehrs ist. Bei Regex-Mustern (Regular Expression, regulärer Ausdruck) basiert dies auf dem Zeichenabstand zu den konfigurierten Näherungsschlüsselwörtern. Für ML-Muster (Maschinellen Lernen) wird dieses Konfidenzniveau durch die ML-Modelle berechnet.



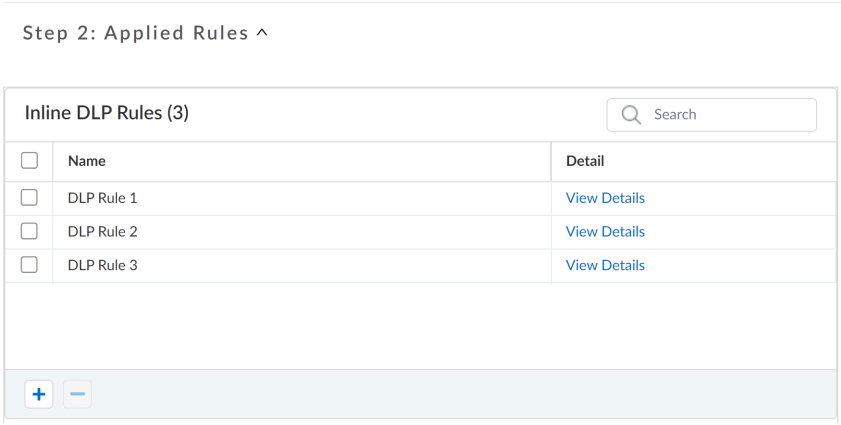

**STEP 9 |** Fügen Sie der Benachrichtigungsvorlage eine oder mehrere **angewandte Regeln** hinzu.

Bei DLP-Regeln muss die Regel **Aktion** auf **Blockieren** gesetzt sein und einer Profilgruppe hinzugefügt werden, die an eine Sicherheitsrichtlinienregel angehängt ist, um eine Access Experience-Benachrichtigung zu generieren. Fügen Sie nur DLP-Regeln hinzu, die einer Profilgruppe hinzugefügt wurden, die einer Sicherheitsrichtlinienregel zugeordnet ist. Das ist erforderlich, damit Enterprise DLP einen DLP-Vorfall generiert, der dann eine Benachrichtigung in der Access Experience-Benutzeroberfläche erzeugt. Eine einzelne DLP-

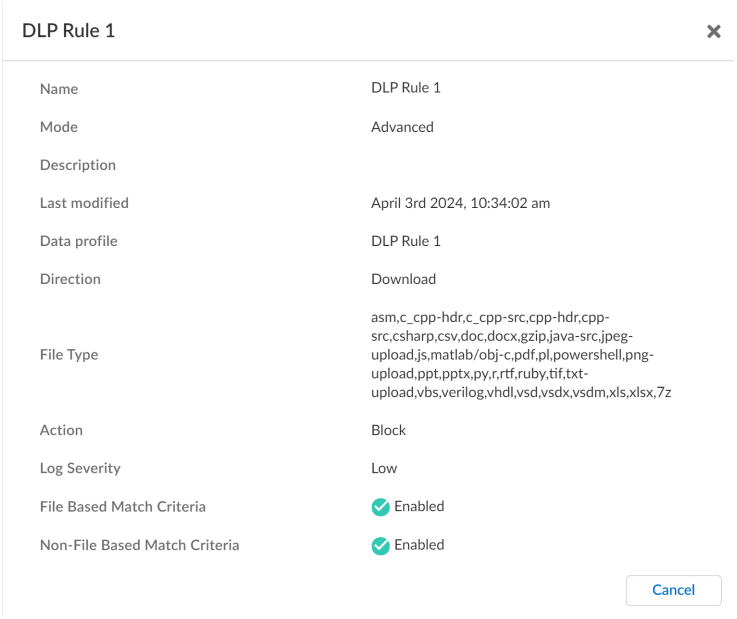
 

Regel kann zu mehreren Vorlagen für Benutzer-Coaching-Benachrichtigungen hinzugefügt werden.

Alle DLP-Regeln, die der Benachrichtigungsvorlage hinzugefügt werden, erzeugen die gleiche **Benachrichtigungsmeldung**, wenn Enterprise DLP sensible Daten blockiert, die mit den Datenprofilen übereinstimmen, die der DLP-Regel zugeordnet sind.




Sie können für jede DLP-Regel, die Sie hinzufügen, **Details anzeigen**, um die spezifischen Inspektionsdetails zu überprüfen. Dazu gehören die **Richtung** der Datenverkehrsuntersuchung, der anwendbare **Dateityp**, die **Aktion** sowie Informationen dazu, ob die DLP-Regel **dateibasierte Übereinstimmungskriterien**, **nicht dateibasierte Übereinstimmungskriterien** oder beides überprüft.



**STEP 10 |** Definieren Sie die **Benachrichtigungsmeldung**, die Benutzer erhalten, wenn Enterprise DLP sensible Daten blockiert, die den Datenprofilen entsprechen, die der DLP-Regel zugeordnet sind.

Die Meldungsvorlagen sind die Access Experience-Toast-Benachrichtigungen, die Benutzer erhalten, wenn Enterprise DLP sensible Daten blockiert. Sie können die folgenden Variablen in Ihren Meldungsvorlagen verwenden. Sie müssen die Klammern für jede Variable angeben.

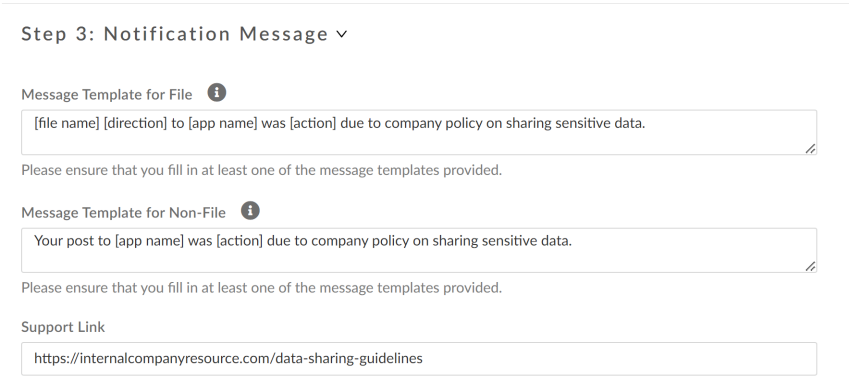
- **`[Dateiname]`** – Dateiname und -erweiterung mit sensiblen Daten, die durch Enterprise DLP blockiert werden.
- (Nur dateibasiert) **`[Richtung]`** – gibt an, ob Enterprise DLP einen Dateiupload oder -download blockiert hat.
- **`[App-Name]`** – Anwendung, über die der Benutzer versucht hat, nicht dateibasierte Inhalte hochzuladen, herunterzuladen oder zu veröffentlichen.
- **`[Aktion]`** – Aktion, die Enterprise DLP ergriffen hat, wenn sensible Daten erkannt wurden. Dieser Wert lautet immer `Blockiert`.

1. Definieren Sie die **Nachrichtenvorlage für Datei**-basierte Erkennungen.

   Überspringen Sie diesen Schritt, wenn die DLP-Regel nicht für dateibasierte Erkennungen konfiguriert ist.
2. Definieren Sie die **Nachrichtenvorlage für nicht dateibasierte** Erkennungen.

   Überspringen Sie diesen Schritt, wenn die DLP-Regel nicht für nicht dateibasierte Erkennungen konfiguriert ist.
3. Fügen Sie einen **Unterstützungslink** hinzu.

   Sie können Links, die Ihre Unternehmensrichtlinie für das Teilen oder Herunterladen sensibler Daten beschreiben, direkt in die Access Experience-Toast-Benachrichtigung einfügen.




**STEP 11 |** Klicken Sie auf **Speichern**.

**STEP 12 |** Der Benutzer, der den Enterprise DLP-Vorfall generiert hat, kann die Datensicherheitsbenachrichtigung anzeigen, um ein Snippet der sensiblen Daten anzuzeigen, die hochgeladen, heruntergeladen oder veröffentlicht wurden.

# Verwalten: Vorgänge

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • NGFW (Managed by Panorama or Strata Cloud Manager)<br>  • Einschließlich VM-Series | ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

**Fehlerbehebung**

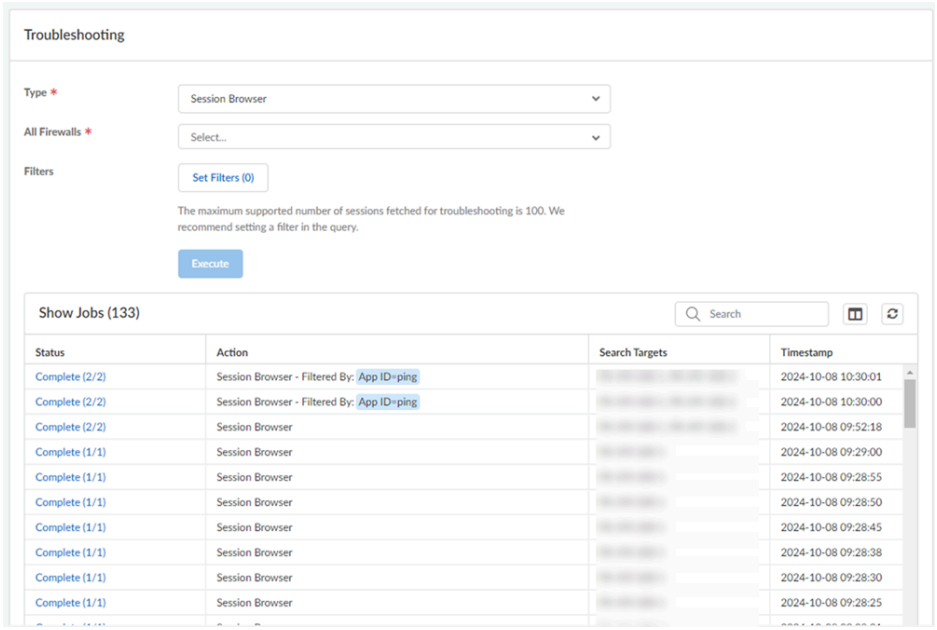
Beheben Sie Probleme Ihrer NGFWs vom Strata Cloud Manager aus, ohne zwischen verschiedenen Firewall-Schnittstellen wechseln zu müssen.

*Weitere Informationen zur Problembehandlung finden Sie hier.*

Das Dashboard zur Fehlerbehebung ermöglicht es Ihnen, Netzwerk-, Identitäts- und Richtlinienprobleme für Ihre über Strata Cloud Manager verwalteten NGFWs zu beheben. Mithilfe des Dashboards zur Fehlerbehebung können Sie Anomalien und problematische Konfigurationen in den folgenden Bereichen lokalisieren:

- ❑ DNS-Proxy
- ❑ NAT
- ❑ Benutzergruppen
- ❑ Dynamische Adressgruppen
- ❑ Dynamische Benutzergruppen
- ❑ Benutzer-ID
- ❑ Sitzungsbrowser

Gehen Sie zu **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Vorgänge** > **Fehlerbehebung** > **Sitzungsbrowser**, um zu beginnen.



# Verwalten: Empfehlung für IoT-Richtlinien

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)*<br>• NGFWs<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)* | ❑ Mindestens eine dieser Lizenzen ist erforderlich, um Ihre Konfiguration mit Strata Cloud Manager zu verwalten; für die einheitliche Verwaltung von NGFWs und Prisma Access benötigen Sie Folgendes:<br>❑ Prisma Access-Lizenz<br>❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>❑ Strata Cloud Manager Essentials<br>❑ Strata Cloud Manager Pro<br>❑ IoT Security-Abonnement für ein erweitertes IoT-Sicherheitsprodukt (Enterprise IoT Security Plus, Industrial IoT Security oder Medical IoT Security) |

IoT Security stellt Strata Cloud Manager automatisch generierte Empfehlungen für Sicherheitsrichtlinienregeln bereit, organisiert nach Geräteprofil. Pro Anwendung und Profil gibt es eine Empfehlung. Wählen Sie ein Profil aus, wählen Sie die Regelempfehlungen aus, die Sie verwenden wollen, und dann die NGFWs oder Prisma Access-Bereitstellungstypen, in denen Sie sie durchsetzen wollen.

# Erste Schritte

Wählen Sie Empfehlungen für Sicherheitsrichtlinienregeln aus und wenden Sie sie auf NGFWs oder Prisma Access an.

**STEP 1 |** Erstellen Sie Ordner oder Snippets für NGFWs.

*Überspringen Sie diesen Schritt, wenn Sie vordefinierte Ordner oder zuvor erstellte Ordner oder Snippets verwenden möchten. Prisma Access-Ordner sind vordefiniert.*

Ordner sind im Wesentlichen Container, die verschiedene Arten von Regeln, Sicherheitskonfigurationen und Objekten enthalten. Beim Importieren der Richtlinienregelempfehlungen, die IoT SecurityIoT Security generiert, enthalten die Ordner NGFWs oder Prisma Access-Bereitstellungen.

Snippets sind ebenfalls eine Art Container, der mehreren Ordnern zugeordnet werden kann. Mit Ordnern und Snippets können Sie Richtlinienregeln in beliebige Firewall-Gruppen oder Bereitstellungen importieren.

Sie können beispielsweise einen Ordner mit dem Namen „Kalifornien“ erstellen und dort 60 Firewalls ablegen und anschließend einen weiteren Ordner mit dem Namen „Hawaii“ erstellen und dort 15 Firewalls ablegen. Anschließend erstellen Sie ein Snippet namens „CA-HI“ und wenden es auf die Ordner „Kalifornien“ und „Hawaii“ an. Wenn Sie Regelempfehlungen nur in Firewalls in Kalifornien importieren möchten, legen Sie den Umfang als **Ordner** fest und wählen Sie den Ordner „Kalifornien“ aus. Wenn Sie die Regelempfehlungen sowohl in Kalifornien als auch in Hawaii importieren möchten, legen Sie den Umfang als **Snippet** fest und wählen Sie das Snippet „CA-HI“ aus.

Abhängig von der Hierarchie der Ordnerstruktur gibt es möglicherweise noch einen übergeordneten Ordner wie „US-West“ oberhalb von „Kalifornien“ und „Hawaii“. Wenn Sie dann Regelempfehlungen importieren, während der Umfang auf **Ordner** festgelegt und **US-West** ausgewählt ist, erben beide untergeordneten Ordner „Kalifornien“ und „Hawaii“ die importierten Regeln. Dies würde jedoch nicht funktionieren, wenn Sie nur Regeln für Kalifornien und Hawaii importieren möchten, diese jedoch über gleichgestellte Ordner wie „Oregon“, „Alaska“, „Washington“ und „Arizona“ unter dem Ordner „US-West“ verfügen. In diesem Fall müssten Sie das Snippet „CA-HI“ verwenden.

**STEP 2 |** Erstellen Sie Sicherheitsrichtlinienregeln.

1. Wählen Sie **Verwalten** > **Konfiguration** > **Empfehlung für IoT-Richtlinien** aus.
2. Wählen Sie einen Profilnamen.

   IoT Security verwendet maschinelles Lernen, um automatisch Empfehlungen für Sicherheitsrichtlinienregeln zu generieren – basierend auf dem normalen, akzeptablen Netzwerkverhalten von IoT-Geräten im selben Geräteprofil. Strata Cloud Manager zeigt

eine nach Anwendung geordnete Liste dieser Empfehlungen an. Für jedes Verhalten können Sie Folgendes sehen:

| Verhaltenskomponente | Erklärung |
|---|---|
| App-Risiko | Dies ist die Risikostufe einer Anwendung, die durch verschiedene Faktoren auf einer steigenden Risikoskala von 1 bis 5 bestimmt wird. |
| Sicherheitsrichtlinie erstellt | Wenn hier ein oder mehrere Namen von Ordnern oder Snippets angezeigt werden, weist dies darauf hin, dass zuvor eine Sicherheitsrichtlinienregel für dieses Verhalten erstellt wurde. Wenn Sie auf einen dieser Namen klicken, wird eine Seitenleiste mit dem Namen des Profils, der Anwendung und des Ordners bzw. Snippets sowie mit der Richtlinienregelaktion geöffnet. Wenn hier **Nein** angezeigt wird, bedeutet das, dass noch keine Regel erstellt wurde. |
| Standort erkannt | **Intern** bedeutet, dass sich das Ziel im lokalen Netzwerk befindet. **Extern** bedeutet, dass das Ziel außerhalb des lokalen Netzwerks liegt. |
| Lokal beobachtet | **Ja** bedeutet, dass das Verhalten in Ihrer IoT Security-Mandantenumgebung beobachtet wurde. **Nein** bedeutet, dass es in mehreren IoT Security-Mandantenumgebungen beobachtet wurde, aber nicht in Ihrer. |
| App-Nutzung | **Allgemein** bedeutet, dass eine Anwendung in mehreren IoT Security-Mandantenumgebungen erkannt wurde. **Eindeutig** bedeutet, dass es in Ihrer Umgebung beobachtet wurde, aber nicht in denen anderer Mandanten, die ebenfalls Geräte im selben Profil aufweisen. |
| Zieladresse und FQDN | Dies ist das Ziel für eine empfohlene Richtlinienregel. Es kann sich um „Beliebige“, eine IP-Adresse oder einen FQDN handeln. |
| Zielprofil | Ein Profil wird angezeigt, wenn das Ziel intern ist und das Geräteprofil des Ziels identifiziert wurde. |

| Verhaltenskomponente | Erklärung |
|---|---|
| Zuletzt gesehen | Bei lokal beobachtetem Verhalten ist dies der Zeitstempel der letzten Beobachtung. Bei häufigem, nicht lokal beobachtetem Verhalten wird ein Bindestrich angezeigt. |

3. Wählen Sie eine oder mehrere Verhaltensweisen aus und klicken Sie dann auf **Sicherheitsrichtlinie erstellen**.
4. Überprüfen Sie die Sicherheitsrichtlinienregeln, die erstellt werden, und wählen Sie dann den Konfigurationsumfang aus, in dem Strata Cloud Manager sie anwenden wird.

   So wenden Sie die Regeln auf eine oder mehrere NGFWs oder Prisma Access-Bereitstellungen in einem Ordner an: Wählen Sie **Ordner** und dann den Ordner aus der Umfangsauswahl aus.

   So wenden Sie die Regeln auf eine oder mehrere NGFWs oder Prisma Access-Bereitstellungen in einem Snippet an: Wählen Sie **Snippet** und dann das Snippet aus der Umfangsauswahl aus.
5. Wählen Sie **Sicherheitsrichtlinie erstellen** aus.

**STEP 3 |** Übertragen Sie die Konfiguration an NGFWs und Prisma Access-Bereitstellungen.

1. Wählen Sie **Verwalten** > **Vorgänge** > **Konfiguration übertragen** aus.
2. Wählen Sie die Ordner mit den Konfigurationsänderungen aus und wählen Sie **Konfiguration übertragen**, **Übertragen** und dann erneut **Übertragen** aus.

   Strata Cloud Manager zeigt in der Spalte „Job-ID“ eine ID-Nummer für die ausgewählten Ordner und in der Spalte „Push-Status“ den Status des Konfigurationsübertragung an.

   Wenn sich der Push-Status von **Ausstehend** zu **Erfolgreich** ändert, wissen Sie, dass die Ausführung der übertragenen Konfiguration gestartet wurde.
3. Um den Status eines Übertragungsjobs anzuzeigen, wählen Sie **Verwalten** > **Vorgänge** > **Push-Status** aus. Hier können Sie den Status des übergeordneten Jobs und auch den Status der untergeordneten Jobs sehen – einen für jede Firewall oder Bereitstellung.

# Verwalten: Enterprise DLP

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)*<br>• NGFWs<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)* | • Enterprise Data Loss Prevention (E-DLP)-Lizenz<br>• **NGFW (Managed by Panorama)** – Support- und Panorama-Geräteverwaltungslizenzen<br>• **Prisma Access (Managed by Strata Cloud Manager)** – Prisma Access-Lizenz<br>• **SaaS Security** – SaaS Security-Lizenz<br>• **NGFW (Managed by Strata Cloud Manager)** – Support- und AIOps for NGFW Premium-Lizenzen<br>Oder eine der folgenden Lizenzen, die die Enterprise DLP-Lizenz enthalten:<br>• Prisma Access-CASB-Lizenz<br>• Next-Generation CASB for Prisma Access and NGFW (CASB-X)-Lizenz<br>• Data Security-Lizenz |

Enterprise Data Loss Prevention (E-DLP) schützt sensible Daten vor unbefugtem Zugriff, Missbrauch, Diebstahl oder Weitergabe. Mit Enterprise DLP in Strata Cloud Manager können Sie die Datensicherheitsstandards Ihres Unternehmens durchsetzen und den Verlust sensibler Daten durch NGFWs sowie durch mobile Prisma Access-Benutzer oder Prisma-Remote-Netzwerke verhindern.

# Funktionshighlights

- **Das Enterprise Data Loss Prevention (E-DLP) Dashboard**

  Gehen Sie zu **Verwalten** > **Konfiguration** > **Data Loss Prevention**, um Enterprise DLP zu konfigurieren und zu verwalten.

  Ihre Enterprise DLP-Konfiguration wird an die Produkte weitergegeben, in denen Sie Enterprise DLP verwenden. So werden hier möglicherweise Einstellungen angezeigt, die an anderer Stelle konfiguriert wurden, und einige Einstellungen, die Sie hier konfigurieren können, können auch in anderen Produkten genutzt werden.

- **Vordefinierte und benutzerdefinierte Enterprise DLP-Einstellungen**

  Enterprise DLP enthält integrierte Einstellungen, mit denen Sie Ihre sensiblen Inhalte schnell schützen können:

  - Vordefinierte reguläre Ausdrücke und ML-basierte Datenmuster definieren häufige Arten sensibler Informationen (wie Kreditkarten und Sozialversicherungsnummern), die Sie möglicherweise erkennen und schützen möchten.
  - Vordefinierte Datenprofile gruppieren Datenmuster, die häufig dieselbe Art der Durchsetzung erfordern.

  Sie können auch benutzerdefinierte Datenmuster und Profile direkt in Strata Cloud Manager erstellen.

- **Untersuchung auf DLP-Vorfälle**

  Ein DLP-Vorfall wird generiert, wenn der Datenverkehr mit einem DLP-Datenprofil übereinstimmt, das mit einer Sicherheitsrichtlinienregel in Strata Cloud Manager verknüpft ist. Im Dashboard „DLP-Vorfälle“ können Sie Details für den Datenverkehr anzeigen, der den Vorfall ausgelöst hat, z. B. abgeglichene Datenmuster, Quelle und Ziel des Datenverkehrs sowie Datei und Dateityp.

- **Scannen nach Bildern in unterstützten Dateiformaten**

  Stärken Sie Ihre Sicherheit, indem Sie mit Optischer Zeichenerkennung (Optical Character Recognition, OCR) versehentlichen Datenmissbrauch, -verlust oder -diebstahl verhindern. OCR ermöglicht es dem DLP Cloud-Dienst, unterstützte Dateitypen mit Bildern zu scannen, die sensible Informationen enthalten, die Ihren Enterprise DLP-Filterprofilen entsprechen.

- **Exakter Datenabgleich (Exact Data Match, EDM)**

  EDM ist ein fortschrittliches Erkennungstool zur Überwachung und zum Schutz sensibler Daten vor Exfiltration. Verwenden Sie EDM, um mit hoher Genauigkeit sensible und personenbezogene Daten wie Sozialversicherungsnummern, Krankenaktennummern, Bankkontonummern und Kreditkartennummern in strukturierten Datenquellen wie Datenbanken, Verzeichnisservern oder strukturierten Datendateien (CSV und TSV) zu erkennen.

- **Benutzerdefinierte Dokumenttypen**

  Laden Sie Ihre benutzerdefinierten Dokumente mit geistigem Eigentum oder sensiblen Informationen in Enterprise Data Loss Prevention (E-DLP) hoch, um benutzerdefinierte Dokumenttypen zu erstellen. Ihre benutzerdefinierten Dokumenttypen werden als

Übereinstimmungskriterien im erweiterten Datenprofil verwendet, um Exfiltrationen zu erkennen und zu verhindern.

- **Email DLP**

  Email DLP verhindert die Exfiltration von E-Mails mit sensiblen Informationen durch KI-/ML-gestützte Datenerkennung. Enterprise DLP kann beispielsweise verhindern, dass sensible Daten über eine ausgehende E-Mail exfiltriert werden, die von einem Verkäufer innerhalb Ihres Unternehmens an seine persönliche E-Mail gesendet wird.

- **Rollenbasierter Zugriff für Enterprise DLP**

  Sie können den rollenbasierten Zugriff auf Enterprise DLP-Steuerungen in Strata Cloud Manager aktivieren. So können Sie steuern, welche Benutzer Lese- und Schreibzugriff auf verschiedene Teile von Enterprise DLP haben.

# Erste Schritte

**STEP 1 |** Aktivieren Sie Enterprise DLP in Strata Cloud Manager.

Um Enterprise DLP einzurichten, müssen Sie ein Entschlüsselungsprofil erstellen, damit der DLP-Clouddienst den Datenverkehr überprüfen kann. Wählen Sie **Verwalten** > **Konfiguration** > **Sicherheitsdienste** > **Entschlüsselung** und gehen Sie dann wie folgt vor:

1. Wählen Sie **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Sicherheitsdienste** > **Entschlüsselung** aus und dann **Regel hinzufügen** aus.

   Die vordefinierten Entschlüsselungsprofil-Einstellungen ermöglichen es Enterprise DLP, den Datenverkehr zu prüfen. Das Ändern der vordefinierten Entschlüsselungsprofil-Einstellungen ist nicht erforderlich, es sei denn, Sie müssen **ALPN entfernen** aktivieren (**Erweiterte Einstellungen** > **SSL-Forward-Proxy**).
2. Fügen Sie das Entschlüsselungsprofil einer **SSL-Forward-Proxy**-Entschlüsselungsregel hinzu.

- So aktivieren Sie Enterprise DLP

**STEP 2 |** (Optional) Wählen Sie **Verwalten** > **Konfiguration** > **Data Loss Prevention** > **Methoden** aus und erstellen Sie ein Datenmuster.

Sie können benutzerdefinierte Enterprise DLP-Datenmuster erstellen, um festzulegen, welche Inhalte vertraulich sind und geschützt werden müssen – dies ist der Inhalt, den Sie filtern. Sie können ein benutzerdefiniertes Datenmuster basierend auf regulären Ausdrücken oder ein Datenmuster basierend auf Dateieigenschaften erstellen.

- So erstellen Sie ein Datenmuster

**STEP 3 |** Erstellen eines Datenprofils

Gruppieren Sie Datenmuster, bei denen die Sicherheit auf dieselbe Weise durchgesetzt werden soll, zu einem Datenprofil hinzu. Sie können Datenprofile auch verwenden, um zusätzliche Übereinstimmungskriterien und Konfidenzstufen für den Abgleich festzulegen.

- So erstellen Sie ein Datenprofil

**STEP 4 |** Erstellen einer DLP-Regel

Geben Sie den Datenverkehr und die Dateitypen an, die Enterprise DLP schützen soll. Legen Sie die Aktion fest, die Enterprise DLP ausführen soll, wenn ein DLP-Vorfall erkannt wird.

- So erstellen Sie eine DLP-Regel

# Verwalten: SaaS-Sicherheit

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)* | ❑ Prisma Access-Lizenz |

Identifizieren Sie mit SaaS Security Inline cloudbasierte Bedrohungen und riskante Benutzeraktivitäten in sanktionierten und nicht sanktionierten Apps.

SaaS Security Inline ist in das Cloud-verwaltete Prisma Access integriert, um Ihnen eine zentrale Ansicht der Netzwerk- und CASB-Sicherheit zu bieten. Es bietet SaaS-Transparenz – einschließlich erweiterter Analyse und Berichterstattung –, sodass Ihr Unternehmen über die erforderlichen Einblicke verfügt, um die Datensicherheitsrisiken der sanktionierten und nicht sanktionierten Nutzung von SaaS-Anwendungen in Ihrem Netzwerk zu verstehen.

Das CASB-Paket (Cloud Access Security Broker) umfasst SaaS Security Inline, Enterprise Data Loss Prevention (DLP) Inline, die SaaS Security API, Data Loss Prevention (DLP) API und SaaS Security Posture Management (SSPM).

Die Next-Generation Cloud Access Security Broker (CASB-X)-Lizenz enthält alle CASB-Komponenten wie SaaS Security Inline, SaaS Security API, SaaS Security Posture Management (SSPM) und Enterprise DLP. Es kann auf Cloud-verwaltete Prisma Access-, Panorama-verwaltete Prisma Access- und Panorama-verwaltete NGFW-Geräte in einer Ein-Mandanten-Umgebung angewendet werden.

**Hier *finden Sie alles, was Sie über SaaS-Sicherheit in Strata Cloud Manager wissen müssen.***

# Erste Schritte

So können Sie SaaS Security Inline in Prisma Access Cloud Management nutzen:

- Vergewissern Sie sich, dass die SaaS Security-Add-on-Lizenz in Ihrem Prisma Access-Abonnement enthalten ist.

  Gehen Sie zu **Verwalten** > **Konfiguration** > **Übersicht**, um zu prüfen, was mit Ihrer Lizenz verfügbar ist.

- Falls Sie dies noch nicht getan haben, aktivieren Sie die SaaS Security Inline-App im Hub.

  Nach der Aktivierung erkennt SaaS Security Inline automatisch alle SaaS-Anwendungen und Benutzer und analysiert die SaaS-Aktivitäts- und -Nutzungsdaten der Benutzer aus Ihren Prisma Access-Protokollen, die in Strata Logging Service gespeichert sind.

- Überprüfen und verwalten Sie Administratorrollen und -zugriff.

  Gehen Sie zu **Einstellungen** > **Identität und Zugriff**, um rollenbasierten Zugriff auf die SaaS-Sicherheitskontrollen in Prisma Access Cloud Management zu gewähren.

  > *Um die SaaS-Sicherheit umfassend verwalten zu können, müssen Benutzer auch Administratoren für die SaaS Security Inline-App sein. Springen Sie direkt vom Prisma Access Cloud Management-Dashboard zur **SaaS-Sicherheitskonsole**, um SaaS Security Inline-Administratoren hinzuzufügen.*

- Erkunden Sie das Dashboard **SaaS-Sicherheit** in Prisma Access Cloud Management.

  Gehen Sie zu **Verwalten** > **Konfiguration** > **Sicherheitsdienste** > **SaaS-Sicherheit**.

  Alle Dashboard-Ansichten werden direkt im Prisma Access Cloud Management unterstützt. Untersuchen Sie diese Ansichten, um riskante SaaS-Anwendungen und -Benutzer zu identifizieren und das SaaS-Sicherheitsmanagement durchzuführen. SaaS Security Posture Management (SSPM) hilft durch kontinuierliche Überwachung dabei, falsch konfigurierte Einstellungen in sanktionierten SaaS-Anwendungen zu erkennen und zu korrigieren.

- Überprüfen und teilen Sie den SaaS-Sicherheitsbericht.

  SaaS Security Inline enthält einen SaaS-Sicherheitsbericht, der eine Momentaufnahme der Anwendungsnutzung mit erweiterten aggregierten Daten und Ansichten bietet. Dieser Bericht dient als Kommunikationstool zwischen Ihrem SaaS-Sicherheitsteam und der Geschäftsleitung. Sie können diesen On-Demand-PDF-Bericht für regelmäßige Check-ins mit Ihrem SaaS-Sicherheitsteam teilen oder den Bericht per E-Mail an Ihre Führungskräfte senden, um die in Ihrer Organisation verwendeten SaaS-Anwendungen und die von ihnen ausgehenden Sicherheitsrisiken hervorzuheben.

  - Hier finden Sie weitere Informationen zum SaaS-Sicherheitsbericht.
  - So generieren Sie den SaaS-Sicherheitsbericht in der SaaS Security Inline-App.

- Sehen Sie, was Sie sonst noch mit SaaS-Sicherheit und Prisma Access Cloud Management tun können.

# SaaS-Richtlinienempfehlungen

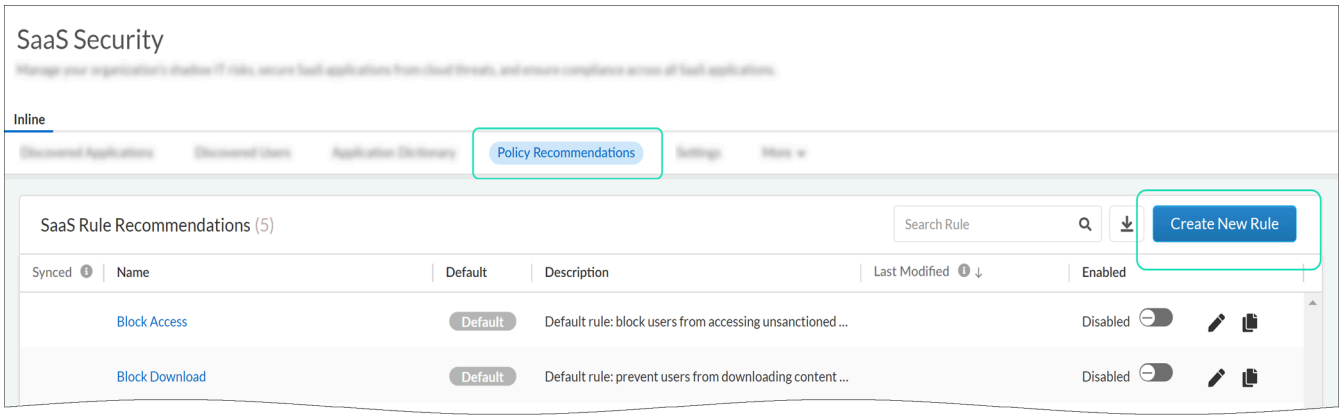
Um Einblick in und Kontrolle über SaaS-Anwendungen zu erhalten, erstellen SaaS-Sicherheitsadministratoren SaaS-Regelempfehlungen mit spezifischen SaaS-Anwendungs-IDs, die von der App-ID Cloud Engine (ACE) bereitgestellt werden.

In Prisma Access Cloud Management können Sie jetzt die von SaaS-Sicherheitsadministratoren empfohlenen Regeln überprüfen und akzeptieren. SaaS-Regelempfehlungen werden zu Ihrer Webzugriffsrichtlinie hinzugefügt. Um SaaS-Regel-Empfehlungen nutzen zu können, muss Websicherheit aktiviert sein.

**So können Sie loslegen – Überprüfen Sie hier den Workflow zum Prüfen und Akzeptieren der SaaS-Richtlinienempfehlungen:**

1. SaaS-Sicherheitsadministratoren erstellen SaaS-Regelempfehlungen in der SaaS Security Inline-App oder direkt in Prisma Access Cloud Management.

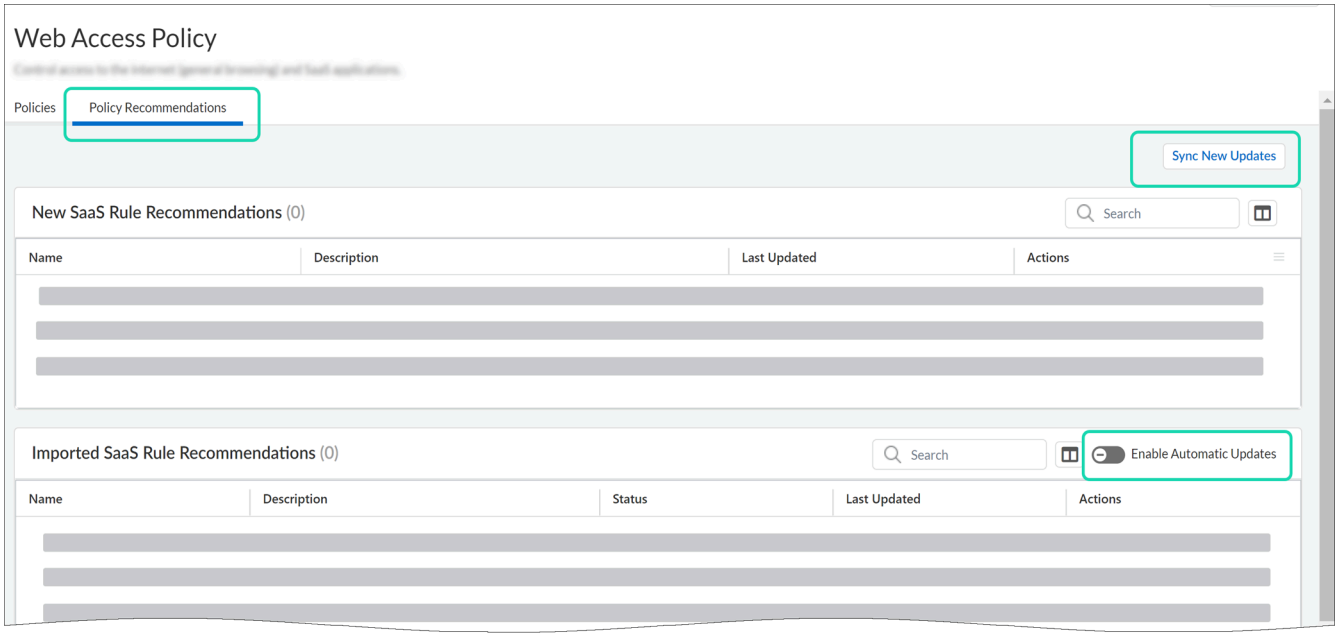
   # Gehen Sie in Prisma Access Cloud Management zu **Verwalten** > **Konfiguration** > **Sicherheitsdienste** > **SaaS-Sicherheit**.



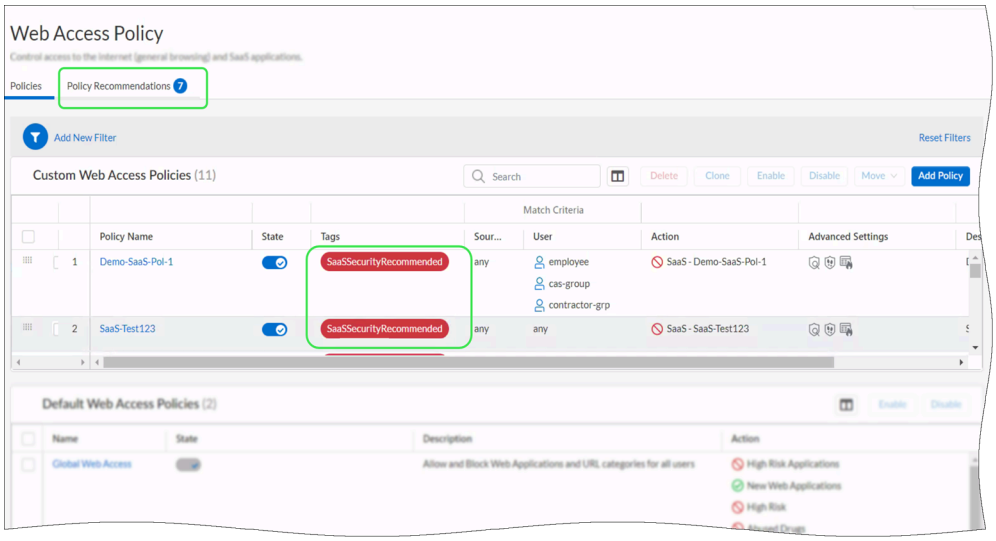

 

2. Sie können SaaS-Regelempfehlungen prüfen und importieren.

   # Gehen Sie zu **Verwalten** > **Websicherheit** > **Webzugriffsrichtlinie**.




3. Die von Ihnen importierten SaaS-Regelempfehlungen sind beschriftet, sodass Sie sie leicht identifizieren können.



# Verwalten: Prisma SD-WAN

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma SD-WAN | ❑ Prisma SD-WAN-Lizenz |

Prisma SD-WAN bietet eine softwaredefinierte Wide-Are-Network-Lösung (SD-WAN), die ältere Wide Are Networks in eine radikal vereinfachte, sichere Anwendungsstruktur (AppFabric) verwandelt. Hierbei werden die heterogenen zugrunde liegenden Transporte in einem einheitlichen hybriden WAN virtualisiert. Kern des Systems ist die Application Performance Engine.

Sie können präzise anwendungsbasierte Analysen anzeigen, eine zuverlässige Richtlinie erstellen und leistungsbasiertes WAN-Datenverkehrsmanagement durchführen. Prisma SD-WAN vereinfacht durch ION-Geräte (Instant-on Network) die Gestaltung, den Aufbau und die Verwaltung von WANs und erweitert die Sicherheit auf Rechenzentrumsniveau sicher auf den Netzwerkrand.

Prisma SD-WAN unterstützt gestapelte Richtlinien für Flussweiterleitungsvorgänge. Mithilfe zentral definierter Richtlinien führt jedes ION-Gerät Aktionen wie automatische Pfadauswahl, Traffic Shaping oder aktive Lastausgleiche zwischen Verbindungen aus, während der Prisma SD-WAN-Controller über alle WAN-Verbindungen hinweg vollständige Transparenz über die Anwendungsleistung und die Reaktionszeiten bietet.

Prisma SD-WAN steuert die Leistung von Netzwerkanwendungen auf der Grundlage von Anwendungsleistungs-SLAs (Service Level Agreements) und Geschäftsprioritäten. Sie können Richtlinien, Ressourcen, CloudBlades und Systemeinstellungen für Prisma SD-WAN mit Strata Cloud Manager konfigurieren.

Wählen Sie **Verwalten** > **Prisma SD-WAN** aus, um Konfigurationen für Folgendes zu verwalten:

- Richtlinien
- Ressourcen
- CloudBlades
- Systeme

# Verwalten: Richtlinien für Prisma SD-WAN

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma SD-WAN | ❑ Prisma SD-WAN-Lizenz |

Prisma SD-WAN unterstützt gestapelte und ursprüngliche Richtlinien. Mithilfe zentral definierter Richtlinien führt jedes ION-Gerät Aktionen wie automatische Pfadauswahl, Traffic Shaping oder aktiven Lastausgleich zwischen Verbindungen aus, während der Prisma SD-WAN-Controller über alle WAN-Verbindungen hinweg vollständige Transparenz über die Anwendungsleistung und die Reaktionszeiten bietet

Konfigurieren Sie Richtlinien in Prisma SD-WAN mit Strata Cloud Manager.

**STEP 1 |** Wählen Sie **Verwalten** > **Prisma SD-WAN** > **Richtlinien** aus.

Sie können die folgenden Arten von Richtlinienausnahmen in Prisma SD-WAN konfigurieren:

- Pfad

  Konfigurieren Sie gestapelte Pfadrichtlinien für Flussweiterleitungs- und Traffic-Shaping-Vorgänge.
- Leistung

  Konfigurieren Sie Leistungsrichtlinien, um Anwendungsleistung und Anwendungs-SLAs zu messen.
- QoS

  Konfigurieren Sie gestapelte QoS-Richtlinien zum Festlegen geschäftlicher Prioritäten.
- Sicherheit

  Konfigurieren Sie gestapelte Sicherheitsrichtlinien, um Regeln zu definieren, die den Anwendungszugriff innerhalb einer Zweigstelle bestimmen.
- NAT

  Konfigurieren Sie gestapelte NAT-Richtlinien, um den Datenschutz interner Netzwerke zu gewährleisten, die mit öffentlichen oder privaten Netzwerken verbunden sind.
- Sicherheit (ursprünglich)

  Dies sind veraltete Sicherheitsrichtlinien. Wenn Sie ein neuer Benutzer sind und mit der ION-Gerätesoftwareversion 6.0.1 beginnen, können Sie nur gestapelte Sicherheitsrichtlinien konfigurieren. Wenn Sie ursprüngliche oder ältere Richtlinien konfiguriert haben, müssen Sie diese älteren Richtlinien in gestapelte Richtlinien umwandeln, bevor Sie Ihr Gerät auf Version 6.0.1 aktualisieren können.
- Netzwerk (ursprünglich)

  Dies sind veraltete Netzwerkrichtlinien. Wenn Sie ein neuer Benutzer sind und mit der ION-Gerätesoftwareversion 6.0.1 beginnen, können Sie nur gestapelte Netzwerkrichtlinien konfigurieren. Wenn Sie ursprüngliche oder ältere Richtlinien konfiguriert haben, müssen Sie diese älteren Richtlinien in gestapelte Richtlinien umwandeln, bevor Sie Ihr Gerät auf Version 6.0.1 aktualisieren können.

**STEP 2 |** Wählen Sie **Bindungen** aus, um Richtlinienstapel an einen Standort zu binden.

Damit Richtlinienregeln in Pfad-, QoS-, Sicherheits- und NAT-Stapeln wirksam sind, müssen Sie die Richtlinienstapel an einen Standort binden. Sie können jeweils nur einen einzigen Pfad-, QoS-, Sicherheits- und NAT-Stapel an einen Standort binden.

# Verwalten: Ressourcentypen für Prisma SD-WAN

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma SD-WAN | ❑ Prisma SD-WAN-Lizenz |

Sie können verschiedene Arten von Ressourcen in Prisma SD-WAN verwalten.

Verwalten Sie Ressourcen in Prisma SD-WAN mit Strata Cloud Manager.

Wählen Sie **Verwalten** > **Prisma SD-WAN** > **Ressourcen** aus.

Sie können die folgenden Ressourcentypen in Prisma SD-WAN verwalten:

- Anwendungen

  Anwendungen bilden den Kern der Prisma SD-WAN-Lösung. Im Netzwerk bereitgestellte ION-Geräte analysieren aktiv jeden Anwendungsfluss, um sicherzustellen, dass Richtlinien für Leistung, Compliance und Sicherheit eingehalten werden und dass für jeden Fluss optimale Netzwerkverbindungen verwendet werden. Das ION-Gerät verwendet Anwendungsdefinitionen und Fingerabdruck-Technologien für Pfadauswahl, QoS und Firewall-Richtlinien.

  Systemanwendungen sind standardmäßig verfügbar, Sie können jedoch benutzerdefinierte Anwendungen für Ihre Unternehmensanforderungen konfigurieren.

- Schaltkreiskategorien

  Schaltkreiskategorien sind eine logische Gruppierung verschiedener Arten von Schaltkreisen und Verbindungen, die im Netzwerk vorhanden sein können. Diese Gruppierung ermöglicht vereinfachte und wiederverwendbare Netzwerkrichtlinienregeln für das gesamte Netzwerk. Beispiele hierfür sind Breitbandinternet über Kabel, LTE-Internetverbindungen mit Gebühren, Satelliten-Internetverbindungen, DSL-Internet oder privates MPLS.

- Netzwerkkontexte

  Der Netzwerkkontext segmentiert den Netzwerkverkehr, um unterschiedliche Netzwerkrichtlinienregeln für dieselbe Anwendung anzuwenden. Eine Regel mit Netzwerkkontext hat immer Vorrang vor einer Regel ohne Netzwerkkontext. Sie können einen oder mehrere Netzwerkkontexte erstellen, aber ein einzelnes LAN kann nur zu einem Netzwerkkontext gehören. Damit die Netzwerkkontexte wirksam werden, müssen Sie sie an die entsprechenden LAN-Segmente anhängen.

- Dienst- und DC-Gruppen

  Verwenden Sie Dienst- und DC-Gruppen, um Drittanbieterendpunkte Gruppen zuzuordnen. So können Sie beim Erstellen von Netzwerkrichtlinienregeln flexibel sein und die Eindeutigkeit über verschiedene Standorte hinweg berücksichtigen. Die Absicht besteht darin, dass die Richtlinienregeln unabhängig vom Standort gleich bleiben.

- Sicherheitszonen

  Sicherheitszonen legen Durchsetzungsgrenzen fest, in denen der Verkehr kontrolliert und gefiltert wird. Jede Sicherheitszone wird Netzwerken zugeordnet, die mit physischen Schnittstellen, logischen Schnittstellen oder Unterschnittstellen eines Geräts verbunden

sind. Diese Schnittstellen auf Zonenebene dienen als Proxy für physische und virtuelle Schaltkreise, wie etwa VLAN-, Layer-3-VPN- und Layer-2-VPN-Schaltkreise.

- Standortvorlagen

  Mithilfe von Standort-Konfigurationsvorlagen können Sie maßgeschneiderte Standortvorlagen erstellen, die Ihren Bereitstellungsanforderungen gerecht werden. So können Sie Zweigstellen und Rechenzentren problemlos und effizient in großem Maßstab bereitstellen. Mit dieser Vorlage können Sie mehrere Standorte bereitstellen. Sie können eine vorhandene Vorlage verwenden, sie bearbeiten oder eine neue Vorlage erstellen, um mehrere Standorte bereitzustellen.

- Präfixfilter

  Ein Präfix ist eine Gruppe aus einer oder mehreren einzelnen IP-Adressen oder IP-Adress-Subnetzen. Präfixe werden mit Pfadsatzrichtlinien und Prioritätsrichtlinien verwendet. Sie können entweder globaler oder lokaler Natur sein.

- **Konfigurationsprofile**

  Verwenden Sie Konfigurationsprofile, um Einstellungen für verschiedene Arten von Ressourcen zu konfigurieren.

  - IPsec

    Erstellen Sie ein IPsec-Profil, um IPsec-VPN-Verbindungen zwischen Zweigstellengeräten und Cloud-Sicherheitsdienst-Endpunkten zu konfigurieren.

  - IPFIX

    Ein IPFIX-Profil ist ein globales IPFIX-Konfigurationsobjekt, das die Collector-Konfiguration, die Filterkonfiguration, die Vorlage zum Exportieren von Fluss-Informationselementen und die Fluss-Sampler-Konfiguration identifiziert.

  - APN

    Erstellen Sie ein APN-Profil (Access Point Name), um den Netzwerkpfad für die mobile Datenverbindung zu definieren. Für die Verbindung mit einem Mobilfunknetz sind APN-Informationen erforderlich.

  - DNS

    Konfigurieren Sie ein DNS-Profil (Domain Name System), um Konfigurationsparameter für den DNS-Dienst anzugeben. Zu den häufig konfigurierten Parametern gehören DNS-

Server, Domänen-Adresszuordnung, Cache-Konfiguration und DNSSEC-Konfiguration. Nachdem das DNS-Dienstprofil erstellt wurde, wird es an ein Gerät gebunden.

- NTP-Vorlagen

  Verwenden Sie NTP-Konfigurationsvorlagen (Network Time Protocol), um NTP-Server hinzuzufügen oder zu bearbeiten.

- Multicast

  Erstellen Sie ein WAN-Multicast-Konfigurationsprofil und verknüpfen Sie es mit einer Zweigstelle, um WAN-Multicast-Routing für die Zweigstelle zu aktivieren.

- VRF

  Erstellen und verknüpfen Sie das globale (standardmäßige) VRF-Profil (Virtual Routing and Forwarding) und weisen Sie es allen Zweigstellen- und Rechenzentrumsstandorten zu.

- IoT-Erkennung

  Nutzen Sie die IoT-Gerätetransparenz, um Geräte in Ihrem Netzwerk zu identifizieren. Zweigstellen-ION-Geräte mit Prisma SD-WAN prüfen Pakete, extrahieren Informationen und generieren Nachrichten, die in einem bestimmten Format an Strata Logging Service gesendet werden.

# Verwalten: CloudBlades für Prisma SD-WAN

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma SD-WAN | ❑ Prisma SD-WAN-Lizenz<br>❑ CloudBlade-Lizenz für das jeweilige CloudBlade |

Verwenden Sie die Prisma SD-WAN-CloudBlades-Plattform für den sicheren Zugriff auf ION-Geräte, um Weboberflächen-Workflows mit benutzerdefinierten Vorlagen zu automatisieren und so die betriebliche Komplexität zu reduzieren.

Konfigurieren Sie CloudBlades in Prisma SD-WAN mit Strata Cloud Manager.

Wählen Sie **Verwalten** > **Prisma SD-WAN** > **CloudBlades** aus.

Sie können die CloudBlades anzeigen, die Sie in Prisma SD-WAN abonniert haben. Befolgen Sie die Schritte im entsprechenden CloudBlade-Integrationshandbuch, um Ihr CloudBlade zu konfigurieren.

# Verwalten: Systemressourcen für Prisma SD-WAN

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma SD-WAN | ❑ Prisma SD-WAN-Lizenz |

Verwalten und überwachen Sie Benutzer und Berechtigungen in Prisma SD-WAN mit den Ressourcen, die auf der Registerkarte **System** verfügbar sind.

Wählen Sie **Verwalten** > **Prisma SD-WAN** > **System** aus.

Sie können die folgenden Arten von Systemressourcen in Prisma SD-WAN konfigurieren:

- Lizenzverwaltung

  Verwenden Sie die Lizenzverwaltung, um Autorisierungstoken für virtuelles ION zu generieren. Dies bietet eine Reihe von Kontrollen, um das unbefugte Hinzufügen virtueller Geräte zu einer Umgebung zu verhindern.

- Auditierungslogs

  Verwenden Sie Auditierungslogs, um die Konfigurationsänderungsdatensätze in einem System anzuzeigen. Sie können diese Protokolle zu Compliance- und Fehlerbehebungszwecken verwenden. Auditierungslogs enthalten Informationen, wie z. B. vorgenommene Änderungen, Eigentümer der Änderung, Zeitpunkt der Änderung und Umfang der Änderung, für einen Standort, ein System oder eine Untergruppe von Standorten.

- Unternehmenspräfixe

  Verwenden Sie Unternehmenspräfixe, damit Prisma SD-WAN-Rechenzentrumsstandorte problemlos Routen an Zweigstellen übermitteln und die Erreichbarkeit gewährleisten können.

- **Zugriffsverwaltung**
  - Benutzerzugriff
    - Benutzerverwaltung

      Fügen Sie einen neuen Benutzer mit einer Systemrolle hinzu, die den Anforderungen Ihres Unternehmens entspricht. Systemrollen sind ein vordefinierter Satz von Berechtigungen für jede Rolle. Diese Rollen beinhalten eine Sammlung von einer oder mehreren Systemberechtigungen. Zu den verfügbaren Systemrollen gehören Root, Superadministrator, IAM-Administrator, Netzwerkadministrator, Sicherheitsadministrator und Benutzer mit schreibgeschütztem Zugriff.

    - Benutzerdefinierte Rollen

      Sie können benutzerdefinierte Rollen erstellen, indem Sie vorhandene Systemrollen und Berechtigungen auf unterschiedliche Weise kombinieren. Sie können sie erstellen, indem Sie eine Reihe von Systemberechtigungen verbinden oder Berechtigungen zu Systemrollen hinzufügen oder daraus entfernen.

- Passwortanforderungen

  Legen Sie die Zeichen- und Sicherheitsanforderungen für Passwörter fest. Sie können auch die Häufigkeit festlegen, in der alte Passwörter wiederverwendet werden können oder aktualisiert werden müssen.

- Gerätezugriff
  - Geräte-Toolkit-Benutzerzugriff
  - Offline-Zugriffsrichtlinie
- Mandantenzugriff
  - Authentifizierungstoken

    Konfigurieren Sie Authentifizierungstoken für den Zugriff auf Prisma SD-WAN-APIs. Sobald ein Token für einen Benutzer generiert wurde, kann es für wiederholte API-Aufrufe verwendet werden, wodurch unnötige Anmeldungen für den Zugriff auf APIs vermieden werden.

    Ein Benutzer mit Zugriff auf ein Auth-Token kann auf alle dem Token zugewiesenen Berechtigungen zugreifen.

    Wählen Sie **Verwalten** > **System** > **Mandantenzugriff** > **Auth-Token** > **Auth-Token erstellen**, um ein Authentifizierungstoken zu erstellen.
- Identitätsmanagement
  - Cloud Identity Engine

# Verwalten: Prisma Access Browser

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access-Lizenz |

Wählen Sie in Strata Cloud Manager **Verwalten** > **Konfiguration** > **Prisma Access Browser** aus.

Prisma Access Secure Enterprise Browser (Prisma Access Browser) ist die einzige Lösung, die sowohl verwaltete als auch nicht verwaltete Geräte über einen nativ integrierten Unternehmensbrowser schützt, der den Schutz auf nicht verwaltete Geräte ausweitet. Siehe Was ist der Prisma Access Browser?.

# Home

Home ist die Landingpage, die angezeigt wird, wenn Sie Prisma Access Browser über Strata Cloud Manager öffnen. Über die Startseite können Sie die Prisma Access Browser-Dashboards verwenden, um aussagekräftige Erkenntnisse aus der Analyse von Nutzerverhaltens- und Browsing-Daten zu gewinnen. Es gibt eine Vielzahl von Dashboards für spezifische Anwendungsfälle, die Sie möglicherweise überwachen wollen, z. B. Benutzerverhalten, Verhinderung von Datenlecks, Websicherheit und Richtlinien. Jedes Dashboard enthält eine Sammlung von Widgets und einige der Widgets werden in mehreren Dashboards angezeigt.

# Analytics

Der Prisma Access Browser-Bildschirm „Ereignisse“ ist das wichtigste Transparenztool, mit dem Sie jede Aktivität in Ihrer Enterprise Browser-Bereitstellung untersuchen können, um sicherzustellen, dass Richtlinien und Regeln ordnungsgemäß funktionieren. Hier können Sie Prisma Access Browser-Ereignisse untersuchen.

# Verzeichnis

- Das Benutzerverzeichnis dient als zentraler Ort für Informationen über die Benutzer und ihre mit Prisma Access Browser verbundenen Geräte, über ihre Mitgliedschaft in Benutzergruppen sowie über die zugehörigen Richtlinienregeln. Verwalten von Prisma Access Browser-Benutzern
- Das Geräteverzeichnis enthält eine Liste Ihrer Prisma Access Browser-Geräte und -Gerätegruppen. Verwalten von Prisma Access Browser-Geräten
- Der Prisma Access Browser ist mit einer vordefinierten Liste verifizierter Anwendungen ausgestattet. Die Liste der überprüften Anwendungen nutzt den App-ID™-Anwendungskatalog von Palo Alto Networks und wird regelmäßig mit der Cloud-Datenbank synchronisiert. Sie können auch benutzerdefinierte und private Anwendungen erstellen. Verwalten von Prisma Access Browser-Anwendungen
- Der Prisma Access Browser verwaltet ein Erweiterungsverzeichnis, das Erweiterungen enthält, die von Endbenutzern im Browser installiert wurden. Mit diesen Informationen können Sie ein ordnungsgemäßes Management von Unternehmensrichtlinien aufrechterhalten, die Transparenz managen und Risikoanalysen durchführen.Verwalten von Prisma Access Browser-Erweiterungen

# Richtlinien

- Sie können Regeln verwenden, um die Benutzer, Benutzergruppen und Gerätegruppen anzugeben, die von den verschiedenen Richtlinien betroffen sind. Diese Regeln steuern den Zugriff auf Webanwendungen, Sicherheitsrichtlinien und Anpassungsoptionen. Mit Regeln können Sie den Benutzerzugriff auf Organisationstools und Organisationskomponenten genau steuern.Verwalten von Prisma Access Browser-Richtlinienregeln
- Die Steuerungen für die Prisma Access Browser-Regeln können innerhalb des Textkörpers der einzelnen Regel konfiguriert werden. Profile (externe Steuerungen) können verwendet werden, wenn Sie wiederverwendbare (Legacy-)Profile speichern und später den Regeln hinzufügen möchten. Verwalten von Prisma Access Browser-Richtlinienprofilen
- Verwenden Sie Anmelderegeln, um zu bestimmen, welche Benutzer und Geräte auf Prisma Access Browser zugreifen dürfen. Verwalten von Prisma Access Browser-Anmelderegeln
- Nachdem Sie die Umgehungsbedingungen in den Richtlinienregeln definiert haben, können Benutzer, die versuchen, eine Aktion auszuführen oder eine Website zu besuchen, die durch die entsprechende Regel blockiert wird, eine Umgehungsanfrage senden. Um Umgehungsbedingungen festzulegen, konfigurieren Sie die Eingabeaufforderungsaktion, mit der Berechtigungsanfragen ermöglicht werden. Verwalten von Prisma Access Browser-Anfragen zur Umgehung von Richtlinienregeln

# Verwaltung

Verwalten Sie Integrationen für zusätzliche Funktionen mit:

- Microsoft 365
- Microsoft Information Protection
- Google Workspace
- Votiro
- CrowdStrike Falcon Intelligence
- OPSWAT MetaDefender
- YazamTech SelektorIT
- Symantec DLP

# Verwalten: Vorgänge

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access<br><br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)*<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | ❑ Mindestens eine dieser Lizenzen ist erforderlich, um Ihre Konfiguration mit Strata Cloud Manager zu verwalten; für die einheitliche Verwaltung von NGFWs und Prisma Access benötigen Sie Folgendes:<br>❑ Prisma Access-Lizenz<br>❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>❑ Strata Cloud Manager Essentials<br>❑ Strata Cloud Manager Pro<br><br>→ Die Ihnen zur Verfügung stehenden Funktionen und Fähigkeiten in Strata Cloud Manager hängen davon ab, welche Lizenz(en) Sie verwenden. |

Verwenden Sie die Strata Cloud Manager-Vorgänge zur Übertragung von Konfigurationsänderungen, Überprüfung früherer Konfigurationsübertragungen und Verwaltung der Snapshots Ihrer Konfigurationsversionen, um sie zu laden oder auf eine vorherige Konfigurationsversion zurückzusetzen.

- Übertragen Ihrer Konfigurationsänderungen
- Überprüfen des Status eines Konfigurationsübertragung
- Bereinigen Ihrer Konfiguration

# Verwalten: Konfiguration übertragen

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)*<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | ❑ Mindestens eine dieser Lizenzen ist erforderlich, um Ihre Konfiguration mit Strata Cloud Manager zu verwalten; für die einheitliche Verwaltung von NGFWs und Prisma Access benötigen Sie Folgendes:<br>❑ Prisma Access-Lizenz<br>❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>❑ Strata Cloud Manager Essentials<br>❑ Strata Cloud Manager Pro<br>→ Die Ihnen zur Verfügung stehenden Funktionen und Fähigkeiten in Strata Cloud Manager hängen davon ab, welche Lizenz(en) Sie verwenden. |

Nachdem Sie Konfigurationsänderungen vorgenommen haben und bereit sind, diese zu aktivieren, müssen Sie die Änderungen an Ihre Firewalls übertragen. Sie haben die Möglichkeit, alle Konfigurationsänderungen zu übertragen oder bestimmte Administratoren auszuwählen, die in die Übertragung einbezogen werden sollen. Für Ihre erste Konfigurationsübertragung ist die Übertragung von Änderungen durch alle Administratoren erforderlich. Sie können auswählen, welche Konfigurationsänderungen Sie an Prisma Access übertragen möchten:

- **Websicherheit**

  Übertragen Sie Websicherheitsupdates an Prisma Access.
- **Mobile Benutzer – GlobalProtect**

  Übertragen Sie Global Protect-Updates an Prisma Access.
- **Mobile Benutzer – Expliziter Proxy**

  Übertragen Sie Expliziter Proxy-Updates an Prisma Access.
- **Remote-Netzwerke**

  Übertragen Sie Remote-Netzwerke-Updates an Prisma Access.
- **Dienstverbindungen**

  Übertragen Sie Dienstverbindung-Updates an Prisma Access.

Sie können eine Konfiguration übertragen, während gerade eine andere Konfigurationsübertragung stattfindet. Prisma Access wendet Konfigurationsänderungen in der Reihenfolge an, in der Sie sie übermitteln.

Falls eine Konfiguration irrtümlicherweise übertragen wurde oder eine Änderung zu Netzwerk- oder Sicherheitsstörungen führt, können Sie die Prisma Access-Konfiguration auf die zuletzt

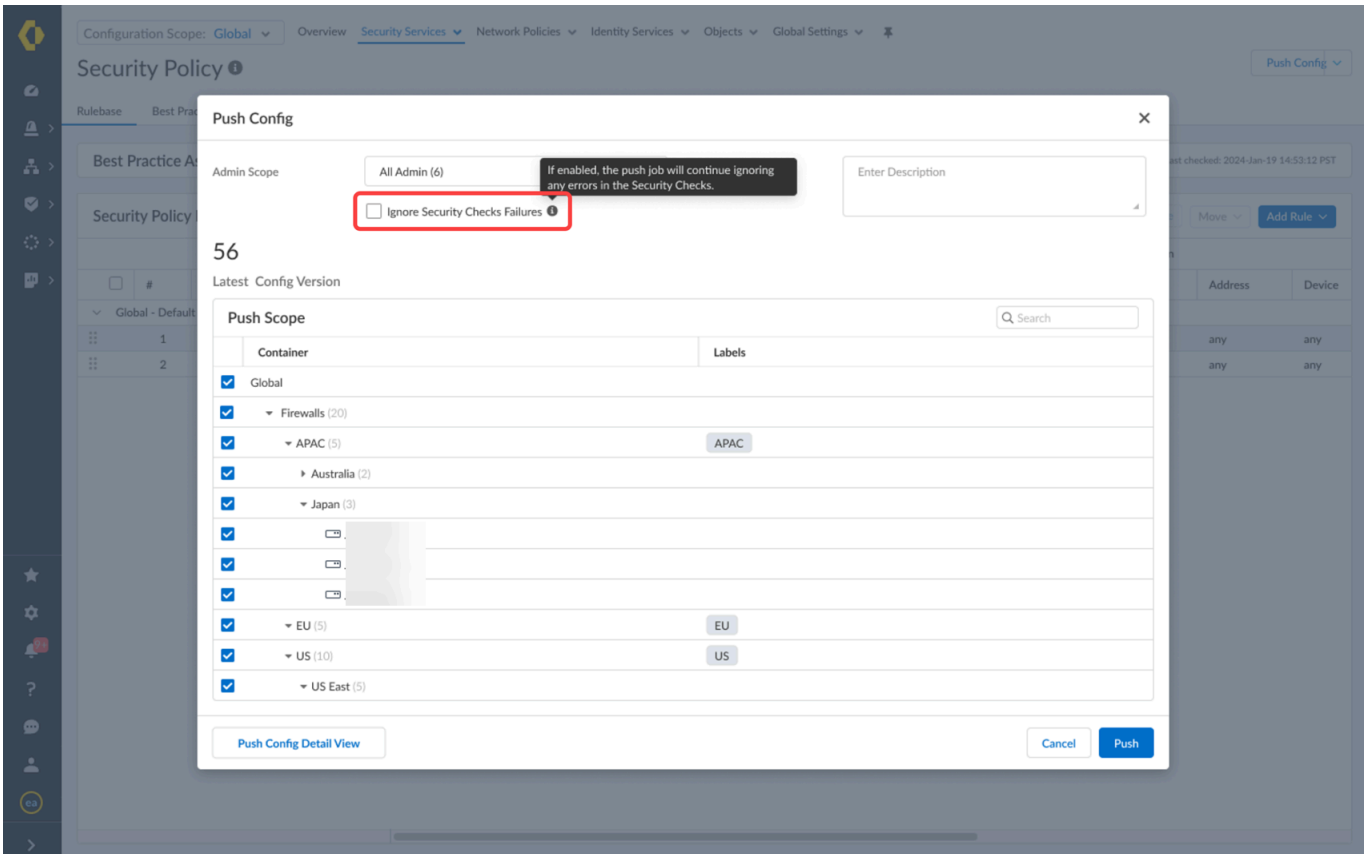
ausgeführte Prisma Access-Konfiguration zurücksetzen. Auf diese Weise können Sie die Prisma Access-Konfiguration auf eine laufende Konfiguration zurücksetzen, von der Sie wissen, dass sie funktionsfähig ist und Ihre Netzwerksicherheit nicht gefährdet. Sie haben nicht die Möglichkeit, eine bestimmte Laufkonfiguration auszuwählen. Prisma Access wählt automatisch die letzte bekannte laufende Konfiguration aus und greift auf diese zurück.

**STEP 1 |** Melden Sie sich bei Strata Cloud Manager an.

**STEP 2 |** Nehmen Sie nach Bedarf Konfigurationsänderungen vor.

**STEP 3 |** Wählen Sie **Konfiguration übertragen** und **Übertragen**, um Ihre Konfigurationsänderungen zu übertragen.

*Alternativ können Sie **Verwalten** > **Vorgänge** > **Konfiguration auf Geräte übertragen** auswählen.*




Im Dialogfeld **Konfiguration übertragen** können Sie **Sicherheitsüberprüfungsfehler ignorieren**. Mit dieser Funktion können Sie Übertragungsvorgänge auch dann fortsetzen, wenn bestimmte Prüfungen den Vorgang blockieren würden. Wenn Sie das Kontrollkästchen deaktiviert lassen (Standardeinstellung) und eine Best-Practice-Überprüfung mit der Aktion „Blockieren“ fehlschlägt, stoppt Strata Cloud Manager die Übertragung.

**STEP 4 |** (Optional) Wählen Sie **Neuen Filter hinzufügen**.

Sie können die im Übertragungsumfang angezeigten Geräte durch Anwenden von Filtern filtern. Das Anwenden von Filtern wirkt sich nur darauf aus, welche Firewalls oder

Prisma Access-Bereitstellungen im Übertragungsumfang angezeigt werden, und hat keinen Einfluss darauf, an welche Geräte Sie übertragen.

**STEP 5 |** Bearbeiten Sie den Übertragungsumfang.

Durch Bearbeiten des Übertragungsumfangs können Sie gezielte Konfigurationsänderungen an einige oder all Ihrer Firewalls oder Prisma Access-Bereitstellungen übertragen.

*Das Durchführen einer teilweisen Konfigurationsübertragung wird nicht unterstützt. Sie müssen die gesamte Strata Cloud Manager-Konfiguration übertragen, wenn Sie …*

- einen neuen Mandanten konfigurieren; *dies ist Ihre erste Konfigurationsübertragung*
- eine Firewall in Strata Cloud Manager einbinden
- *Mobile Prisma Access-Benutzer und -Remote-Benutzer einbinden*
- *einen* Ordner *umbenennen oder verschieben, sodass er in einem anderen Ordner verschachtelt ist*
- *eine Firewall in einen anderen Ordner verschieben*
- *ein* Snippet*umbenennen, verknüpfen oder die Verknüpfung trennen*
- *eine Konfiguration laden*
- *die Konfiguration auf die zuletzt übertragene Konfiguration oder auf einen Snapshot einer früheren Konfigurationsversion zurücksetzen*

- **Administratorbereich** – Wählen Sie aus, welche Administratorkonfigurationsänderungen in die Übertragung einbezogen werden sollen. Standardmäßig wählt der Administratorbereich den aktuellen Benutzer aus und die von diesem Benutzer vorgenommenen Änderungen werden an die ausgewählten Firewalls oder Prisma Access-Bereitstellungen übertragen. Wenn Sie **Änderungen aller Administratoren** auswählen, umfasst das alle Konfigurationsänderungen, die von allen Administratoren vorgenommen wurden.

  Das Bearbeiten des Administratorbereichs zum Auswählen bestimmter Administratoren umfasst alle von den ausgewählten Administratoren vorgenommenen Konfigurationsänderungen. Diese Option kann nicht verwendet werden, wenn Sie Ihre erste Konfigurationsübertragung durchführen. Das Auswählen bestimmter Konfigurationsänderungen zum Einbeziehen in die Übertragung wird nicht unterstützt.
- **Übertragungsumfang** – Wählen Sie die Bereitstellungstypen oder Ordner aus, an die Sie übertragen möchten. Wenn Sie eine Bereitstellung oder einen Ordner auswählen, werden die Konfigurationsänderungen an alle Firewalls oder Bereitstellungen übertragen.

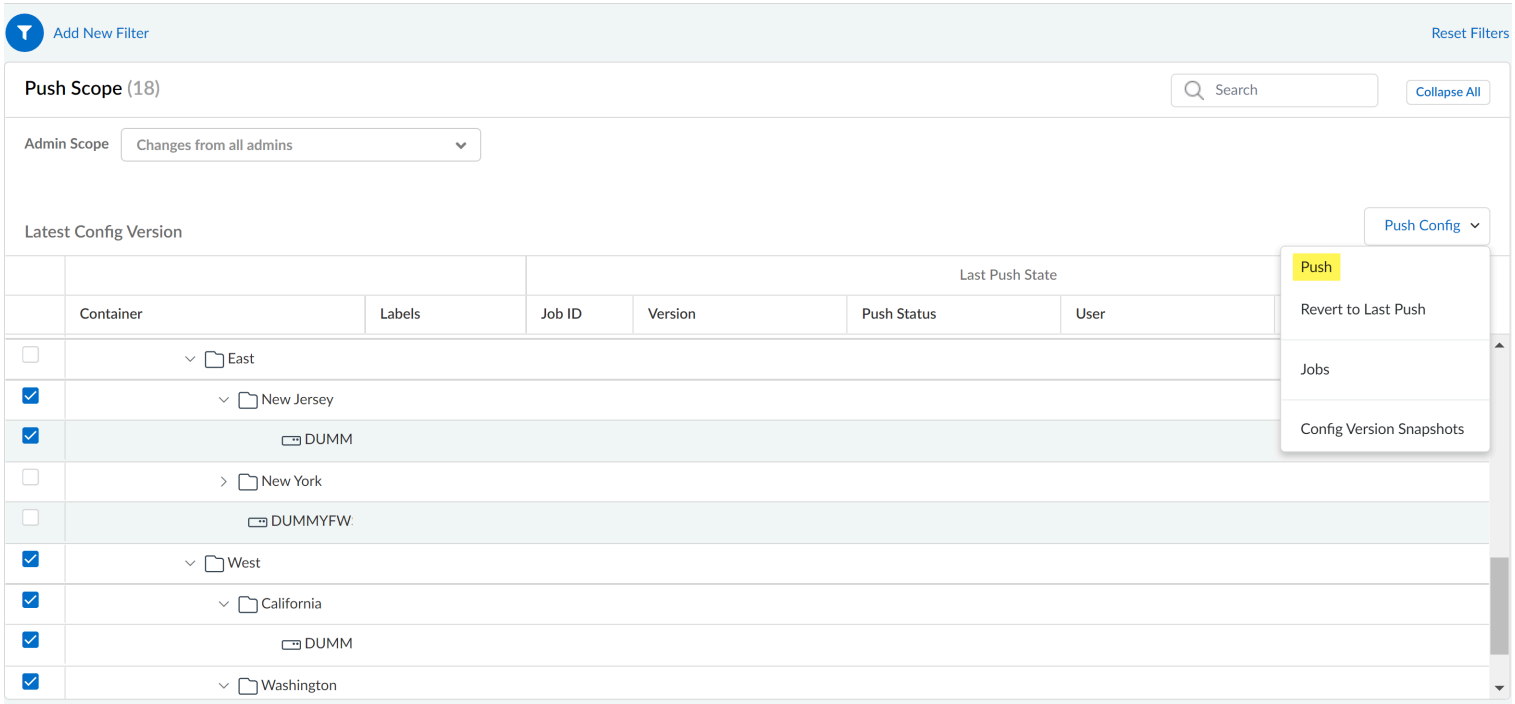
  Wenn Sie einen Ordner auswählen, der Unterordner enthält, werden alle Unterordner und die zugehörigen Firewalls oder Prisma Access-Bereitstellungen in die Übertragung

einbezogen. Wenn Sie eine bestimmte Firewall oder Prisma Access-Bereitstellung auswählen, wird automatisch der damit verknüpfte Ordner ausgewählt.

**STEP 6 |** Wählen Sie **Konfiguration übertragen** und **Übertragen**.

Überprüfen Sie die Übertragungsziele und wählen Sie **Übertragen**.




**STEP 7 |** Überprüfen Sie den Push-Status der Konfiguration.

Falls eine Konfiguration irrtümlicherweise übertragen wurde oder eine Änderung zu Netzwerk- oder Sicherheitsstörungen führt, können Sie Ihre Prisma Access-Konfiguration zurücksetzen.

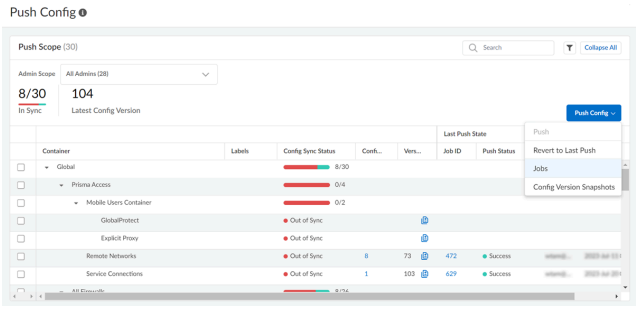
# Konfigurationsversionen wiederherstellen, laden und vergleichen

## Prisma Access-Jobs anzeigen

Sie können den **Jobverlauf** in Prisma Access anzeigen, um Details zu von Administratoren initiierten Vorgängen sowie zu automatischen Inhalts- und Lizenzaktualisierungen anzuzeigen. Dies umfasst sämtliche Konfigurations-Commits, -Übertragungen und -Rücksetzungen. Sie können die Jobansicht verwenden, um Fehler bei fehlgeschlagenen Vorgängen zu beheben, Warnungen im Zusammenhang mit abgeschlossenen Commits zu untersuchen oder ausstehende Commits abzubrechen.

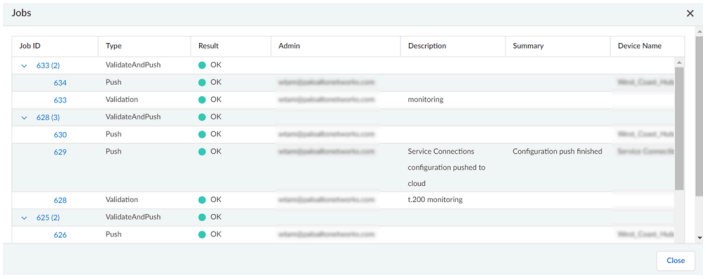
**STEP 1 |** Starten Sie Prisma Access.

**STEP 2 |** Wählen Sie in der oberen Menüleiste **Konfiguration übertragen** aus und zeigen Sie die Prisma Access-**Jobs** an.




**STEP 3 |** Führen Sie eine der folgenden Aufgaben aus:

- **Untersuchen Sie Warnungen oder Fehler** – Lesen Sie die Einträge in der Spalte „Zusammenfassung“, um Einzelheiten zu Warnungen oder Fehlern zu erfahren.
- **Zeigen Sie eine Commit-Beschreibung an** – Wenn ein Administrator eine Commit-Beschreibung eingegeben hat, können Sie in der Spalte „Beschreibung“ nachsehen, was der Zweck des Commits ist.
- **Überprüfen Sie die Position eines Vorgangs in der Warteschlange** – Zeigen Sie die Position und den Status des Vorgangs an, um die Position des Vorgangs zu bestimmen.



# Verwalten: Push-Status

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)*<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | ❑ Mindestens eine dieser Lizenzen ist erforderlich, um Ihre Konfiguration mit Strata Cloud Manager zu verwalten; für die einheitliche Verwaltung von NGFWs und Prisma Access benötigen Sie Folgendes:<br>❑ Prisma Access-Lizenz<br>❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>❑ Strata Cloud Manager Essentials<br>❑ Strata Cloud Manager Pro<br>→ Die Ihnen zur Verfügung stehenden Funktionen und Fähigkeiten in Strata Cloud Manager hängen davon ab, welche Lizenz(en) Sie verwenden. |

Überprüfen Sie den Push-Status Ihrer früheren Konfigurationsübertragungen an Ihre Firewalls, um Details wie das Ergebnis des Übertragungsvorgangs, den Administrator, der die Übertragung initiiert hat, und die Ziel-Firewalls zu überprüfen.

**STEP 1 |** Melden Sie sich bei Strata Cloud Manager an.

**STEP 2 |** Übertragen Sie Ihre Konfigurationsänderungen.

**STEP 3 |** Wählen Sie **Verwalten** > **Vorgang** > **Push-Status** und suchen Sie den Konfigurationsübertragungsvorgang, den Sie überprüfen möchten.

**STEP 4 |** Erweitern Sie die `Job-ID` für die Konfigurationsübertragung, die Sie überprüfen möchten.

Ein Konfigurationsjob zur `Validierung` wird immer ausgeführt, bevor eine Konfigurationsübertragung erfolgt. Wenn Sie an mehrere Firewalls übertragen, erhält jede Konfigurationsübertragung eine eindeutige `Job-ID` mit Übertragungsdetails.

**STEP 5 |** Überprüfen Sie die Details zum Push-Status der Konfiguration.

Überprüfen Sie beispielsweise das `Ergebnis` der Übertragung, den `Administrator`, der die Konfigurationsübertragung initiiert hat, die `Zusammenfassung` der Konfigurationsübertragung sowie die `Endzeit` und `Startzeit` der Konfigurationsübertragung.

Das `Ergebnis` der Konfigurationsübertragung kann entweder `OK` lauten, wenn sie erfolgreich war, oder `FEHLGESCHLAGEN`, wenn die Konfigurationsübertragung fehlgeschlagen ist.

**STEP 6 |** Klicken Sie auf die eindeutige `Job-ID` für eine Konfigurationsübertragung an eine Firewall, um die Jobdetails zu überprüfen.

Die Jobdetails enthalten detaillierte Informationen zu `Warnungen` und `Fehlern`, die bei der Durchführung der Konfigurationsübertragung aufgetreten sind. Wenn beispielsweise eine Übertragung an eine Firewall fehlgeschlagen ist, können Sie die Jobdetails überprüfen, um zu verstehen, warum die Konfigurationsübertragung fehlgeschlagen ist.

# Verwalten: Snapshots der Konfigurationsversion

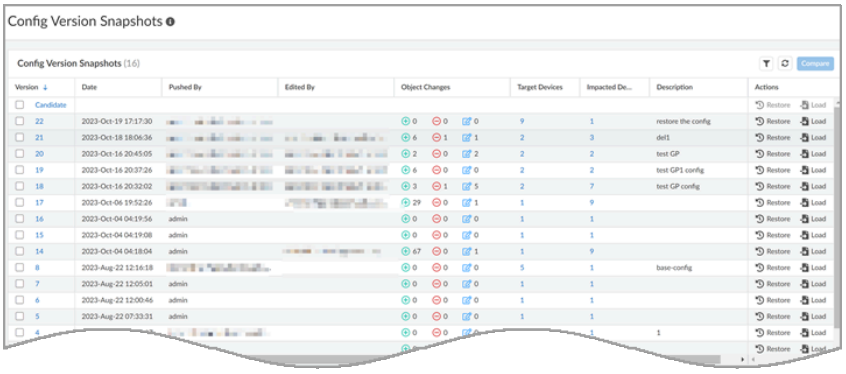
| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)*<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | ❑ Mindestens eine dieser Lizenzen ist erforderlich, um Ihre Konfiguration mit Strata Cloud Manager zu verwalten; für die einheitliche Verwaltung von NGFWs und Prisma Access benötigen Sie Folgendes:<br>❑ Prisma Access-Lizenz<br>❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>❑ Strata Cloud Manager Essentials<br>❑ Strata Cloud Manager Pro<br>→ Die Ihnen zur Verfügung stehenden Funktionen und Fähigkeiten in Strata Cloud Manager hängen davon ab, welche Lizenz(en) Sie verwenden. |

Konfigurations-Snapshots geben Ihnen einen Einblick in Ihren Strata Cloud Manager-Konfigurationsverlauf. Wenn eine Konfigurationsübertragung unbeabsichtigte Auswirkungen auf die Sicherheit oder unerwarteten Einfluss auf den Datenverkehr hat, können Sie die Konfiguration wiederherstellen, indem Sie zu einer früheren Version zurückkehren. Sie können auch Konfigurationen vergleichen, um zu sehen, was sich zwischen den Versionen geändert hat.

## Übersicht über den Konfigurations-Snapshot

Auf dem Bildschirm „Snapshots der Konfigurationsversion“ können Sie per Push übertragene Konfigurationen überprüfen, Konfigurations-Snapshots mit Ihrem Konfigurationskandidaten vergleichen und ältere Konfigurationen laden oder wiederherstellen.

Wählen Sie **Verwalten** > **Vorgänge** > **Snapshots der Konfigurationsversion** aus, um Konfigurations-Snapshots zu suchen und Versionen wiederherzustellen, zu laden oder zu vergleichen.



1. **Neuen Filter hinzufügen** – Wählen Sie Filter aus, um Konfigurationsversionen nach Spalte zu sortieren und zu filtern.
2. **Version** – die Versionsnummer der per Push übertragenen Konfiguration.

   Mit **Kandidaten** können Sie die derzeit anstehenden Konfigurationsänderungen an Strata Cloud Manager mit einer früheren Konfigurationsversion vergleichen.

   *Die Konfigurationsversionsnummer ist inkrementell. Wenn Sie beispielsweise 10 Versionen haben und die Konfigurationsversion 2 wiederherstellen, ändert sich die Konfigurationsversion von 10 zu 11 (sie wird nicht mehr als „2“ angezeigt).*
3. **Datum** – Datum und Uhrzeit der Push-Konfigurationsübertragung.
4. **Per Push übertragen durch** – Administrator, der die Änderungen übertragen hat.
5. **Bearbeitet von** – Administrator, der die Konfigurationsänderungen vor der Push-Übertragung vorgenommen hat.
6. **Objektänderungen** – Sehen Sie, wie viele Objekte bei der Push-Konfigurationsübertragung hinzugefügt, entfernt oder geändert wurden.
7. **Zielgeräte** – Geräte, die im Rahmen der Push-Übertragung des Konfigurations-Snapshots als Ziel ausgewählt wurden.

   Beim Durchführen der Aktion **Wiederherstellen** können Sie auswählen, auf welchen Geräten der Vorgang ausgeführt werden soll.
8. **Betroffene Geräte** – Geräte, die seit der letzten Push-Konfigurationsübertragung geändert wurden. Bei „Betroffene Geräte“ werden nur Geräte berücksichtigt, die von der letzten Snapshot-Push-Übertragung betroffen waren.

   ***Betroffene Geräte und Zielgeräte***

   *Wenn Sie über zwei Geräte (A und B) verfügen und nur an Gerät A übertragen, wird A zum Ziel- und betroffenen Gerät.*

   *Wenn Sie dann erneut an Gerät A und B übertragen, sind A und B beide Zielgeräte, aber nur B ist ein betroffenes Gerät.*

   Beim Ausführen der Aktion **Laden** sind die aufgelisteten Geräte betroffen.
9. **Beschreibung** – Hier finden Sie alle Informationen, die zum Zeitpunkt der Push-Übertragung der Konfiguration bereitgestellt wurden.
10. **Aktualisieren** – Aktualisieren Sie die Informationen in der Snapshot-Tabelle.
11. **Filter zurücksetzen** – Löschen Sie alle Filter, um alle Konfigurationsversionen anzuzeigen.
12. **Vergleichen** – Sehen Sie, was sich von Version zu Version geändert hat.

    Sie können immer nur zwei Versionen gleichzeitig vergleichen.

13. **Aktionen** – Sie können eine Konfigurationsversion **wiederherstellen** oder **laden**.

- **Wiederherstellen** – stellt eine frühere Konfigurationsversion wieder her.

  Durch das Wiederherstellen einer Konfigurationsversion wird die laufende Konfiguration in den Bereitstellungen im Rahmen des ursprünglichen Pushs direkt aktualisiert und Sie müssen nicht **Konfiguration übertragen** auswählen.

  Stellen Sie alle Geräte oder Bereitstellungen im ursprünglichen Umfang der Konfigurationsübertragung wieder her oder wählen Sie bestimmte Geräte oder Bereitstellungen zur Wiederherstellung aus. Sie können die Konfiguration nicht erweitern, um Geräte oder Bereitstellungen außerhalb des ursprünglichen Umfangs einzuschließen.

  Durch das Wiederherstellen einer Konfigurationsversion wird die Kandidatenkonfiguration weder gelöscht noch geändert. Die laufende Konfiguration wird gespeichert. Durch das Wiederherstellen einer Konfiguration wird lediglich die laufende Konfigurationsversion aktualisiert. Bei Verwendung der Wiederherstellungsaktion scheinen Bereitstellungen möglicherweise nicht synchron zu sein.
- **Laden** – Laden Sie eine frühere Version als Kandidatenkonfiguration in Strata Cloud Manager. Ihre aktuelle Kandidatenkonfiguration geht verloren, wenn eine ältere Konfiguration geladen wird.

  Nehmen Sie Aktualisierungen an der neuen Kandidatenkonfiguration vor oder wenden Sie die Konfiguration auf neue Geräte und Bereitstellungen außerhalb des ursprünglichen Konfigurations-Snapshots an und führen Sie **Konfiguration übertragen** aus, wenn Sie bereit sind.
- **Speichern** – Speichern Sie die Kandidatenkonfiguration als benannten Snapshot, um sie als bekannte Konfiguration zu verwenden. Mit einer bekannten Konfiguration können Sie Ihre Bereitstellungen problemlos in einen bekannten und funktionsfähigen Zustand versetzen. Sie können zwischen Ihren **benannten Snapshots** und den automatisch protokollierten Konfigurationsübertragungen in **Versions-Snapshots** hin- und herschalten.

*Strata Cloud Manager speichert bis zu 6 Monate an Snapshots bzw. 200 einzelne Snapshots.*

## Speichern eines benannten Snapshots

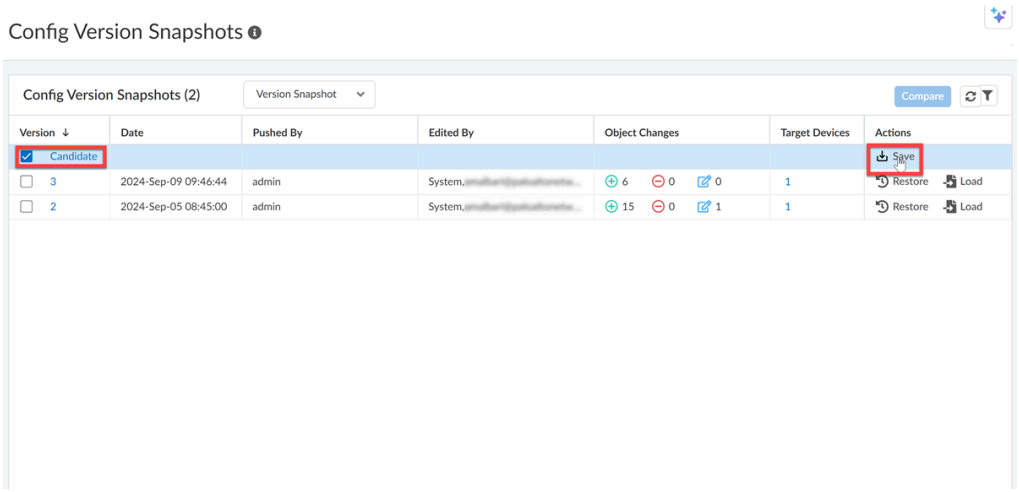
Speichern Sie den aktuellen Konfigurationskandidaten als benannten Snapshot. Sie können eine Teilkonfiguration nicht als benannten Snapshot speichern. Durch das Speichern eines benannten Snapshots können Sie einen bekannten Konfigurationsstatus laden, ohne einzelne Snapshots verfolgen zu müssen, die letztendlich aus der Snapshot-Tabelle der Konfigurationsversionen gelöscht werden.

**STEP 1 |** Melden Sie sich bei Strata Cloud Manager an.

**STEP 2 |** Wählen Sie **Verwalten** > **Vorgänge** > **Snapshots der Konfigurationsversion**.

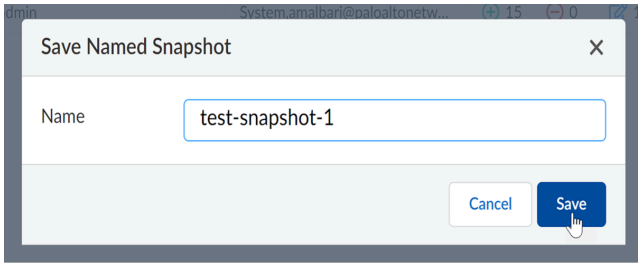
**STEP 3 |** Wählen Sie den **Kandidaten** aus.




**STEP 4 |** Klicken Sie auf **Save (Speichern)**.

**STEP 5 |** Geben Sie einen **Namen** mit maximal 64 Zeichen ein.

Der Name für den Snapshot lautet standardmäßig **config_[Jahr]-[Monat]-[Tag]-[Zeitstempel]**.



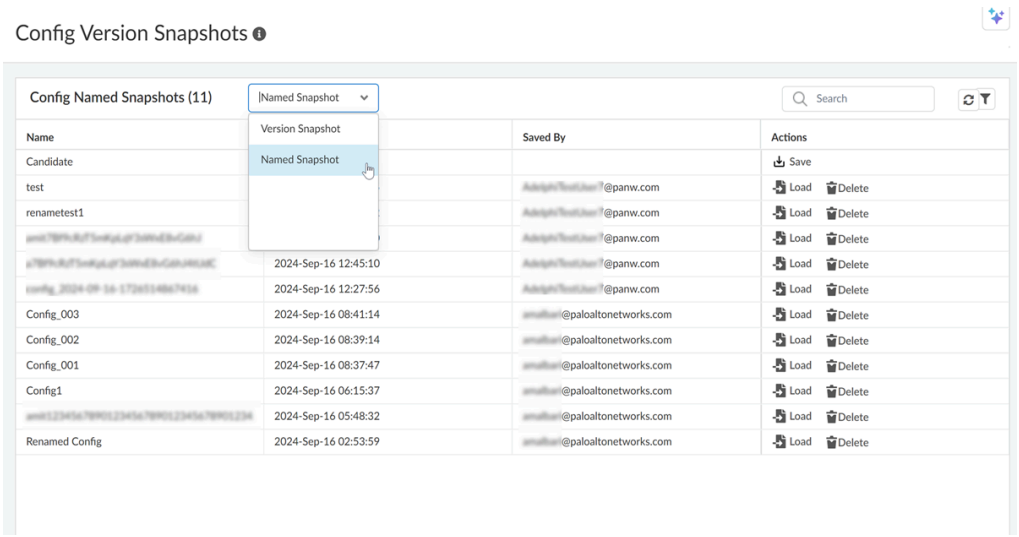

**STEP 6 |** **Speichern** Sie Ihren Snapshot.

**STEP 7 |** (Optional) Überprüfen Sie, ob Ihr Snapshot gespeichert wurde, indem Sie zu **Benannte Snapshots** in der Tabelle der Konfigurationsversions-Snapshots navigieren.

***Verwalten benannter Snapshots***

*Administratoren können ihre eigenen benannten Snapshots löschen. Superuser können alle benannten Snapshots löschen.*




# Wiederherstellen eines Snapshots

Stellen Sie eine zuvor übertragene Konfiguration wieder her. Durch das Wiederherstellen einer älteren Konfiguration wird die in den Bereitstellungen und Geräten ausgeführte Konfiguration aktualisiert. Diese Änderungen werden nicht in Strata Cloud Manager widergespiegelt, daher scheinen Bereitstellungen und Geräte möglicherweise nicht synchron zu sein.

Nur konfigurierte Geräte im Rahmen der ursprünglichen Push-Konfigurationsübertragung können auf eine ausgewählte Version wiederhergestellt werden.

**STEP 1 |** Melden Sie sich bei Strata Cloud Manager an.

**STEP 2 |** Wählen Sie **Verwalten** > **Vorgänge** > **Snapshots der Konfigurationsversion**.

**STEP 3 |** Wählen Sie die Konfigurationsversion aus, die Sie wiederherstellen möchten.

1. (Optional) Wählen Sie die Versionsnummer aus, um die durch den Konfigurations-Snapshot vorgenommenen Änderungen zu überprüfen.

**STEP 4 |** Wählen Sie **Wiederherstellen** aus.

1. (Optional) Wählen Sie die Geräte aus, auf die die Wiederherstellungsaktion abzielen soll.
2. Wählen Sie **Wiederherstellen** aus.

**STEP 5 |** (Optional) Wählen Sie **Verwalten** > **Konfiguration** > **Vorgänge** > **Konfiguration übertragen** aus, um zu bestätigen, dass die Konfiguration wiederhergestellt wurde.

# Laden eines Snapshots

Laden Sie einen früheren Konfigurations-Snapshot, um ihn als Kandidatenkonfiguration zu verwenden.

Nachdem die Konfiguration geladen wurde, können Sie vor der Push-Übertragung weiterhin Änderungen daran vornehmen.

**STEP 1 |** Melden Sie sich bei Strata Cloud Manager an.

**STEP 2 |** Wählen Sie **Verwalten** > **Vorgänge** > **Snapshots der Konfigurationsversion**.

**STEP 3 |** Wählen Sie die Konfigurationsversion aus, die Sie laden möchten.

1. (Optional) Wählen Sie die Versionsnummer aus, um die durch den Konfigurations-Snapshot vorgenommenen Änderungen zu überprüfen.

**STEP 4 |** **Laden** Sie die Version.

**STEP 5 |** (Optional) Ändern Sie den geladenen Konfigurationskandidaten nach Bedarf.

**STEP 6 |** Wählen Sie **Konfiguration übertragen** aus.

# Verwalten: Sicherheitsstatus

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)*<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | ❑ Mindestens eine dieser Lizenzen ist erforderlich, um Ihre Konfiguration mit Strata Cloud Manager zu verwalten; für die einheitliche Verwaltung von NGFWs und Prisma Access benötigen Sie Folgendes:<br>❑ Prisma Access-Lizenz<br>❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>❑ Strata Cloud Manager Essentials<br>❑ Strata Cloud Manager Pro<br>→ Die Ihnen zur Verfügung stehenden Funktionen und Fähigkeiten in Strata Cloud Manager hängen davon ab, welche Lizenz(en) Sie verwenden. |

Verwenden Sie diese Tools, um Ihren Sicherheitsstatus zu verbessern und sicherzustellen, dass Sie vor Bedrohungen geschützt sind, indem Sie die Best Practices für Sicherheitsrichtlinien befolgen.

- Passen Sie Sicherheitsstatusprüfungen für Ihre Bereitstellung an, um relevante Empfehlungen in Verwalten: Einstellungen für den Sicherheitsstatus zu maximieren.
- Verwenden Sie die Konfigurationsbereinigung, um nicht verwendete Konfigurationsobjekte und Richtlinienregeln zu identifizieren und zu entfernen.
- Konfigurieren Sie Compliance-Prüfungen, um unverhältnismäßig tolerante Sicherheitsregeln zu verfeinern und zu optimieren, sodass nur Anwendungen zugelassen werden, die in Ihrem Netzwerk tatsächlich verwendet werden.
- Erstellen Sie Ihre eigenen Verwalten: Einstellungen für den Sicherheitsstatus – Passen Sie vorhandene Best-Practice-Überprüfungen an und erstellen und verwalten Sie spezielle Ausnahmen, um eine bessere Anpassung an die Geschäftsanforderungen Ihres Unternehmens zu gewährleisten.
- Verwenden Sie die Richtlinienanalyse, um schnell sicherzustellen, dass die Aktualisierungen Ihrer Sicherheitsrichtlinienregeln Ihren Anforderungen entsprechen und keine Fehler oder Fehlkonfigurationen verursachen (z. B. Änderungen, die zu doppelten oder widersprüchlichen Regeln führen).

# Verwalten: Richtlinienanalyse

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • NGFW (von Panorama verwaltet)<br>• VM-Series, funded with Software NGFW Credits (von Panorama verwaltet)<br>• Prisma Access (Managed by Panorama) | ❑ Es wird mindestens eine der folgenden Lizenzen benötigt:<br>❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>❑ Strata Cloud Manager Pro<br>❑ Panorama CloudConnector-Plug-in für von Panorama verwaltete Bereitstellungen |

Aktualisierungen Ihrer Sicherheitsrichtlinienregeln sind häufig zeitkritisch und erfordern schnelles Handeln. Sie möchten jedoch sicherstellen, dass alle Aktualisierungen Ihres Regelsatzes für die Sicherheitsrichtlinien Ihren Anforderungen entsprechen und keine Fehler oder Fehlkonfigurationen verursachen (z. B. Änderungen, die zu doppelten oder widersprüchlichen Regeln führen).

Hierzu ermöglicht Ihnen die Richtlinienanalyse in Strata Cloud Manager die Optimierung von Zeit und Ressourcen bei der Implementierung einer Änderungsanforderung. Die Richtlinienanalyse dient nicht nur dem Analysieren und Bereitstellen von Vorschlägen für eine mögliche Konsolidierung oder Entfernung bestimmter Regeln, um Ihren Absichten zu entsprechen, sondern sucht in Ihrem Regelsatz auch nach Anomalien wie Schatten, Redundanzen, Verallgemeinerungen, Korrelationen und Konsolidierungen.

Verwenden Sie die Richtlinienanalyse, um den Regelsatz Ihrer Sicherheitsrichtlinien zu ergänzen oder zu optimieren.

- **Vor dem Hinzufügen einer neuen Regel** – Prüfen Sie, ob neue Regeln hinzugefügt werden müssen. Die Richtlinienanalyse empfiehlt, wie Sie Ihre vorhandenen Sicherheitsrichtlinienregeln am besten ändern, um Ihre Anforderungen zu erfüllen und, sofern möglich, eine weitere Regel hinzuzufügen.
- **Optimierung Ihres vorhandenen Regelsatzes** – Finden Sie heraus, wo Sie Ihre Regeln aktualisieren können, um eine aufgeblähte Struktur zu vermeiden, Konflikte zu vermeiden und sicherzustellen, dass die Datenverkehrsüberwachung mit der Absicht Ihres Regelsatzes für die Sicherheitsrichtlinien übereinstimmt.

Analysieren Sie Ihre Sicherheitsrichtlinienregeln sowohl vor als auch nach dem Durchführen eines Commits für Ihre Änderungen.

- **Richtlinienanalyse vor Änderung** – ermöglicht es Ihnen, die Auswirkung einer neuen Regel zu bewerten und die Absicht der neuen Regeln im Vergleich zu den bereits vorhandenen Regeln zu analysieren, um Empfehlungen zu geben, wie die Absicht am besten erreicht werden kann.
- **Richtlinienanalyse nach Änderung** – ermöglicht es Ihnen, den vorhandenen Regelsatz zu bereinigen, indem Sie Schatten, Redundanzen und andere Anomalien identifizieren, die sich im Laufe der Zeit angesammelt haben.

Weitere Informationen finden Sie unter Richtlinienanalyse.

# Verwalten: Richtlinienoptimierer

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access<br><br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)*<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | ❑ Mindestens eine dieser Lizenzen ist erforderlich, um Ihre Konfiguration mit Strata Cloud Manager zu verwalten; für die einheitliche Verwaltung von NGFWs und Prisma Access benötigen Sie Folgendes:<br>❑ Prisma Access-Lizenz<br>❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>❑ Strata Cloud Manager Pro<br><br>→ Die Ihnen zur Verfügung stehenden Funktionen und Fähigkeiten in Strata Cloud Manager hängen davon ab, welche Lizenz(en) Sie verwenden. |

*Testen Sie den Policy Optimizer (Richtlinienoptimierer), solange er als Early-Access-Version verfügbar ist. Wenn Sie diese Funktion auch nach Ablauf des Early-Access-Zeitraums weiter nutzen möchten, wenden Sie sich an Ihr Account-Team.*

Zu weit gefasste Regeln führen zu Sicherheitslücken, da sie Anwendungen zulassen, die in Ihrem Netzwerk nicht verwendet werden. Mit der Richtlinienoptimierung können Sie diese unverhältnismäßig toleranten Regeln in spezifischere, fokussiertere Regeln umwandeln, die nur die Anwendungen zulassen, die Sie tatsächlich verwenden.

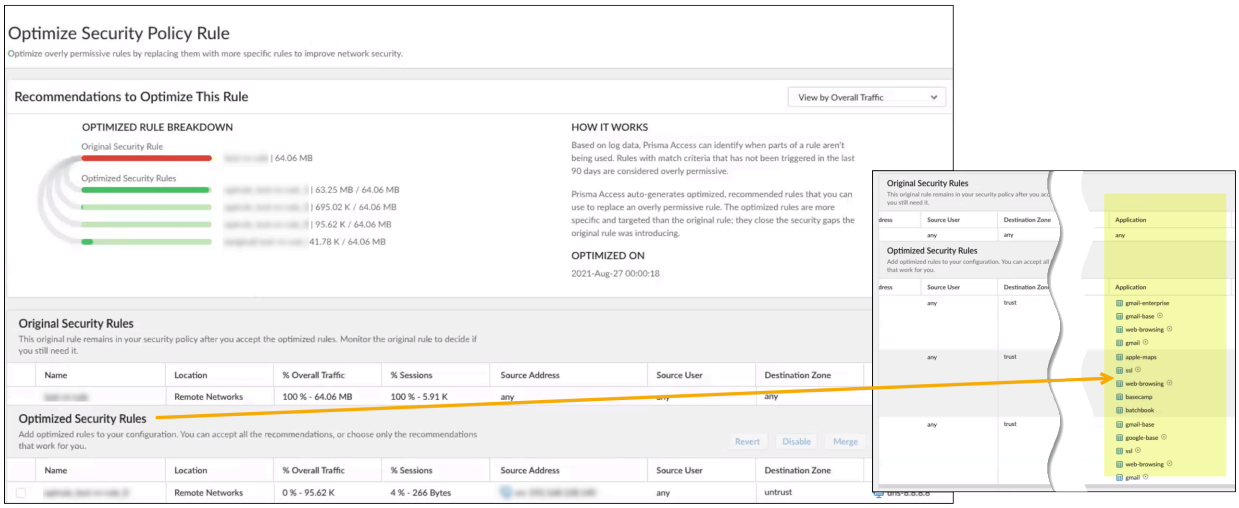
Für die Richtlinienoptimierung werden nur Regeln berücksichtigt, die länger als 90 Tage in der Vergangenheit erstellt wurden.

## Funktionsweise

Strata Cloud Manager analysiert Protokolldaten und kategorisiert Regeln als unverhältnismäßig tolerant, wenn sie **beliebigen** Anwendungsverkehr zulassen. Die Regeln müssen mindestens 90 Tage alt sein. Diese Regeln können Sicherheitslücken schaffen, wenn dadurch Datenverkehr zugelassen wird, der für die Verwendung im Unternehmen nicht erforderlich ist.

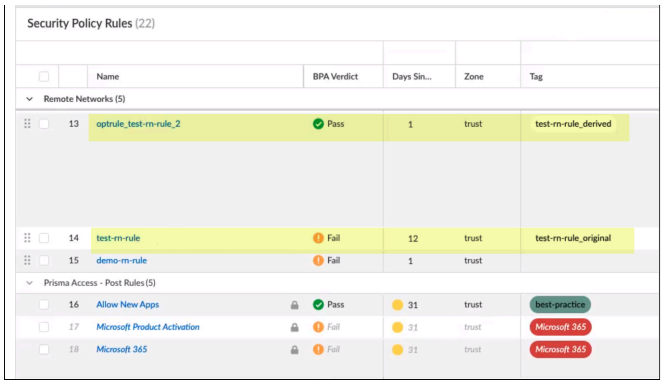
Bei Regeln, die als unverhältnismäßig tolerant identifiziert werden, generiert Strata Cloud Manager automatisch Empfehlungen, die Sie akzeptieren können, um die Regel zu optimieren. Die neuen, empfohlenen Regeln sind spezifischer und zielgerichteter als die ursprüngliche Regel; sie erlauben explizit nur die Anwendungen, die in den letzten 90 Tagen in Ihrem Netzwerk erkannt wurden.

Wählen Sie eine unverhältnismäßig tolerante Regel aus, um Optimierungsempfehlungen zu überprüfen, anzupassen und zu akzeptieren. Wenn Sie diese Regeln durch die spezifischeren, empfohlenen Regeln ersetzen, sorgen Sie für eine Stärkung Ihres Sicherheitsstatus.




Das Akzeptieren von Empfehlungen zur Optimierung einer Regel hebt die ursprüngliche Regel nicht auf. Die ursprüngliche Regel bleibt unterhalb der neuen Regeln in Ihrer Sicherheitsrichtlinie aufgeführt; so können Sie die Regel überwachen und sie entfernen, wenn Sie sicher sind, dass sie nicht benötigt wird.

Sowohl die ursprüngliche Regel als auch die optimierten Regeln werden mit Tags versehen, damit Sie sie in Ihrer Sicherheitsrichtlinie leicht identifizieren können:




# Optimieren einer Regel

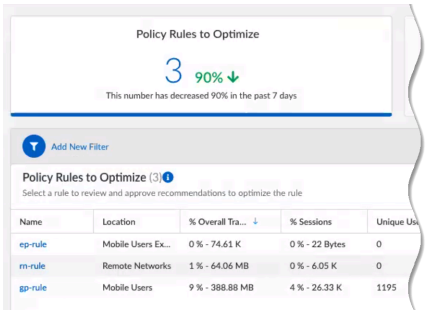
**STEP 1 |** Besuchen Sie die **Konfigurationsbereinigung**, um zu sehen, ob es Regeln gibt, die Sie optimieren können.

Gehen Sie zu **Verwalten** > **Sicherheitsstatus** > **Richtlinienoptimierer**.

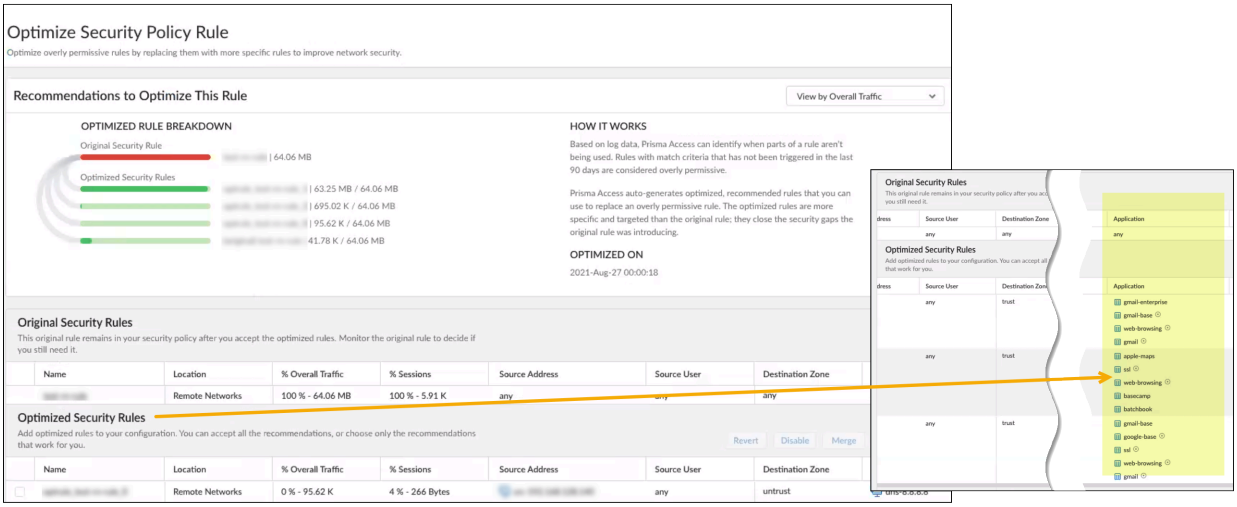
**STEP 2 |** Überprüfen Sie unverhältnismäßig tolerante Regeln und wählen Sie eine Regel, um die Optimierungsempfehlungen anzuzeigen.

Wenn es mehrere unverhältnismäßig tolerante Regeln gibt, konzentrieren Sie sich darauf, die Regeln zu optimieren, die den meisten Datenverkehr beeinflussen; so können Sie bei der Stärkung Ihrer Sicherheit die größten Vorteile erzielen.




**STEP 3 |** Überprüfen Sie die empfohlenen, optimierten Regeln.

Sie können sehen, wie viel Datenverkehr der ursprünglichen Regel jede neue Regel abdecken wird. Beachten Sie die spezifischen Anwendungen, die jede neue Regel abdeckt.



**STEP 4 |** Akzeptieren Sie einige oder alle Regelempfehlungen.

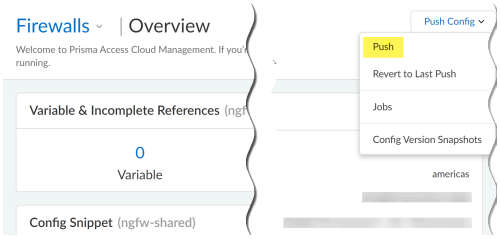
Die Annahme der neuen, optimierten Regeln fügt die Regeln zu Ihrem Regelsatz hinzu. Sie sind noch nicht aktiv; das passiert im nächsten Schritt, wenn Sie die Konfiguration per **Konfiguration übertragen** an Prisma Access übertragen.

Über **Alle akzeptieren** akzeptieren Sie die empfohlenen Regeln im aktuellen Zustand. Sie können auch Änderungen vornehmen, bevor Sie die optimierten Regeln akzeptieren:

- Entfernen Sie eine Regel aus der Optimierung. Fügen Sie diese Regel zu einer Liste von Regeln hinzu, die Sie von der Optimierung ausschließen möchten (dieses Mal und in Zukunft).
- Deaktivieren Sie eine optimierte Regel. Dies bedeutet, dass Sie diese Regel nicht akzeptieren und sie nicht zum Regelsatz hinzugefügt wird.
- Machen Sie alle Änderungen rückgängig. Dadurch werden alle Änderungen, die Sie vorgenommen haben, rückgängig gemacht und die Regeln wieder auf die Empfehlungen zurückgesetzt.
- Führen Sie Regeln zusammen. Sie können sich hierzu entscheiden, wenn sich die empfohlenen Regeln ähneln.

Nachdem Sie die optimierten Regeln akzeptiert haben, werden Sie aufgefordert, den **Regelsatz zu aktualisieren**. Wenn Sie zustimmen, werden die optimierten Regeln zu Ihrer Sicherheitsrichtlinie hinzugefügt. Allerdings werden sie noch nicht im Datenverkehr durchgesetzt.

**STEP 5 |** Über **Konfiguration übertragen** können Sie die Konfigurationsupdates an Prisma Access senden und die optimierten Regeln durchsetzen.

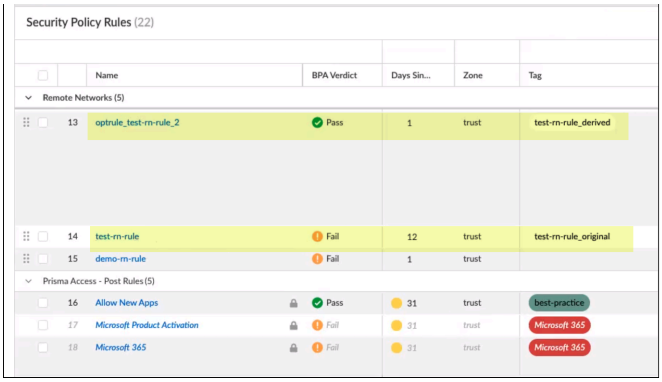



**STEP 6 |** Überwachen Sie die ursprüngliche Regel, bis Sie sicher sind, dass Sie sie nicht mehr benötigen.

Die ursprünglichen unverhältnismäßig toleranten Regeln verbleiben in Ihrer Sicherheitsrichtlinie; sie sind unterhalb der optimierten Regeln in Ihrem Regelsatz aufgeführt

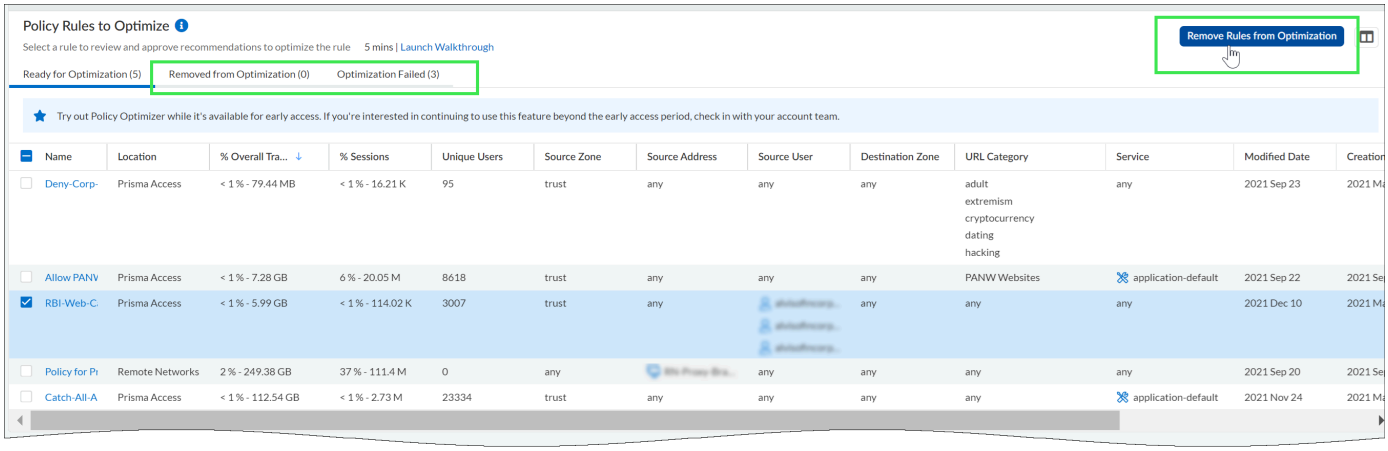
 

und werden mit Tags versehen, damit Sie sie leicht identifizieren können. Der Tagname hängt „_original“ an den Regelnamen an (z. B. „Sicherheitsregelname_original“).




## Ausschließen einer Regel von der Optimierung

Verschieben Sie eine Regel in die Liste **Von Optimierung ausgeschlossen**, wodurch Prisma Access sie nicht optimiert. Die Regeleinstellungen bleiben wie gehabt.



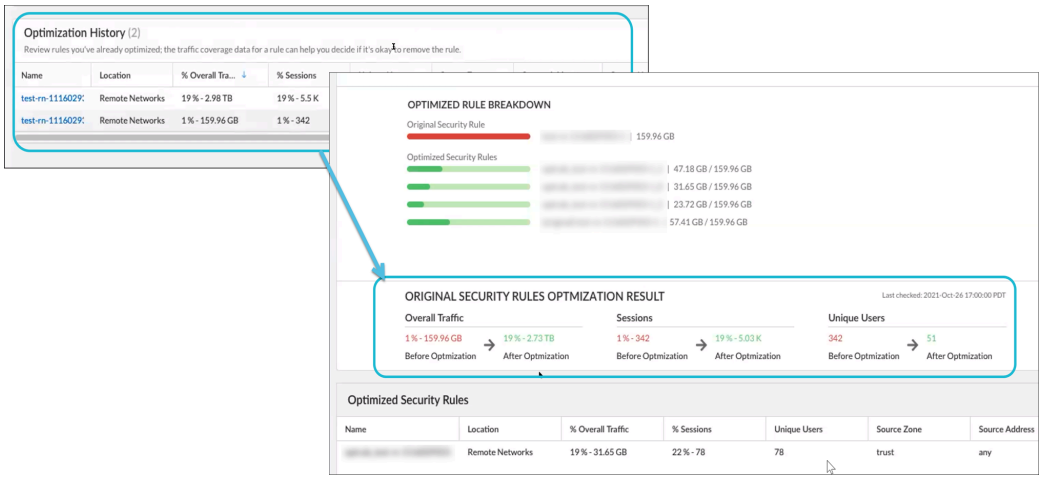

Stellen Sie sicher, dass Sie **Konfiguration übertragen** auswählen, nachdem Sie eine Regel in die Ausschlussliste verschoben haben. Nach der Übertragung der Konfiguration kann es bis zu 24 Stunden dauern, bis die Regel in der Liste angezeigt wird. Sie können die Regel jederzeit wieder zur Optimierungsliste hinzufügen.

## Nachverfolgen von Optimierungsergebnissen

Die Richtlinienoptimierung zeigt einen Verlauf der von Ihnen optimierten Sicherheitsregeln. Verlaufsdaten beinhalten die Optimierungsergebnisse: Vergleichen Sie die Datenverkehrsabdeckung der ursprünglichen Regel mit den optimierten Regeln.

Die Daten, die Sie für den **Verlauf der Richtlinienoptimierung** sehen, beziehen sich auf die letzten 30 Tage. Wenn eine ursprüngliche Regel (eine von Ihnen optimierte Regel) sechs Monate lang keine Treffer auslöst, wird sie aus dem Richtlinienoptimierungsverlauf entfernt und stattdessen als Richtlinienregel mit null Treffern klassifiziert.



# Verwalten: Konfigurationsbereinigung

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access<br><br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)*<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | ❑ Mindestens eine dieser Lizenzen ist erforderlich, um Ihre Konfiguration mit Strata Cloud Manager zu verwalten; für die einheitliche Verwaltung von NGFWs und Prisma Access benötigen Sie Folgendes:<br>❑ Prisma Access-Lizenz<br>❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>❑ Strata Cloud Manager Pro<br><br>→ Die Ihnen zur Verfügung stehenden Funktionen und Fähigkeiten in Strata Cloud Manager hängen davon ab, welche Lizenz(en) Sie verwenden. |

Verwenden Sie die Konfigurationsbereinigung, um nicht verwendete Konfigurationsobjekte und Richtlinienregeln zu identifizieren und aus Ihrer Strata Cloud Manager-Konfiguration zu entfernen. Durch das Entfernen nicht verwendeter Konfigurationsobjekte wird die Firewallverwaltung vereinfacht, da hierdurch Unordnung vermieden wird und nur die Konfigurationsobjekte erhalten bleiben, die zur Durchsetzung der Sicherheit erforderlich sind.

**STEP 1 |** Melden Sie sich bei Strata Cloud Manager an.

**STEP 2 |** Wählen Sie **Verwalten** > **Sicherheitsstatus** > **Konfigurationsbereinigung** aus.

**STEP 3 |** Wählen Sie die ungenutzten Objekte und Richtlinienregeln in Ihrer gesamten Strata Cloud Manager-Konfiguration der letzten 6 Monate.

- **Zu optimierende Richtlinienregeln** – Klicken Sie hierauf, um die Richtlinienregeln zu überprüfen, die unverhältnismäßig tolerant sind, und sie in spezifischere, fokussiertere Regeln umzuwandeln, die nur die Anwendungen zulassen, die Sie tatsächlich verwenden.
- **Nicht verwendete Objekte (letzte 6 Monate)** – alle Konfigurationsobjekte, die in den letzten 6 Monaten in keiner Konfiguration oder Richtlinienregel verwendet wurden.
- **Objekte mit null Treffern (letzte 6 Monate)** – Richtlinienregeln mit Konfigurationsobjekten, bei denen das Konfigurationsobjekt in der Richtlinienregel null Treffer erhält.

  Für die hier aufgelisteten Konfigurationsobjekte wurden nur in den Richtlinienregeln, denen sie zugeordnet sind, null Treffer erzielt. Ihre Verwendung kann zu Treffern in den anderen Richtlinienregeln führen, in denen sie verwendet werden.
- **Regeln mit null Treffern (letzte 6 Monate)** – alle Richtlinienregeln, für die es in den letzten 6 Monaten keine Übereinstimmungen im Datenverkehr gab.

**STEP 4 |** Wenden Sie zusätzliche Filter an, um bestimmte, nicht verwendete Objekte und Richtlinienregeln zu finden.

**Neuen Filter hinzufügen** wird für **Nicht verwendete Objekte (letzte 6 Monate)** und **Richtlinienregeln mit null Treffern (letzte 6 Monate)** unterstützt.

- **Nicht verwendete Objekte (letzte 6 Monate)** – Sie können ungenutzte Objekte basierend auf Folgendem filtern und **löschen**:
  - **Name** – Suchen Sie nach einem bestimmten Konfigurationsobjektnamen und wählen Sie ihn aus.
  - **Standort** – Konfigurationsumfang, in dem der Konfigurationsobjektname erstellt wurde.
  - **Objekttyp** – Konfigurationsobjekttyp.
  - **Tage ohne Verwendung** – die Anzahl der Tage, an denen das Konfigurationsobjekt nicht verwendet wurde.
    - **< 50** – weniger als 50 Tage ungenutzt.
    - **>= 50, <= 100** – zwischen 50 und 100 Tagen ungenutzt.
    - **> 100** – mehr als 100 Tage ungenutzt.
- **Richtlinienregeln mit null Treffern (letzte 6 Monate)** – Sie können Richtlinienregeln mit null Treffern basierend auf **Name**, **Tage mit null Treffern** oder `Quell`- und `Ziel`-Daten filtern und **aktivieren**, **deaktivieren** oder **löschen**.

# Verwalten: Einstellungen für den Sicherheitsstatus

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden<br>• Prisma Access (Managed by Panorama or Strata Cloud Manager)<br>• Prisma SD-WAN | Jede dieser Lizenzen beinhaltet den Zugriff auf Strata Cloud Manager:<br>❑ Prisma Access<br>❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>❑ Prisma SD-WAN<br>❑ Strata Cloud Manager Essentials<br>❑ Strata Cloud Manager Pro<br>→ Die Funktionen und Fähigkeiten, die Ihnen in Strata Cloud Manager zur Verfügung stehen, hängen davon ab, welche Lizenz(en) Sie verwenden. |

Strata Cloud Manager nutzt eine Reihe vordefinierter Best-Practice-Überprüfungen, die auf branchenspezifische Cybersicherheitskontrollen wie CIS (Center for Internet Security) und NIST (National Institute of Standards and Technology) abgestimmt sind, sowie benutzerdefinierte Prüfungen, die Sie basierend auf den spezifischen Anforderungen Ihrer Organisation erstellen. Bei diesen Prüfungen werden Konfigurationen und Einstellungen innerhalb der Cloud-Infrastruktur ausgewertet und Abweichungen von Best Practices oder Compliance-Anforderungen identifiziert.

Die Sicherheitsstatusprüfungen in Strata Cloud Manager umfassen eine Reihe von Sicherheitsbereichen, darunter Netzwerksicherheit, Datenschutz sowie Identitäts- und Zugriffsverwaltung. Diese Prüfungen bewerten Firewall-Regeln, Verschlüsselung, Authentifizierungsmechanismen und den allgemeinen Zustand der Konfigurationen.

Wenn bei Ihrer Konfiguration Abweichungen festgestellt werden, bietet Strata Cloud Manager aussagekräftige Erkenntnisse und Empfehlungen zur Behebung der Probleme. Außerdem kann die Lösung den Prozess zur Korrektur von Fehlkonfigurationen und nicht konformen Einstellungen teilweise automatisieren, damit Sie mit minimalem manuellen Eingriff eine sichere und konforme Cloud-Umgebung gewährleisten können.

Die Einstellungen für den Sicherheitsstatus vereinen die Funktionen der beiden Einstellungsseiten für die AIOps- und Strata Cloud Manager-Sicherheitsprüfung.

Wählen Sie **Verwalten** > **Sicherheitsstatus** > **Einstellungen** aus, um Sicherheitsstatusprüfungen für Ihre Bereitstellung anzuzeigen, zu verwalten und anzupassen. So können Sie relevante Empfehlungen maximieren.

- **Sicherheitsüberprüfungen** – Liste der Best-Practice-Überprüfungen, die zur Bewertung Ihrer Konfiguration verwendet werden.

  Ihre Konfiguration wird mit diesen Prüfungen verglichen, um den Sicherheitsstatus Ihrer Geräte zu bewerten und Sicherheitsbenachrichtigungen zu generieren. Sie können die folgenden Aktionen ausführen, um diese Prüfungen basierend auf Ihrer Umgebung zu verwalten:

  1. Legen Sie den Schweregrad für Ihre benutzerdefinierten Prüfungen fest, um die Prüfungen zu bestimmen, die für Ihre Bereitstellung am kritischsten sind.

     *Sie können den Schweregrad für Ihre benutzerdefinierten Prüfungen ändern, aber die Schweregrade für die Best-Practice-Überprüfungen von Palo Alto Networks sind festgelegt und können nicht geändert werden.*

  2. Erstellen und löschen Sie Ihre eigenen benutzerdefinierten Prüfungen, klonen und bearbeiten Sie vorhandene Prüfungen, um neue zu erstellen, und definieren Sie spezielle

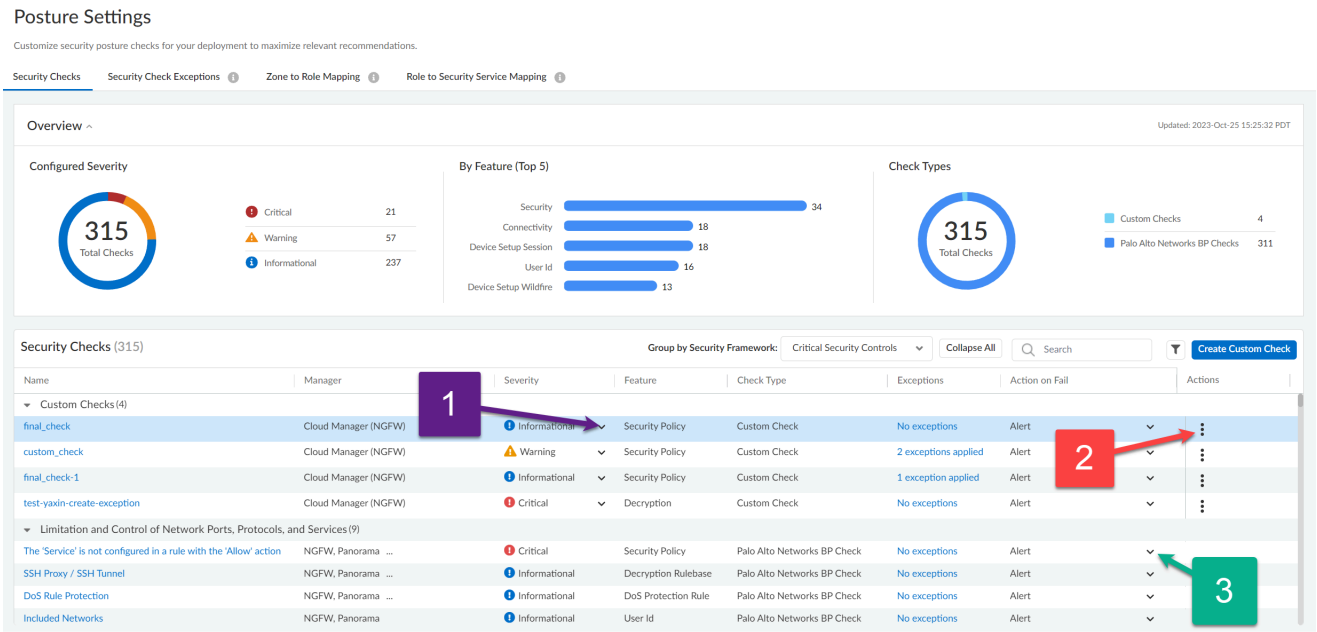
Ausnahmen für Prüfungen, die auf Teile Ihrer Bereitstellung nicht angewendet werden sollen.

*Bei der ersten Implementierung dieser Prüfungen können Sie Prüfungen klonen, die sich im benutzerdefinierten Prüfungsframework befinden.*

3. Legen Sie die Reaktion für den Fall einer fehlgeschlagenen Prüfung fest.
   - **Benachrichtigen** (Standard) – sendet eine Benachrichtigung für die fehlgeschlagene Prüfung.
   - **Blockieren** – stoppt potenzielle Fehlkonfigurationen, bevor diese in Ihre Bereitstellung gelangen. „Blockieren“ kann je nach Handhabung Folgendes bedeuten:
     - **Inline-Prüfungen in Strata Cloud Manager** – verhindert das Festschreiben oder Übertragen einer nicht konformen Konfiguration, hindert Sie jedoch nicht daran, Ihre Konfiguration lokal zu speichern.
     - **Echtzeit*-Inline-Prüfungen in Strata Cloud Manager** – verhindert, dass Sie eine nicht konforme Konfiguration überhaupt erst speichern.
     - **Von Panorama verwaltet**** – verhindert, dass Sie eine nicht konforme Konfiguration an Panorama übermitteln, hindert Sie jedoch nicht daran, sie in der Panorama-Kandidatenkonfiguration zu speichern.
     - PAN-OS-Webschnittstelle, API oder CLI-Verwaltung – „Blockieren“ hat keine erzwungene Auswirkung auf Konfigurationen, die weder von der Cloud noch von Panorama verwaltet werden.

     - ** Aufgrund ihrer logischen Komplexität werden einige Inline-Prüfungen asynchron nach einem festen Zeitplan, aber nicht in Echtzeit ausgeführt. Wenn bei einer Echtzeitprüfung Ihrer Konfiguration ein Fehler auftritt, können Sie diese Konfiguration speichern – nicht einmal lokal.*
     - *** Das Panorama CloudConnector-Plug-in ist erforderlich, um die Commit-Aktion „Blockieren“ in Panorama zu erzwingen.*




- **Ausnahmen von Sicherheitsüberprüfungen**

  Deaktivieren Sie einzelne Überprüfungen für von Ihnen angegebene Geräte oder Gerätegruppen.
- **Zone-zu-Rolle-Zuordnung**

  Ordnen Sie die Zonen in NGFWs Rollen zu, um benutzerdefinierte Empfehlungen zu erhalten.
- **Rolle-zu-Sicherheitsdienst-Zuordnung**

  Verwalten Sie die Sicherheitsdienste, die für den Datenverkehr zwischen Zonen und Rollen in allen NGFWs erforderlich sind.

## Erstellen einer benutzerdefinierten Prüfung

Erstellen Sie aus einer vorhandenen Prüfung Ihre eigene benutzerdefinierte Prüfung. Alternativ können Sie direkt mit Schritt 4 fortfahren, um eine benutzerdefinierte Prüfung von Grund auf neu zu erstellen.

**STEP 1 |** Wählen Sie **Verwalten** > **Sicherheitsstatus** > **Einstellungen** aus.

**STEP 2 |** Identifizieren Sie die Prüfung, die Sie klonen möchten, und klicken Sie auf **Klonen**.

**STEP 3 |** **Bearbeiten** Sie die geklonte Prüfung und fahren Sie mit Schritt 5 fort, um Ihre Änderungen vorzunehmen.

**STEP 4 |** Gehen Sie zu **Verwalten** > **Sicherheitsstatus** > **Einstellungen** und wählen Sie **Benutzerdefinierte Prüfung erstellen** aus.

**STEP 5 |** Geben Sie die **allgemeinen Informationen** für Ihre Prüfung an. Ihre benutzerdefinierte Prüfung muss einen **Namen** und eine **Beschreibung** aufweisen. Sie sollten jedoch auch eine **Empfehlung** und eine **Begründung** für Ihre Prüfung hinzufügen, damit andere die Absicht und die Best Practices für Ihre benutzerdefinierte Prüfung verstehen.

**STEP 6 |** (Optional) Wählen Sie einen **Objekttyp** aus – der Abschnitt Ihrer Konfiguration, für den Sie eine Prüfung erstellen, der bestimmt, welche **abzugleichenden Regeleigenschaften** Sie beim Erstellen Ihrer Prüfung auswählen können.

**STEP 7 |** Nutzen Sie den **Logikgenerator** für Ihre benutzerdefinierte Prüfung.

1. **Ausdruck hinzufügen** – Fügen Sie eine einzelne Logikzeile hinzu, die die Übereinstimmungskriterien für eine Konfiguration beschreibt.

| Abzugleichende Regeleigenschaften | Abgleichsoperator | Spezifische Kriterien |
|---|---|---|
| • Allgemein – Name, Beschreibung, Position und Zeitplan<br>• Quellen – Zonen, Adressen, Benutzer<br>• Ziele – Zonen und Adressen<br>• Anwendungen, Dienste und URLs<br>• Aktionen und erweiterte Inspektion | • Ist<br>• Ist nicht<br>• Ist leer<br>• Ist nicht leer<br>• Beginnt mit<br>• Endet mit<br>• Enthält<br>• Größer als<br>• In<br>• Ist gleich oder größer als<br>• Ist gleich oder kleiner als<br>• Kleiner als<br>• Gleich<br>• Nicht gleich<br>• Enthält nicht<br>• Alle von<br>• Einige von<br>• Keine von | [Textfeld] |

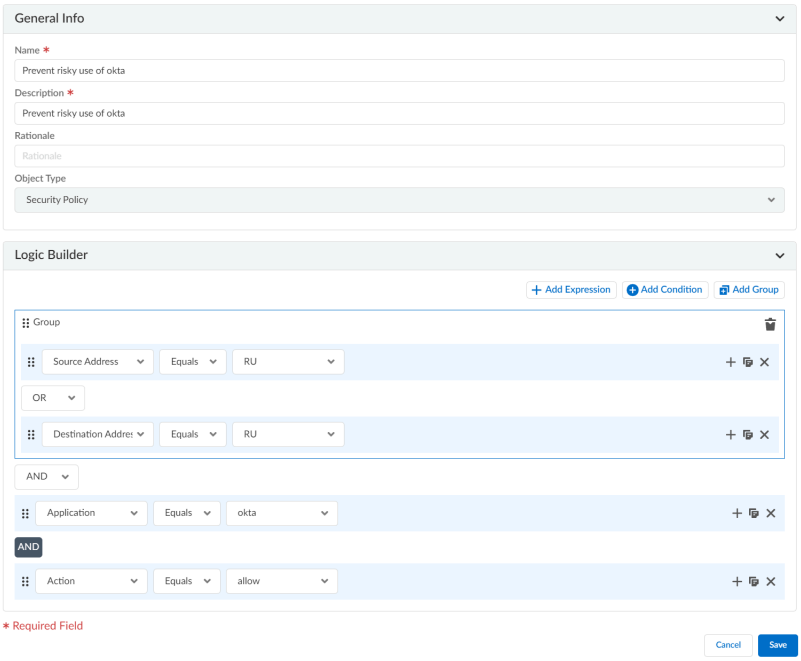
2. **Bedingung hinzufügen** – Verwenden Sie logische Operatoren (wie „AND“, „OR“, „IF“, „THEN“, „ELSE“ und „ELSE IF“), um Ausdrücke, zusätzliche Bedingungen und Gruppen zu verbinden oder zu kombinieren.
3. **Gruppe hinzufügen** – Erstellen Sie einen Satz von Ausdrücken, Bedingungen oder beidem. Zusammengenommen ergibt diese Gruppe eine Wahr-oder-falsch-Bedingung.

- + *Fügt einen neuen Ausdruck oder eine neue Bedingung hinzu.*
- *Klont einen Ausdruck oder eine Bedingung.*
- ✕ *Entfernt einen Ausdruck oder eine Bedingung.*

Der Ausdruck in diesem Beispiel gibt eine Warnung aus, wenn er Richtlinienregeln erkennt, die Okta-Datenverkehr von und zu russischen IP-Adressen zulassen. Das

Beispiel veranschaulicht lediglich die Funktionsweise des Logikgenerators und stellt keine Empfehlung dar.




**STEP 8 |** **Speichern** Sie Ihre Prüfung.

## Verwalten Ihrer Prüfungen

Sie können für Ihre Sicherheitsüberprüfungen die folgenden **Aktionen** ausführen:

- **Klonen*** – erstellt eine Kopie der Prüfung.
- **Bearbeiten**** – Nehmen Sie Änderungen an einer vorhandenen benutzerdefinierten Prüfung vor.
- **Löschen**** – entfernt eine von Ihnen erstellte benutzerdefinierte Prüfung.

Wählen Sie die Prüfungen aus, für die Sie eine Aktion ausführen möchten, und wählen Sie die entsprechende Aktion aus.

- ** Sie können jeweils nur eine Prüfung klonen.*
- *** Sie können nur benutzerdefinierte Prüfungen bearbeiten oder löschen.*
- *Zum Bearbeiten einer benutzerdefinierten Prüfung benötigen Sie möglicherweise die Berechtigung eines Administrators.*

## Erstellen einer Ausnahme für eine Prüfung

Bei Bedarf können Sie einschränken, wo in Ihrer Bereitstellung Prüfungen angewendet werden.

**STEP 1 |** Wählen Sie **Verwalten** > **Sicherheitsstatus** > **Einstellungen** > **Ausnahmen von Sicherheitsüberprüfungen**Sicherheitsüberprüfungsausnahme erstellen aus.

Wählen Sie alternativ **Verwalten** > **Sicherheitsstatus** > **Einstellungen** aus, identifizieren Sie die Prüfung, die Sie ausschließen möchten, und wählen Sie sie aus (Spalte **Ausnahmen**).

**STEP 2 |** Geben Sie die Informationen an, die Sie benötigen, um für Ihre Prüfung eine **Ausnahmeregel zu erstellen**. Geben Sie einen Namen, einen Grund sowie Bedingungen für Ihre Ausnahme an.

*Die Funktion **Sicherheitsüberprüfungsausnahme** ist derzeit nur auf Benachrichtigungen sowie die Dashboards **Best Practices** und **Einblicke in den Sicherheitsstatus** anwendbar.*

**STEP 3 |** (Optional) Fügen Sie eine **Ticketnummer** oder eine **Beschreibung** für Ihre Ausnahme hinzu, damit andere die Absicht und den Hintergrund Ihrer Ausnahme verstehen.

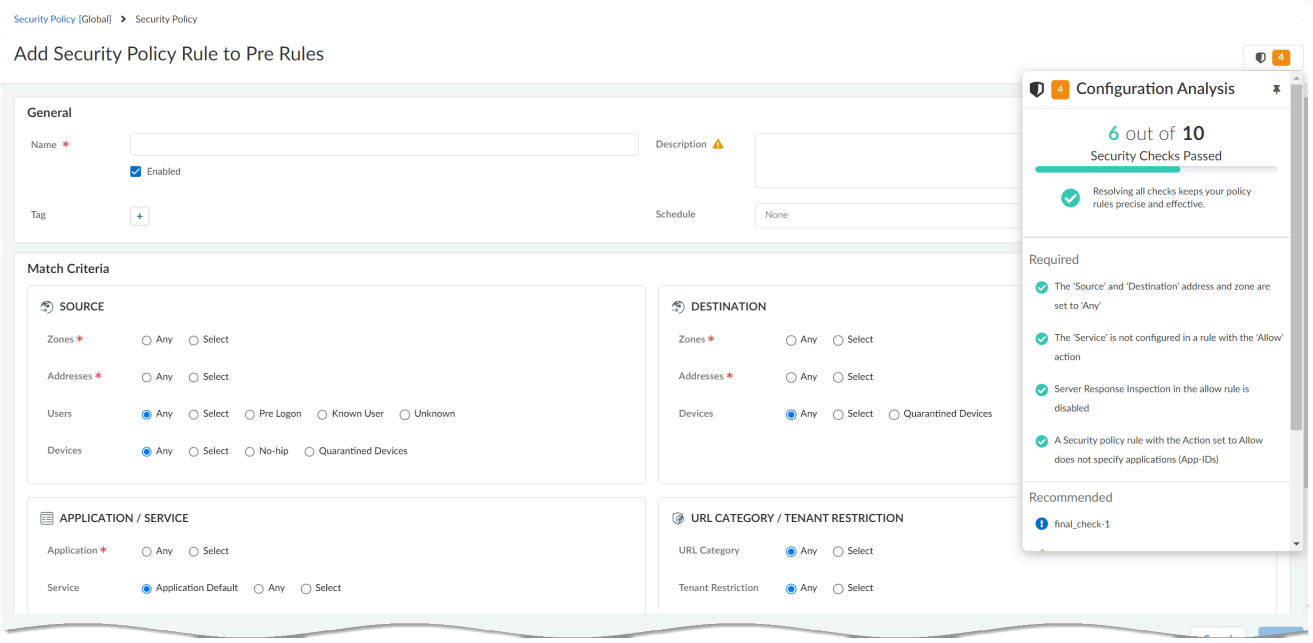
**STEP 4 |** **Speichern** Sie Ihre Ausnahme.

## Ihre Prüfungen in Aktion

Überprüfungen auf Feldebene zeigen Ihnen genau, wo Ihre Konfiguration nicht den Best Practices entspricht oder eine benutzerdefinierte Prüfung nicht besteht. Die Prüfungen bieten eine Inline-Anleitung zu Best Practices, mit der Sie sofort Maßnahmen ergreifen können.

Darüber hinaus können Sie Sicherheitsprüfungen von jedem Ort aus einsehen und verwalten.

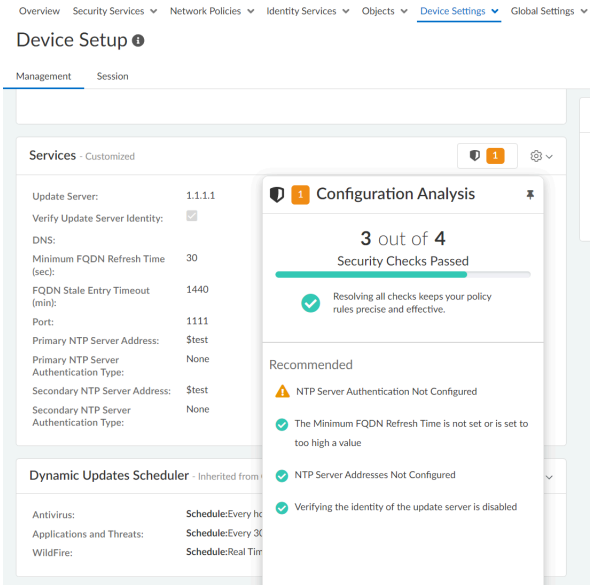
- Richtlinienregeln erstellen und verwalten – Mit Sicherheitsrichtlinienregeln können Sie Regeln durchsetzen und Maßnahmen ergreifen; sie können so allgemein oder spezifisch sein wie nötig. (**Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Sicherheitsdienste** > **Sicherheitsrichtlinie**)




- Geräte einrichten – Konfigurieren Sie Dienstrouten, Verbindungseinstellungen, zulässige Dienste und Einstellungen für den Administratorzugriff für die Verwaltungs- und

Hilfsschnittstellen für Ihre Firewalls. (**Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Geräteeinstellungen** > **Geräteeinrichtung**)




Wenn die Konfiguration, die Sie speichern möchten, Ihre Kriterien nicht erfüllt, haben Sie die Möglichkeit, das Problem zu beheben oder die Warnung zu überschreiben* und Ihre Änderungen trotzdem zu speichern.

- ** Die Überschreibungsberechtigung wird durch die rollenbasierte Zugriffssteuerung (RBAC) geregelt und muss für Ihre Rolle aktiviert sein, damit diese Option angezeigt wird. Aktionen im Zusammenhang mit Überschreibungen, benutzerdefinierten Prüfungen und Ausnahmen werden in Auditierungslogs protokolliert:* ***Vorfälle und BenachrichtigungenProtokoll-ViewerAudit (Protokolltyp)****.*
- *Alles, was Sie mit benutzerdefinierten Prüfungen, Überschreibungen und Ausnahmen tun, wird im Audit protokolliert:* ***Vorfälle und Benachrichtigungen*** *>* ***Protokoll-Viewer*** *>* ***Audit (Protokolltyp)****.*

# Verwalten: Zugriffssteuerung

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)*<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | ❑ Mindestens eine dieser Lizenzen ist erforderlich, um Ihre Konfiguration mit Strata Cloud Manager zu verwalten; für die einheitliche Verwaltung von NGFWs und Prisma Access benötigen Sie Folgendes:<br>❑ Prisma Access-Lizenz<br>❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>❑ Strata Cloud Manager Pro<br>❑ Software-NGFW-Credits<br>*(für VM-Series-Software-NGFWs)*<br>→ Die Ihnen zur Verfügung stehenden Funktionen und Fähigkeiten in Strata Cloud Manager hängen davon ab, welche Lizenz(en) Sie verwenden. |

Mithilfe der rollenbasierten Zugriffssteuerung (Role-Based Access Control, RBAC) können Sie die Berechtigungen und Verantwortlichkeiten administrativer Benutzer (Administratoren) definieren. Jeder Administrator muss über ein Benutzerkonto verfügen, für das eine Rolle und eine Authentifizierungsmethode angegeben sind. Prisma Access Cloud Management implementiert eine benutzerdefinierte RBAC, mit der Sie Rollen oder spezifische Berechtigungen verwalten und administrativen Benutzern Zugriffsrechte zuweisen können. Mit RBAC können Sie Benutzer und deren Zugriff auf verschiedene Ressourcen innerhalb von Cloud Management verwalten.

*RBAC wird für SaaS Security Inline und Verhaltensbedrohungen nicht unterstützt. Alle Registerkarten unter **Erkannte Anwendungen** und **Verhaltensbedrohungen** sind für alle Benutzer sichtbar, unabhängig von ihren zugewiesenen Rollen.*

***WEITERE RBAC-RESSOURCEN***

- Wer kann „Allgemeine Dienste: Identität und Zugriff“ nutzen: Cloud-verwaltetes Prisma Access
- Wie sieht der allgemeine Ablauf für „Allgemeine Dienste: Identität und Zugriff“ aus?
- Informationen zu Rollen und Berechtigungen über allgemeine Dienste

# Administratorrollen

Ein Benutzer in Prisma Access ist eine Person, der Administratorrechte zugewiesen wurden; hierbei definiert die Rolle die Art des Zugriffs, den der Administrator auf den Dienst hat. Wenn Sie eine Rolle zuweisen, geben Sie die Berechtigungsgruppe und die Kontogruppen an, die der Administrator verwalten kann. Der Hub verfügt über die folgenden integrierten Berechtigungsgruppen für Administratoren, die Prisma Access verwenden.

- **App-Administrator** – hat vollen Zugriff auf die angegebene App, einschließlich aller App-Instanzen, die in Zukunft hinzugefügt werden. Der App-Administrator kann Rollen für App-Instanzen zuweisen sowie App-Instanzen speziell für diese App aktivieren.
- **Instanzadministrator** – hat vollen Zugriff auf die App-Instanz, der diese Rolle zugewiesen ist. Der Instanz-Administrator kann andere Benutzer zu Instanz-Administratoren für die App-Instanz ernennen. Falls die App über vorgegebene oder benutzerdefinierte Rollen verfügt, kann der Instanz-Administrator diese Rollen anderen Benutzern zuweisen.
- **Super Reader** – kann alle Konfigurationselemente, Protokolle und Einstellungen anzeigen. Super Reader können keine Änderungen an anderen Einstellungen vornehmen.
- **Audit-Administrator** – kann nur Protokolle und Protokolleinstellungen anzeigen und verwalten. Audit-Administratoren können keine Änderungen an anderen Einstellungen vornehmen.
- **Verschlüsselungsadministrator** – kann Protokolle anzeigen und Verschlüsselungseinstellungen wie IKE, IPSec, Hauptschlüsselverwaltung und Zertifikatskonfiguration verwalten. Verschlüsselungsadministratoren können andere Einstellungen weder anzeigen noch ändern.
- **Sicherheitsadministrator** – kann Protokolle anzeigen und alle Einstellungen verwalten, außer den Verschlüsselungseinstellungen, die der Rolle „Verschlüsselungsadministrator“ zur Verfügung stehen.
- **Websicherheitsadministrator** – kann nur Konfigurationselemente anzeigen, die sich auf die Websicherheit beziehen.
- **Data-Loss-Prevention-Administrator** – kann auf die Enterprise-DLP-Einstellungen zugreifen, kann aber Konfigurationsänderungen nicht per Push an Prisma Access übertragen.
- **Datensicherheitsadministrator** – kann auf Enterprise-DLP- und SaaS-Sicherheitskontrollen zugreifen, kann aber Konfigurationsänderungen nicht per Push an Prisma Access übertragen.
- **SaaS-Administrator** – kann auf die SaaS-Sicherheitseinstellungen zugreifen, kann aber Konfigurationsänderungen nicht per Push an Prisma Access übertragen.

# Benutzerdefinierte rollenbasierte Zugriffssteuerung – Einrichtung

Hier erfahren Sie, wie Sie eine vordefinierte Rolle verwenden oder eine benutzerdefinierte Rolle erstellen, einem Benutzer eine Rolle zuweisen und den Benutzerumfang verwalten, wenn Sie auf die Prisma Access-Anwendung zugreifen.

**STEP 1 |** Hinzufügen einer benutzerdefinierten Rolle über allgemeine Dienste

Wenn Sie eine detailliertere Zugriffssteuerung benötigen als mit den vordefinierten Rollen möglich, können Sie benutzerdefinierte Rollen hinzufügen, um zu definieren, welche Berechtigungen für Ihre Benutzer durchgesetzt werden. Ähnlich wie vordefinierte Rollen handelt es sich bei benutzerdefinierten Rollen um eine Reihe von Berechtigungen und Berechtigungssätzen. Im Gegensatz zu vordefinierten Rollen können benutzerdefinierte Rollen jeweils nur den Benutzern in der Hierarchie unter der Manden-Dienstgruppe (Tenant Service Group, TSG) zugewiesen werden, in der sie definiert sind. Dadurch werden Namenskonflikte zwischen ähnlich benannten benutzerdefinierten Rollen vermieden, die von verschiedenen Kunden definiert wurden.

Wenn Sie auf der obersten Ebene (übergeordneten Ebene) der Hierarchie eine benutzerdefinierte Rolle hinzufügen, wird diese Rolle den untergeordneten Mandanten zugewiesen, sodass der übergeordnete Mandant die untergeordneten Mandanten verwalten kann.

**STEP 2 |** Hinzufügen des Benutzerzugriffs über allgemeine Dienste

Über „Allgemeine Dienste: Zugriff und Identität“ können Sie Benutzerzugriff auf die Plattform sowie auf die von Ihnen erstellten Mandanten hinzufügen.

**STEP 3 |** Zuweisen einer vordefinierten Rolle zu einem Mandantenbenutzer oder Dienstkonto über allgemeine Dienste

Wenn Sie bereits Benutzer hinzugefügt haben und weitere Rollen hinzufügen möchten, können Sie vordefinierte Rollen auch im Batch zuweisen. Weitere Informationen zu Rollen und Berechtigungen finden Sie hier.

**STEP 4 |** Erstellen eines neuen Umfangs in der Prisma Access  Cloud Management-Benutzeroberfläche

Mit Prisma Access Cloud Management können Sie (als Administrator) einem Cloud Management-Benutzer (der kein Administrator ist) einen Verwaltungsumfang zuweisen, um Berechtigungen basierend auf Umfängen wie Ordnern und Snippets zuzuordnen.

Bei den Berechtigungen handelt es sich um Aktionen, die im System zulässig sind. Berechtigungen stellen einen bestimmten Satz von API-Aufrufen (Application Programming Interface) dar, die Sie zum Lesen, Schreiben und Löschen von Objekten innerhalb der Systeme verwenden. Alle Berechtigungen sind in Rollen gruppiert.

# Verwalten: Verwaltung des Umfangs

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)*<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | ❑ Mindestens eine dieser Lizenzen ist erforderlich, um Ihre Konfiguration mit Strata Cloud Manager zu verwalten; für die einheitliche Verwaltung von NGFWs und Prisma Access benötigen Sie Folgendes:<br>❑ Prisma Access-Lizenz<br>❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>❑ Strata Cloud Manager Pro<br>→ Die Ihnen zur Verfügung stehenden Funktionen und Fähigkeiten in Strata Cloud Manager hängen davon ab, welche Lizenz(en) Sie verwenden. |

Konfigurieren Sie die Umfangsverwaltung, um eine benutzerdefinierte rollenbasierte Zugriffssteuerung durchzusetzen. Auf diese Weise können Sie angeben, welche Strata Cloud Manager-Administratoren auf bestimmte Ordner, Firewalls, Prisma Access-Bereitstellungen und Snippet-Konfigurationen zugreifen und diese ändern können. Die Definition der Umfangsverwaltung für Ihre Cloud-Administratoren stellt sicher, dass nicht zu viel bereitgestellt wird, und definiert die Lese- und Schreibzugriffsberechtigungen für die ausgewählten Ordner, Firewalls, Prisma Access-Bereitstellungen und Snippet-Konfigurationen. Es werden mehrere Plattform- und Unternehmensrollen für allgemeine Dienste verwendet, um die Lese- und Schreibzugriffsberechtigungen für einen Strata Cloud Manager-Administrator zu definieren.

Die Konfiguration der Umfangsverwaltung wird für Ihren gesamten Strata Cloud Manager-Mandanten definiert. Die Umfangsverwaltung kann nicht für einen bestimmten Ordner, eine Prisma Access-Bereitstellung oder einen Firewall-Konfigurationsumfang definiert werden.

*Nur ein Cloud Management-Administrator oder ein Superuser kann ein Umfangsobjekt erstellen. Das Widget „Verwaltung des Umfangs“ ist für Benutzer mit anderen Rollen nicht verfügbar.*

**STEP 1 |** Melden Sie sich bei Strata Cloud Manager an.

**STEP 2 |** Wählen Sie **Verwalten** > **Zugriffssteuerung** > **Verwaltung des Umfangs** aus.

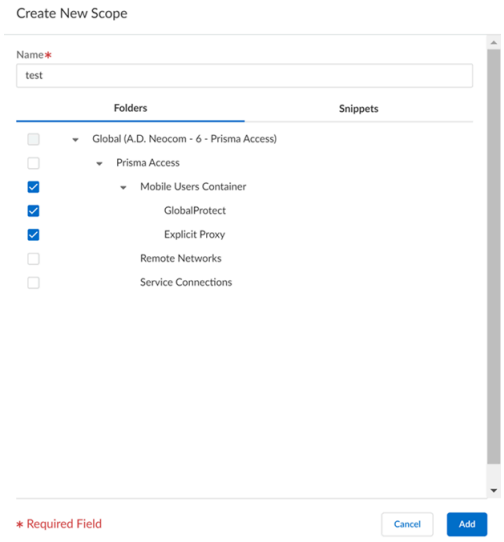
**STEP 3 |** Wählen Sie **Neuen Umfang erstellen**.

**STEP 4 |** Definieren Sie die Konfiguration der Umfangsverwaltung.

Umfangsverwaltungskonfigurationen werden als `Umfangsobjekt` bezeichnet.

1. Geben Sie einen beschreibenden **Namen** ein.
2. Wählen Sie **Ordner** aus und markieren (aktivieren) Sie die Ordner, Firewalls und Prisma Access-Bereitstellungen, die Sie in den Umfang aufnehmen möchten.

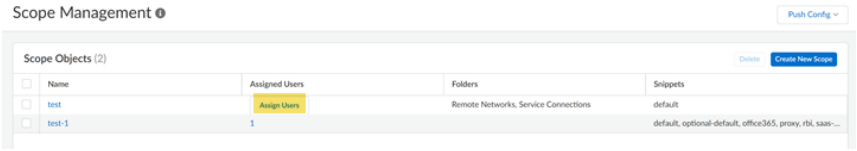
   *Die Auswahl einer Firewall umfasst auch den Ordner, dem die ausgewählte Firewall in der Umfangsverwaltungskonfiguration zugeordnet ist. Nur der unmittelbar zugeordnete Ordner ist enthalten, nicht der übergeordnete Ordner.*
3. Wählen Sie **Snippets** aus und markieren (aktivieren) Sie die Snippets, die Sie einbeziehen möchten.
4. Fügen Sie über **Hinzufügen** das Umfangsobjekt hinzu.



**STEP 5 |** Wenden Sie die Umfangsverwaltungskonfiguration auf Strata Cloud Manager-Administratoren an.

1. Weisen Sie dem Umfangsobjekt, das Sie im vorherigen Schritt erstellt haben, über **Benutzer zuweisen** Benutzer zu.




2. Wählen Sie eine **Rolle** für den Strata Cloud Manager-Administrator aus. Sie können beispielsweise „MSP-Superuser“ für einen Benutzer auswählen, der Zugriff auf alle Funktionen für alle Mandanten benötigt.

   Die Standardeinstellung ist `Keine`. Weitere Informationen zu den Lese - und Schreibzugriffsberechtigungen für jede verfügbare Rolle finden Sie in den verschiedenen Plattform- und Unternehmensrollen für allgemeine Dienste.

   *Wählen Sie einen spezifischen Strata Cloud Manager-Administrator aus und wählen Sie **Rolle löschen**, um die derzeit zugewiesene Rolle für allgemeine Dienste zu entfernen. Dadurch wird die Standardrolle `Keine` auf den Administrator angewendet.*

3. Um einen vorhandenen Umfang zu ändern, den Namen zu bearbeiten und Ordner hinzuzufügen oder sie zu entfernen, wählen Sie das Umfangsobjekt aus, ändern Sie den Umfang nach Bedarf und **aktualisieren** Sie den Umfang.
4. Um die zugewiesenen Benutzer zu ändern, weitere Benutzer hinzuzufügen oder die Benutzer zu ändern, klicken Sie auf **Zugewiesene Benutzer**, ändern Sie sie nach Bedarf und **schließen** Sie das Fenster.

# Verwalten: IP-Beschränkungen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)*<br>• NGFW, einschließlich derer, die durch Software-NGFW-Credits finanziert werden | ❑ Mindestens eine dieser Lizenzen ist erforderlich, um Ihre Konfiguration mit Strata Cloud Manager zu verwalten; für die einheitliche Verwaltung von NGFWs und Prisma Access benötigen Sie Folgendes:<br>❑ Prisma Access-Lizenz<br>❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>❑ Strata Cloud Manager Pro<br>→ Die Ihnen zur Verfügung stehenden Funktionen und Fähigkeiten in Strata Cloud Manager hängen davon ab, welche Lizenz(en) Sie verwenden. |

Geben Sie vertrauenswürdige IP-Adressen für Prisma Access Cloud Management-Administratoren an. Nur Administratoren, die sich über diese Quell-IP-Adressen anmelden (und sich auch erfolgreich authentifizieren), können auf Prisma Access Cloud Management zugreifen.

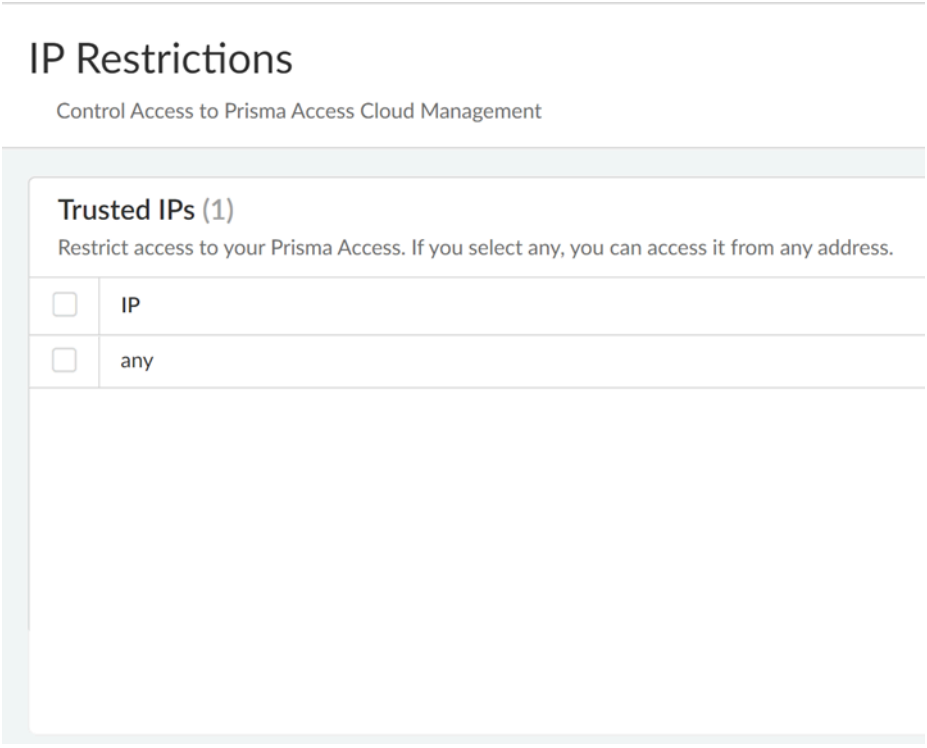
Die IP-Adressen müssen öffentliche Adressen sein. Standardmäßig werden keine vertrauenswürdigen Adressen erzwungen (die Liste ist auf **Beliebige** festgelegt).

Um loszulegen, gehen Sie zu **Verwalten** > **Zugriffssteuerung** > **IP-Beschränkungen**.

Bei IP-Beschränkungen wird die Subnetzadresse nicht unterstützt. Es werden nur IP-Adressen und IP-Adressbereiche unterstützt. Geben Sie keine Subnetze an, die sich mit den folgenden IP-Adressen und Subnetzen überschneiden, da Prisma Access diese IP-Adressen und Subnetze für den internen Gebrauch reserviert:

- 169.254.169.253 und 169.254.169.254
- 100.64.0.0/10
- 169.254.201.0/24
- 169.254.202.0/24

Wir empfehlen die Verwendung eines RFC-1918- und RFC-6598-konformen IP-Adresspools. Obwohl die Verwendung nicht RFC-1918- und RFC-6598-konformer (öffentlicher) IP-Adressen unterstützt wird, raten wir aufgrund möglicher Konflikte mit dem öffentlichen Internet-IP-Adressraum davon ab.



# Workflows: Strata Cloud Manager

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• NGFW (Managed by Strata Cloud Manager)<br>• Prisma SD-WAN | Eine oder mehrere dieser Lizenzen, abhängig vom Workflow:<br>❑ AIOps for NGFW Premium-Lizenz<br>❑ Strata Logging Service-Lizenz (für Protokollierung erforderlich)<br>❑ Prisma Access-Lizenz<br>❑ Prisma SD-WAN<br>❑ Remote-Browser-Isolation-Lizenz |

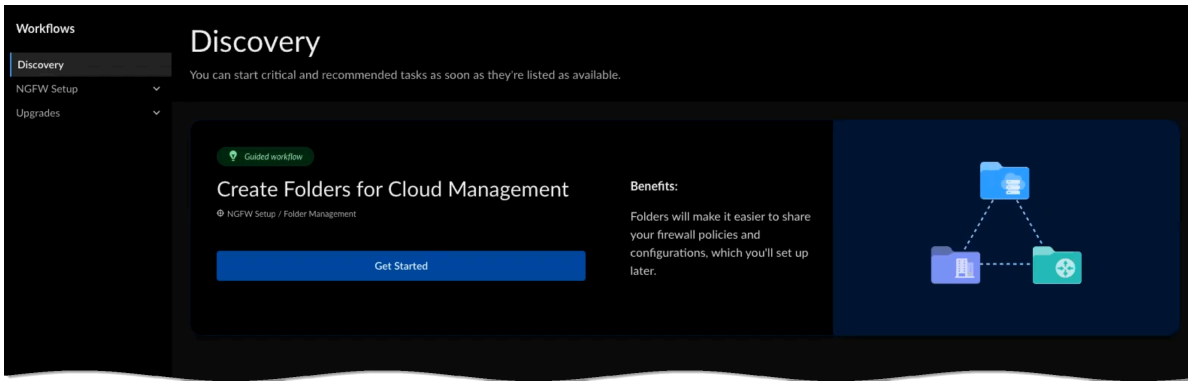
Wenn Sie zum ersten Mal zu Ihren Workflows navigieren, werden im **Discovery**-Dashboard wichtige und empfohlene Maßnahmen angezeigt, mit denen Sie Ihren Sicherheitsstatus oder Ihr Konfigurationsmanagement verbessern können, sobald diese für Sie verfügbar sind. Fahren Sie hier fort, um mobile NGFWs und Prisma Access-Benutzer sowie Remote-Netzwerke einzurichten und einzubinden und Software-Upgrades für NGFWs zu planen.

- Onboarding-Aufgaben entdecken
- Einrichten Prisma Access
- NGFWs einrichten
- Einrichten Prisma SD-WAN
- Software-Upgrades (NGFW)
- Software-Upgrades (Prisma Access)

# Workflows: Discovery

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• NGFW (Managed by Strata Cloud Manager)<br>• Prisma SD-WAN | ❑ AIOps for NGFW Premium-Lizenz oder Prisma Access-Lizenz |

In Discovery können Sie wichtige und empfohlene Aufgaben starten, sobald sie verfügbar sind. Möglicherweise gibt es geführte Workflows oder Aufgaben, die Sie selbst erledigen können. In diesem Thema zeigen wir Ihnen, wie Sie mithilfe des geführten Workflows mühelos und intuitiv Ihre Ordnerstruktur erstellen und ihr Geräte zuweisen können.




Gehen Sie wie folgt vor, um Ordner für Ihre Firewalls zu erstellen:

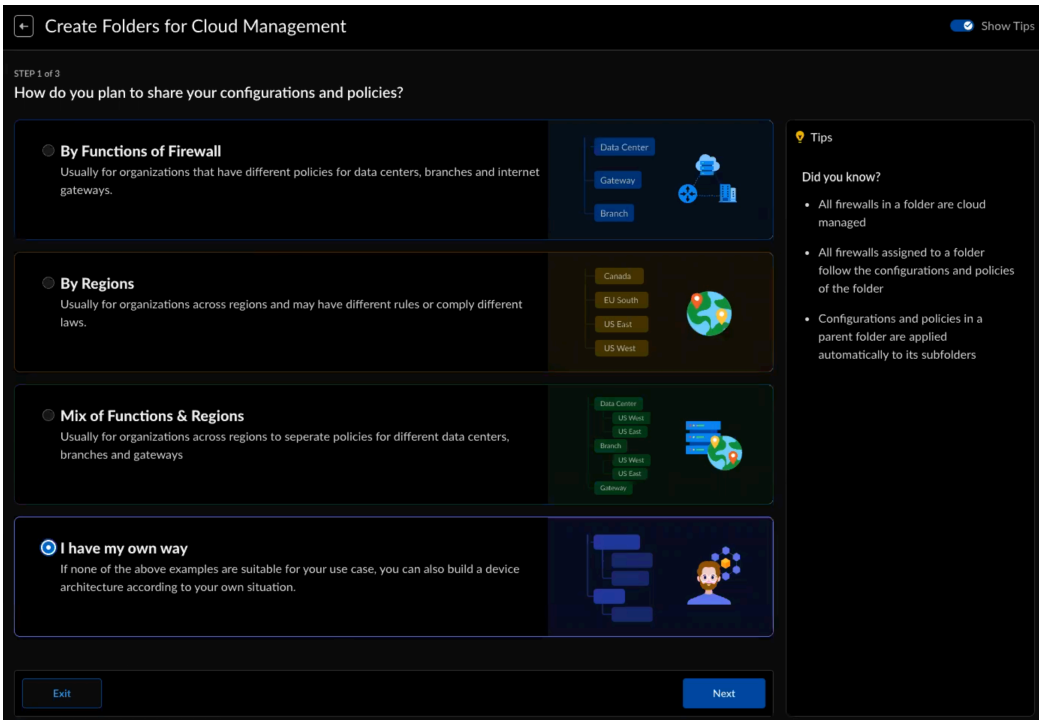
**STEP 1 |** Gehen Sie zu **Workflows** > **Discovery** und wählen Sie **Erste Schritte** aus.

**STEP 2 |** Wählen Sie aus, wie Sie Ihre Richtlinienregeln und Konfigurationen freigeben möchten.

- **Nach Funktionen der Firewall** – Hat Ihr Unternehmen unterschiedliche Richtlinien für Rechenzentren, Zweigstellen und Internet-Gateways? Dann könnte dies die richtige Option für Sie sein.
- **Nach Region** – Umfasst Ihre Organisation Regionen, in denen unterschiedliche Regeln gelten oder unterschiedliche Gesetze eingehalten werden? Dann erwägen Sie diese Option.
- **Mix aus Funktionen und Regionen** – Muss Ihr regionsübergreifendes Unternehmen separate Richtlinien für verschiedene Rechenzentren, Filialen und Internet-Gateways festlegen? Dann probieren Sie diese Option aus.
- **Ich habe meinen eigenen Weg** – Wenn keines der oben genannten Beispiele für Ihren Anwendungsfall geeignet ist, können Sie auch eine Gerätearchitektur entsprechend für Ihre eigene Situation erstellen.

Für dieses Beispiel wählen wir die Option **Ich habe meinen eigenen Weg**.



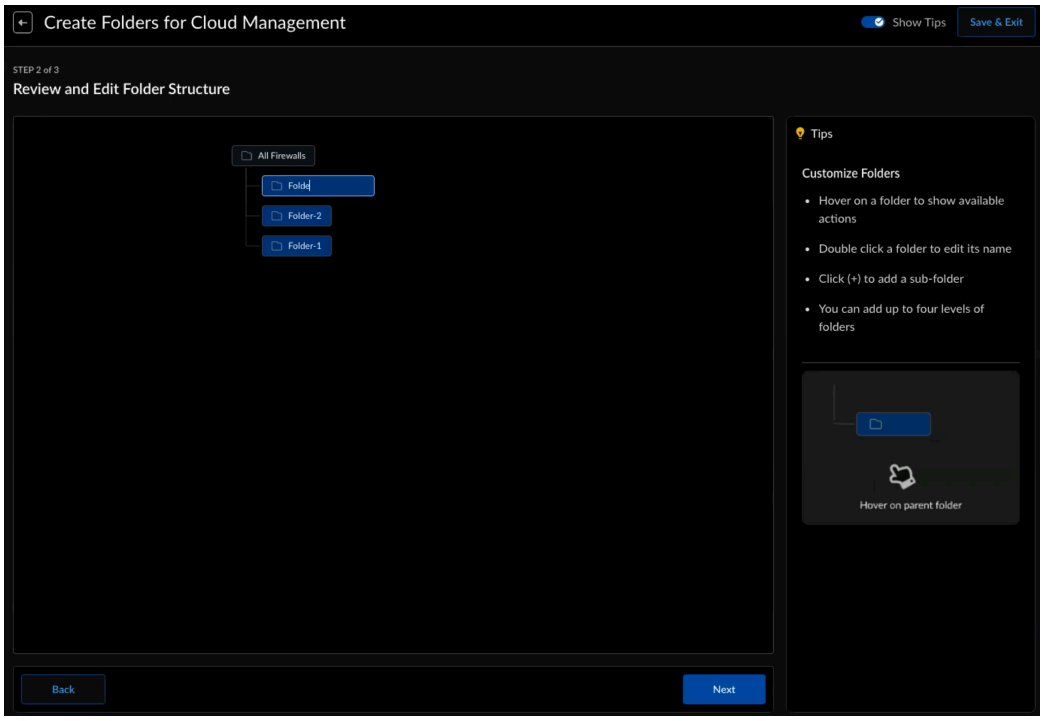

*Aktivieren Sie **Tipps anzeigen**, um sich Hilfetexte anzusehen, die Ihnen helfen, eine fundierte Entscheidung zu treffen.*

**STEP 3 |** Wählen Sie **Weiter**, um Ihre Ordnerstruktur zu erstellen.

**STEP 4 |** Verwenden Sie die folgenden Aktionen, um Ihre Ordnerstruktur auf Grundlage der Vorlage zu erstellen, die Sie in Schritt 1 ausgewählt haben. Mögliche Aktionen:

- **Neuen Ordner hinzufügen** – Bewegen Sie den Mauszeiger über einen Ordner, um die Option zum Hinzufügen eines neuen Ordners anzuzeigen. Klicken Sie auf und geben Sie Ihrem neuen Ordner einen Namen.
- **Ordner löschen** – Bewegen Sie den Mauszeiger über einen Ordner, um die Option zum Löschen des Ordners anzuzeigen. Wählen Sie , um den Ordner zu löschen.
- **Ordner umbenennen** – Doppelklicken Sie auf einen Ordner, um einen neuen Namen für den Ordner einzugeben. Drücken Sie die Eingabetaste oder klicken Sie auf eine Stelle außerhalb des Textfelds, damit Ihr neuer Name übernommen wird.
- **Erweitern oder reduzieren** Sie Ordnerknoten, die untergeordnete Elemente aufweisen.



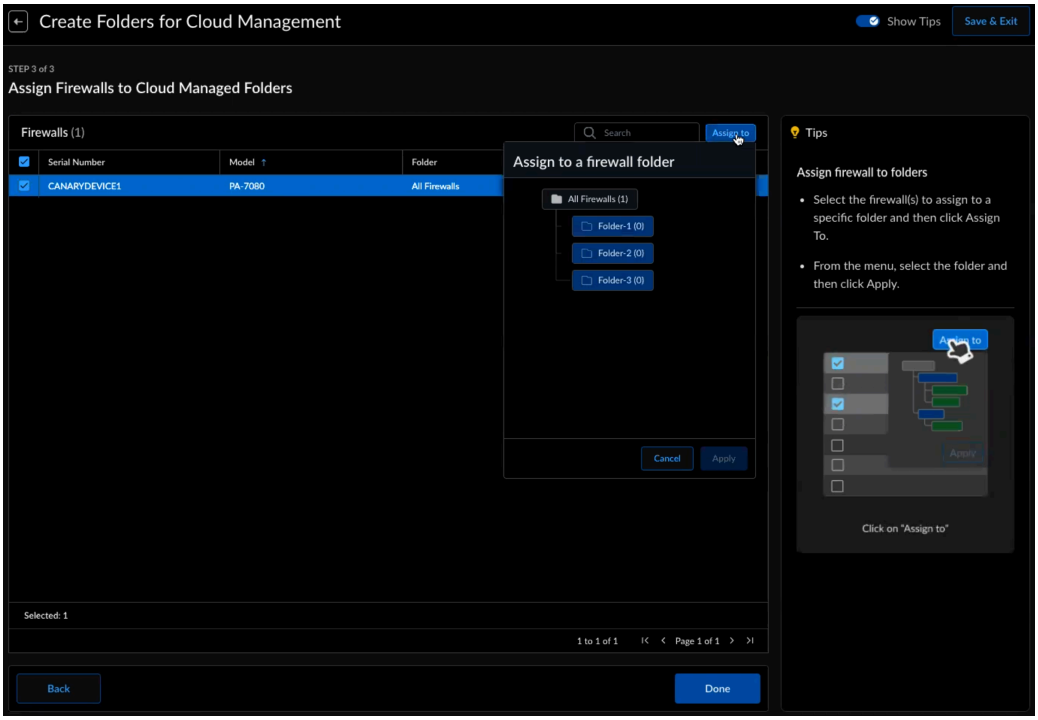

- *Ordnerbäume können maximal vier Ebenen enthalten.*
- *Ordner auf oberster Ebene können nicht gelöscht oder umbenannt werden.*
- *In den Tipps finden Sie Hinweise zu bestimmten Ordneraktionen.*
- *Wir speichern Ihre Arbeit: Sie können **jederzeit** abbrechen und später weitermachen.*

**STEP 5 |** Wählen Sie **Weiter**, um Ihre Firewalls Ordnern zuzuweisen.

**STEP 6 |** Wählen Sie eine oder mehrere Firewalls aus dieser Liste aus.

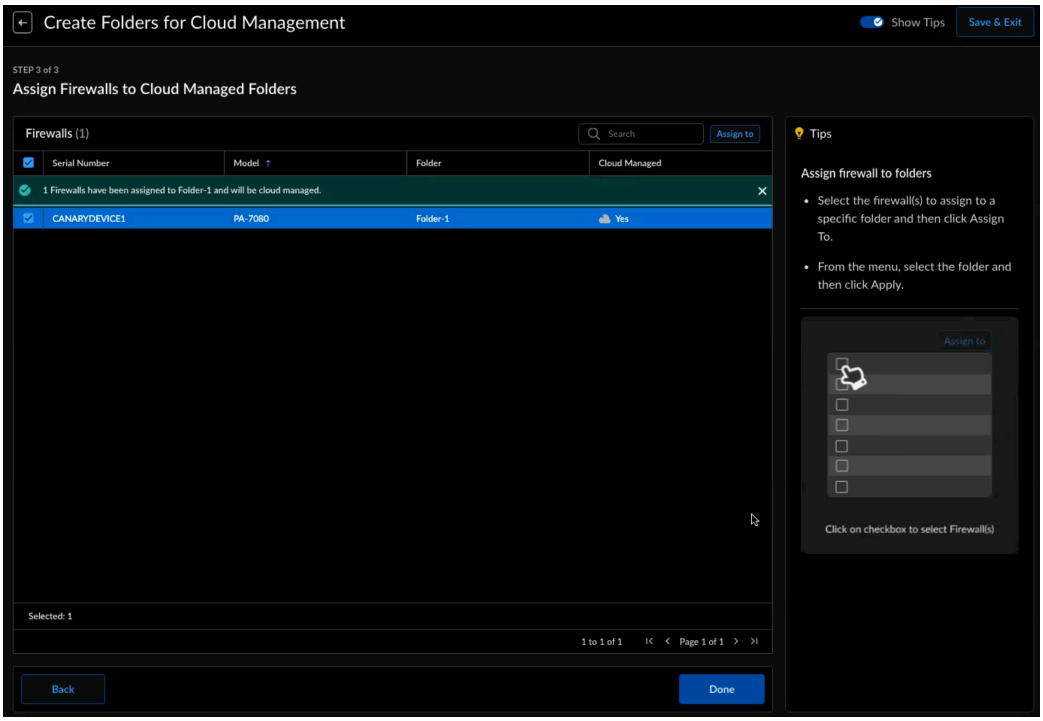
 

**STEP 7 |** Wählen Sie **Zuweisen zu**, wählen Sie einen Ordner aus, dem Sie Ihre Firewalls zuweisen möchten, und wählen Sie dann **Anwenden** aus. Die Cloud-Verwaltung ist für Firewalls aktiviert, die Sie einem **Cloud-verwalteten** Ordner zuweisen.

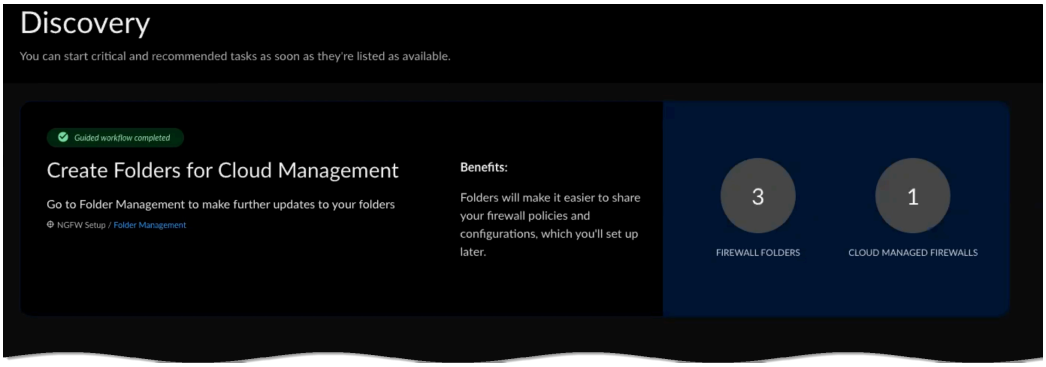


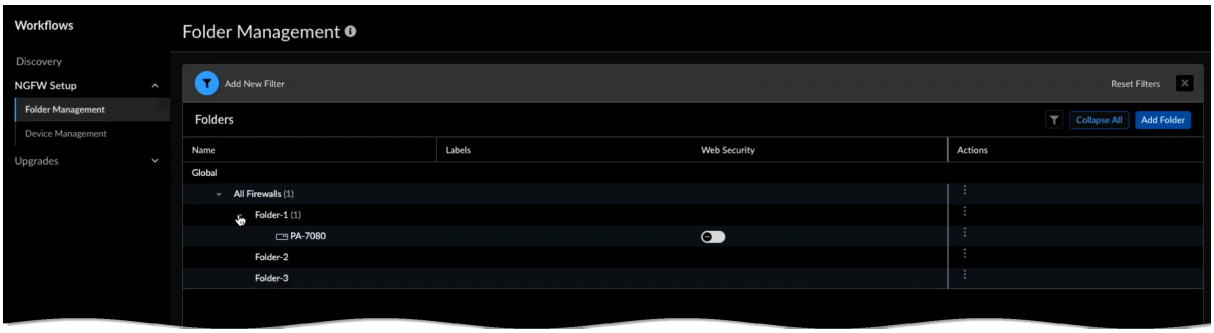

 

**STEP 8 |** Bestätigen Sie Ihre Aufgaben und wählen Sie **Fertig** aus.




Die von Ihnen erstellten Ordner und die von Ihnen zugewiesenen Firewalls werden auf der **Discovery-Hauptseite** sowie auf der Registerkarte **NGFW-Setup** > **Ordnerverwaltung** angezeigt.



# Workflows: NGFW-Setup

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • NGFW (Managed by Strata Cloud Manager) | ❑ AIOps for NGFW Premium-Lizenz (für Cloud-Verwaltung von NGFWs erforderlich)<br>❑ Strata Logging Service-Lizenz (für Protokollierung erforderlich)<br>❑ Wenn Sie eine Prisma Access-Lizenz besitzen, können Sie die **Ordnerverwaltung** verwenden, um Ihre vordefinierten Ordner anzuzeigen und Websicherheit für einen Ordner zu aktivieren. |

Im Rahmen der Einrichtung Ihrer NGFWs für die Cloud-Verwaltung müssen Sie Ihre Next-Generation-Firewalls in Strata Cloud Manager einbinden. Zum Onboarding gehört das Einrichten von Ordnern, um Firewalls zu gruppieren, die ähnliche Einstellungen erfordern. Erfahren Sie mehr über die Workflows: Ordnerverwaltung und verwenden Sie die Seite **Geräteverwaltung**, um Details zu allen Geräten in Ihrer Ordnerhierarchie anzuzeigen.

**STEP 1 |** Aktivieren Sie die Strata Logging Service- und AIOps für NGFW Premium-Lizenzen.

Die Strata Logging Service-Lizenz ist für die Protokollierung erforderlich und die AIOps for NGFW Premium-Lizenz für die Cloud-Verwaltung von NGFW.

**STEP 2 |** Erstellen Sie einen oder mehrere Ordner.

Ordner werden verwendet, um Ihre Firewalls oder Bereitstellungstypen logisch zu gruppieren und so die Konfigurationsverwaltung zu vereinfachen.

**STEP 3 |** eine Firewall in Strata Cloud Manager einbinden

Um eine Firewall in Strata Cloud Manager einzubinden, müssen Sie die lokalen Panorama-Einstellungen in der Firewall konfigurieren und die Firewall mit Ihrem Strata Cloud Manager-Mandanten verknüpfen. Nach der Anmeldung können Sie mit der Konfiguration der allgemeinen Firewall- und der Sitzungseinstellungen fortfahren.

**STEP 4 |** (Nur HA) Konfigurieren Sie Ihre verwalteten Firewalls bei Bedarf in einer Konfiguration mit hoher Verfügbarkeit (High Availability, HA).

**STEP 5 |** Erstellen Sie ein oder mehrere Snippets.

Snippets werden verwendet, um Konfigurationsobjekte zu gruppieren, die auf Ordner, Bereitstellungen oder einzelne Firewalls angewendet werden. Das erleichtert und beschleunigt den Onboarding-Prozess, da Sie allgemeine Basiskonfigurationen standardisieren und anschließend schnell anwenden und übertragen können.

**STEP 6 |** Erstellen Sie Ihre Konfigurationsobjekte.

Konfigurationsobjekte sind Bausteine für Ihre Netzwerk- und Richtlinienregelkonfigurationen.

**STEP 7 |** Erstellen und konfigurieren Sie die Netzwerk- und Richtlinienregelkonfiguration.

**STEP 8 |** Übertragen Sie Konfigurationsänderungen von Strata Cloud Manager zu Ihrer verwalteten Firewall.

# Workflows: Geräteverwaltung

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • NGFW (Managed by Strata Cloud Manager) | ☐ AIOps for NGFW Premium |

Eine Palo Alto Networks-NGFW, die von Strata Cloud Manager verwaltet wird, wird als *Von der Cloud verwaltetes Gerät* bezeichnet. Strata Cloud Manager kann Firewalls mit PAN-OS 10.2.3 oder höher verwalten.

Weitere Informationen zu den Voraussetzungen für Strata Cloud Manager finden Sie hier.

Mit dem Dashboard **Geräteverwaltung (Workflows > NGFW-Setup > Geräteverwaltung)** können Sie wichtige Geräte- und Versionsdetails zu all Ihren verwalteten Geräten überprüfen und auswählen, welche Geräte in die Cloud-Verwaltung verschoben werden sollen.

## Anzeigen aller Details zu Cloud-verwalteten NGFWs

Auf der Registerkarte **Von der Cloud verwaltete Geräte (Workflows > NGFW-Setup > Geräteverwaltung > Von der Cloud verwaltete Geräte)** werden all Ihre eingebundenen SCM-Firewalls, die Ordner, denen sie zugewiesen sind, sowie wichtige Details dazu angezeigt.

| Geräteinformationen | Beschreibung |
|---|---|
| Name | Der Name der NGFW und die Ordner, unter denen sie organisiert ist. |
| Beschriftungen | Alle der NGFW angehängten Beschriftungen. |
| Status der Konfigurationssynchronisierung | Der Synchronisationsstatus der NGFW:<br>• Synchron<br>• Nicht synchron |
| HA-Status | Der HA-Status der eingebundenen NGFW:<br>• **Aktiv** – normaler Betriebsstatus bei der Verkehrsverarbeitung.<br>• **Passiv** – normaler Backup-Zustand.<br>• **Wird initiiert** – Die Firewall befindet sich nach dem Hochfahren bis zu 60 Sekunden in diesem Zustand. |

| Geräteinformationen | Beschreibung |
|---|---|
| | • **Nicht funktionsfähig** – Fehlerzustand.<br>• **Ausgesetzt** – Ein Administrator hat die Firewall deaktiviert.<br>• **Vorläufig** – für ein Verbindungs- oder Pfadüberwachungsereignis in einer Aktiv/Aktiv-Konfiguration. |
| Seriennummer | Die Seriennummer der eingebundenen NGFW. |
| Modell | Die Modellnummer der eingebundenen NGFW. |
| Typ | Der Typ der eingebundenen NGFW:<br>• VM<br>• PA |
| Adresse | Die IP-Adresse der eingebundenen NGFW. |
| Lizenz | Die Lizenzinformationen für die eingebundene NGFW<br>• Übereinstimmend<br>• Nicht übereinstimmend |
| Softwareversion \| App und Bedrohung \| Antivirus \| URL-Filterung | Zeigt die Software- und Inhaltsversionen an, die derzeit in der Firewall installiert sind. Weitere Einzelheiten finden Sie unter Firewall-Software- und -Inhaltsupdates. |
| Gerätewörterbuch | Eine Datei für den Import in Firewalls. Die Wörterbuchdatei stellt Strata Cloud Manager- und Firewall-Administratoren eine Liste von Geräteattributen bereit, aus der sie beim Importieren empfohlener Sicherheitsrichtlinienregeln wählen können. |
| Actions (Aktionen) | Die Aktionen für die eingebundene Firewall:<br>• Lizenzinformationen abrufen<br>• Neu starten<br>• Routingmodus ändern<br>• Lokale Konfigurationsverwaltung<br>• Bootstrap erzwingen |

## Entfernen einer NGFW aus von der Cloud verwalteten Geräten

Auf der Registerkarte **Verfügbare Geräte** werden alle NGFWs angezeigt, die für die Integration in SCM verfügbar sind, sowie NGFWs, die bereits von Strata Cloud Manager verwaltet werden.

*Weitere Informationen zum Onboarding-Prozess für Strata Cloud Manager finden Sie hier.*

Über die Registerkarte „Verfügbare Geräte“ können Sie Geräte zu und aus Strata Cloud Manager verschieben.

**STEP 1 |** Melden Sie sich bei Strata Cloud Manager an.

**STEP 2 |** Wählen Sie **Workflows** > **NGFW-Setup** > **Geräteverwaltung** > **Verfügbare Geräte** aus.

1. Wählen Sie **Zurück zu verfügbaren Geräten** aus, um eine Firewall aus Strata Cloud Manager zu verschieben.

### Wiederherstellen eines Snapshots der lokalen Konfigurationsversion auf einer Firewall

Sie können jede beliebige Version wiederherstellen und die Konfigurationsdetails im XML-Format herunterladen.

**STEP 1 |** Melden Sie sich bei Strata Cloud Manager an.

**STEP 2 |** Wählen Sie **Workflows** > **NGFW-Setup** > **Geräteverwaltung** aus und wählen Sie dann unter **Aktionen** die Option **Lokale Konfigurationsverwaltung** aus.

**STEP 3 |** **Laden** Sie die Version, um die lokale Konfiguration wiederherzustellen.

**STEP 4 |** Klicken Sie auf **Ja**, um die lokale Konfiguration auf der Firewall durch die Konfigurationsversion zu ersetzen. Ein neuer Commit-Job wird erstellt.

Sie können die Ansicht **Jobs** verwenden, um Fehler bei fehlgeschlagenen Vorgängen zu beheben, Warnungen im Zusammenhang mit abgeschlossenen Commits zu untersuchen oder ausstehende Commits abzubrechen.

**STEP 5 |** Wählen Sie **Herunterladen**, um die Konfigurationsdetails für die ausgewählte Version herunterzuladen.

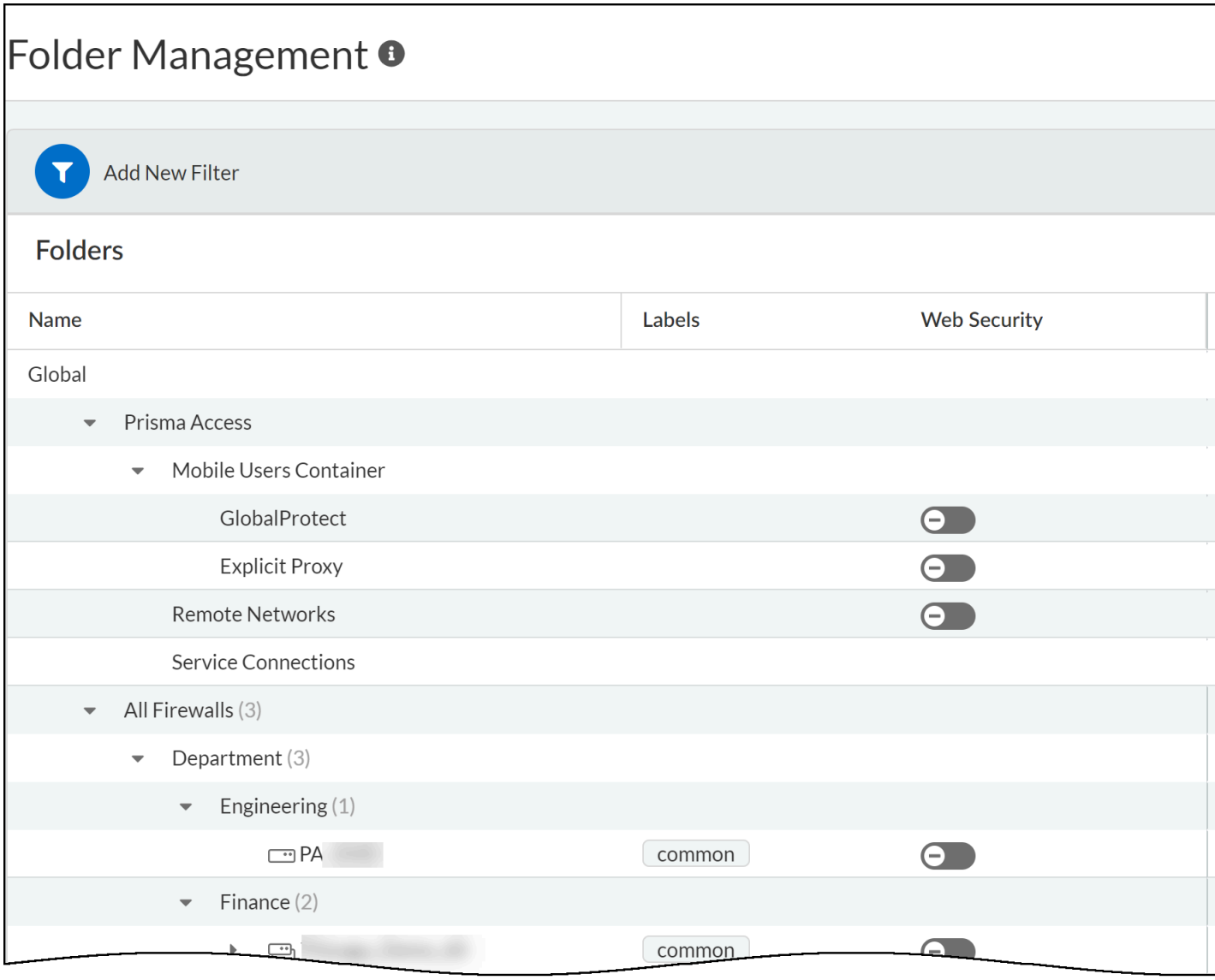
## Workflows: Ordnerverwaltung

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• NGFW (Managed by Strata Cloud Manager) | ☐ AIOps for NGFW Premium-Lizenz<br>☐ Prisma Access-Lizenz |

Ordner werden verwendet, um Ihre Firewalls oder Bereitstellungstypen (mobile Prisma Access-Benutzer, Remote-Netzwerke oder Dienstverbindungen) logisch zu gruppieren und so das Konfigurationsmanagement zu vereinfachen. Sie können einen Ordner erstellen, der mehrere verschachtelte Ordner enthält, um Firewalls und Bereitstellungen zu gruppieren, die ähnliche Konfigurationen erfordern. Bereits verschachtelte Ordner können auch mehrere verschachtelte Ordner enthalten.

Ordner für Prisma Access und Ihre NGFWs sind getrennt: Sie können NGFWs nicht in einem Ordner mit Prisma Access-Bereitstellungen gruppieren. Sie können jedoch problemlos gemeinsame Einstellungen global für alle Ordner anwenden oder Verwalten: Snippets

verwenden, um Standardeinstellungen und Richtlinienanforderungen einfach auf mehrere Ordner anzuwenden.



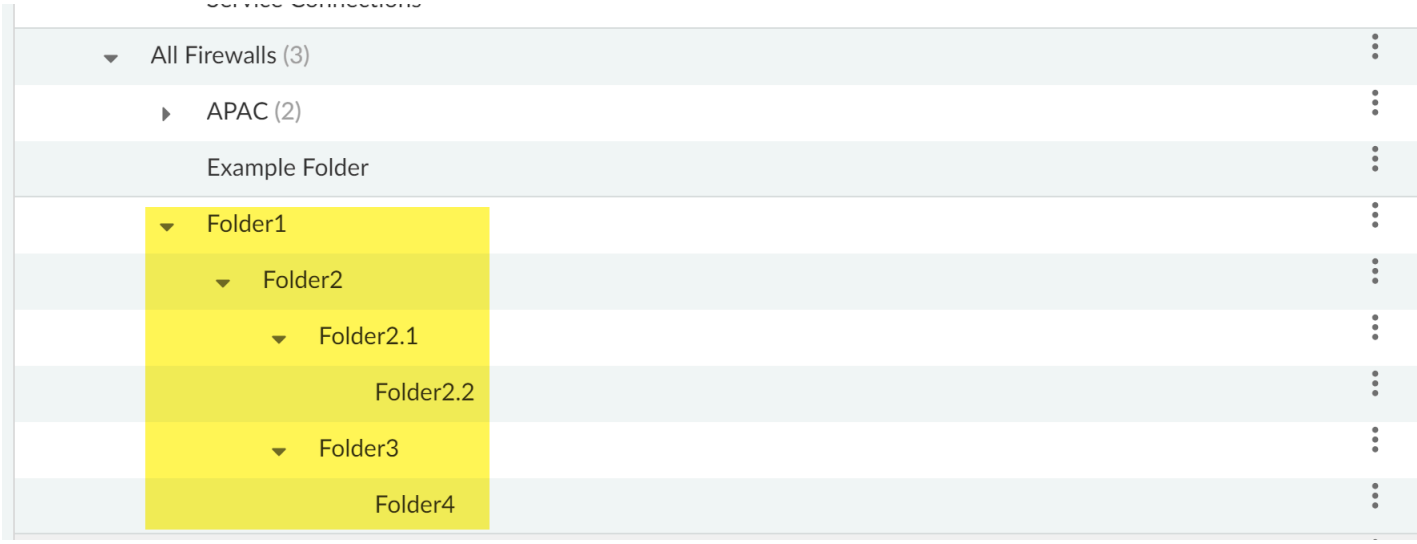

- NGFW
- Prisma Access

## Ordnerverwaltung (NGFWs)

Um die Verwaltung von Ordnern und Firewalls zu erleichtern, können Sie Beschriftungen anwenden, um bestimmte Gruppen von Firewalls zu filtern und für Konfigurationsänderungen als Ziel auszuwählen. Darüber hinaus zeigt jeder Ordner die derzeit installierte Softwareversion, die Release-Versionen für dynamische Inhalte und die GlobalProtect-App-Version der mit dem Ordner verknüpften Firewalls an.

Bei Firewallordnern unterstützt Strata Cloud Manager bis zu vier verschachtelte Ordner innerhalb einer bestimmten Ordnerhierarchie, wobei der Standardordner `Alle Firewalls` immer die oberste Ebene jeder Ordnerhierarchie ist. Beachten Sie beispielsweise Folgendes, wenn Sie Ihre Ordnerhierarchie entwerfen. Im folgenden Beispiel sind `Folder1`, `Folder2`, `Folder3` und

`Folder4` unter dem Ordner `Alle Firewalls` verschachtelt und Sie können dieser bestimmten Ordnerhierarchie keine zusätzlichen Ordner hinzufügen. Außerdem sind `Folder2.1` und `Folder2.2` unter `Folder2` verschachtelt und Sie können auch hier keine weiteren Ordner verschachteln.




### Ordner erstellen

Erstellen Sie Ordner, um Ihre Firewalls logisch zu gruppieren und so die Konfigurationsverwaltung zu vereinfachen. Sie können einen Ordner unter dem Standardordner `Firewalls` oder unter einem anderen vorhandenen Ordner erstellen.

**STEP 1 |** Melden Sie sich bei Strata Cloud Manager an.

**STEP 2 |** Gehen Sie zu **Workflows** > **NGFW-Setup** > **Ordnerverwaltung** und wählen Sie **Ordner hinzufügen** aus.

**STEP 3 |** Geben Sie dem Ordner einen aussagekräftigen **Namen**.

**STEP 4 |** (Optional) Geben Sie eine **Beschreibung** für den Ordner ein.

**STEP 5 |** (Optional) Weisen Sie ein oder mehrere **Beschriftungen** zu.

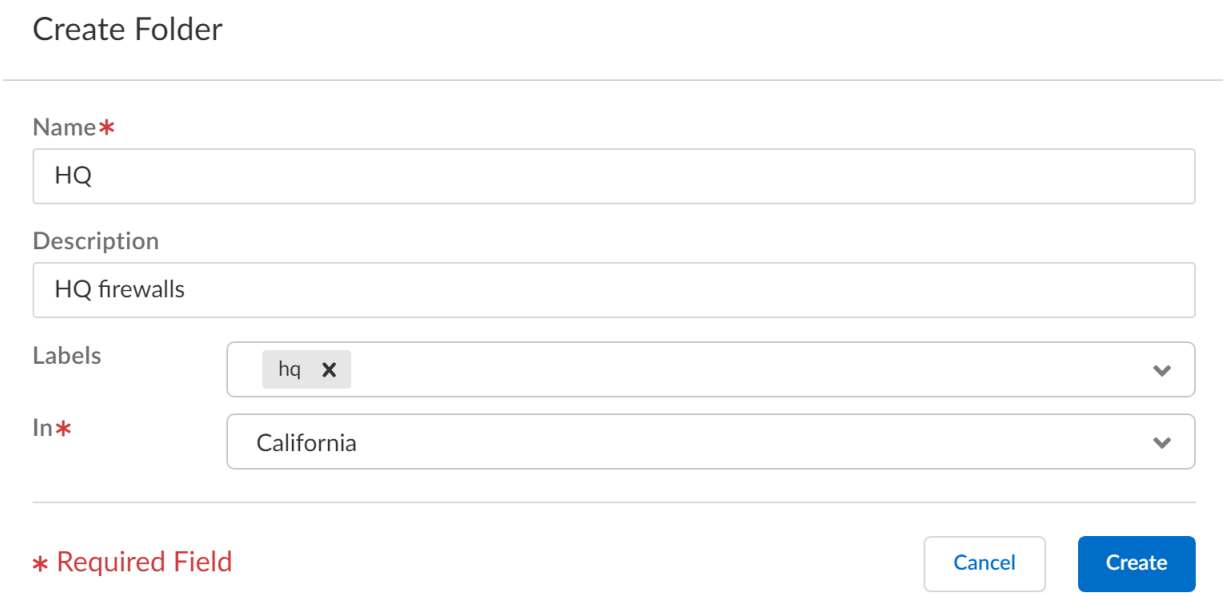
Sie können eine vorhandene Beschriftung auswählen oder eine neue Beschriftung erstellen, indem Sie die Beschriftung eingeben, die Sie erstellen möchten.

**STEP 6 |** Geben Sie unter **In** an, wo der Ordner erstellt werden soll.

Sie können **Alle Firewalls** auswählen oder alternativ einen vorhandenen Ordner auswählen, um den Ordner darunter zu verschachteln.

**STEP 7 |** **Erstellen** Sie den Ordner.

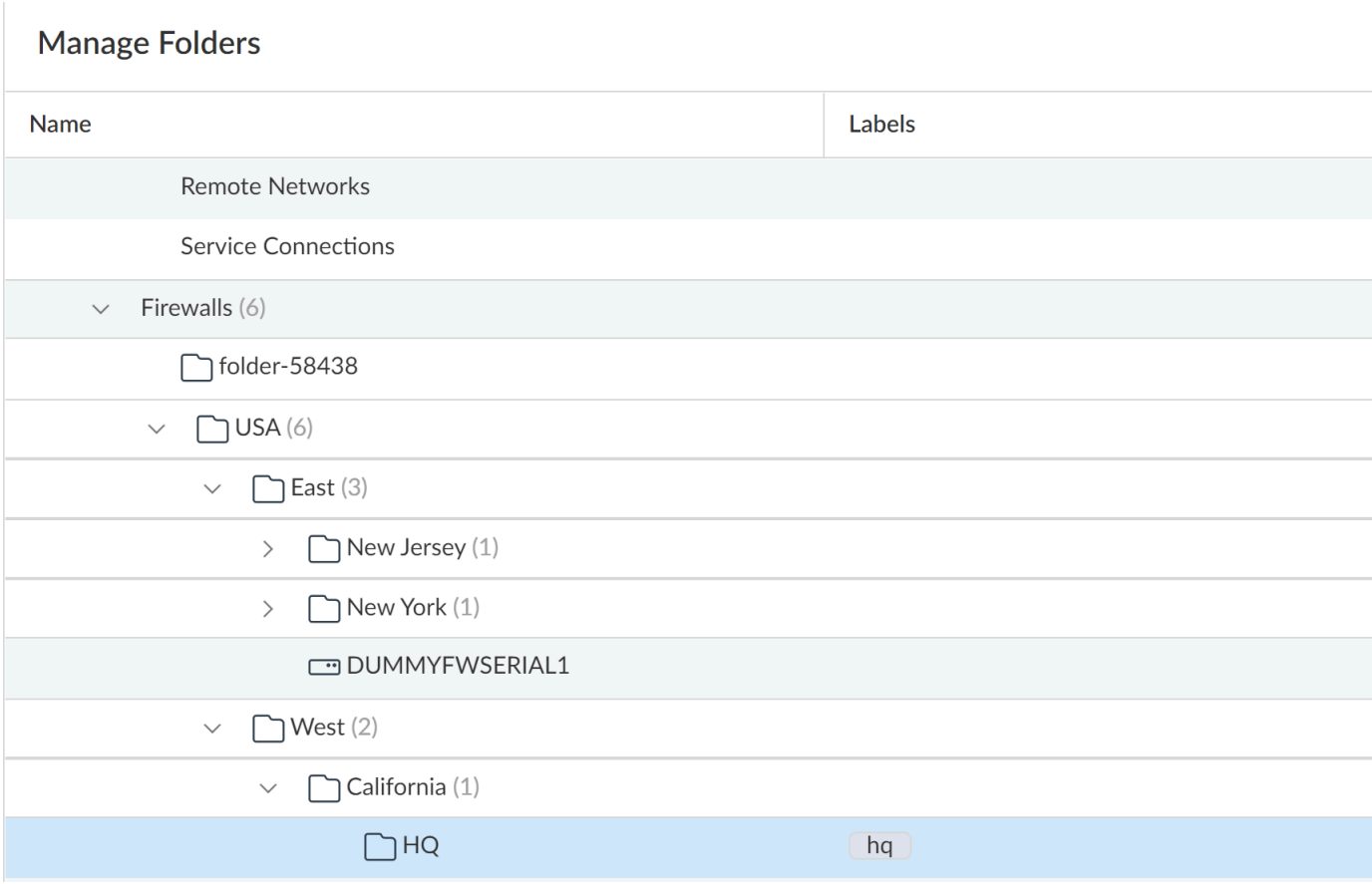



### Ordner ändern

Ändern Sie einen vorhandenen Ordner, um den Namen und die Beschreibung zu bearbeiten und Beschriftungen hinzuzufügen oder zu ändern. Darüber hinaus können Sie den Ordner nach Bedarf verschieben oder löschen.

**STEP 1 |** Melden Sie sich bei Strata Cloud Manager an.

**STEP 2 |** Wählen Sie **Workflows** > **NGFW-Setup** > **Ordnerverwaltung** aus und erweitern Sie das Menü „Aktionen“.



**STEP 3 |** Ändern Sie den Ordner nach Bedarf.

- **Bearbeiten** Sie den Ordner.
  1. Bearbeiten Sie den **Namen** des Ordners.
  2. (Optional) Bearbeiten Sie die **Beschreibung** des Ordners.
  3. Wählen oder erstellen Sie **Beschriftungen**.

     Sie können dem Ordner völlig andere Beschriftungen zuweisen oder zusätzliche Beschriftungen hinzufügen.
  4. Klicken Sie auf **Speichern**.
- **Verschieben** Sie den Ordner und wählen Sie das **Ziel** aus.

  Sie können einen Ordner auf folgende Arten verschieben.
  - Sie können einen Ordner verschieben, um ihn unter einem anderen Ordner zu verschachteln.
  - Sie können einen verschachtelten Ordner in den Ordner `Firewalls` verschieben.
  - Sie können einen verschachtelten Ordner von einem Ordner in einen anderen verschieben.

  **Verschieben** Sie den Ordner, nachdem Sie das Ordnerziel ausgewählt haben.
- **Löschen** Sie den Ordner und klicken Sie zur Bestätigung auf **OK**.

  Sie können nur Ordner löschen, denen keine Firewalls zugeordnet und keine Ordner untergeordnet sind.

## Ordnerverwaltung (Prisma Access)

Prisma Access-Ordner sind vordefiniert; Sie können sie verwenden, um den Konfigurationsumfang festzulegen und sicherzustellen, dass die Bereitstellungstypen von Prisma Access – mobile Benutzer, Remote-Netzwerke und Dienstverbindungen – alle globalen Einstellungen erhalten, gefolgt von Einstellungen, die für jeden Typ erforderlich oder spezifisch sind.

Die unter einem Ordner definierten Konfigurationen werden von allen Ordnern übernommen, die in dieser Ordnerhierarchie verschachtelt sind. Beispielsweise können Sie gemeinsame Einstellungen konfigurieren, die für GlobalProtect, explizite Proxys, Remote-Netzwerke und Dienstverbindungen im **Prisma Access**-Ordner gelten. In ähnlicher Weise können Sie Einstellungen konfigurieren, die für GlobalProtect und explizite Proxys im **Container für mobile Benutzer** gelten.

Sie können die Ordnerhierarchie für Prisma Access nicht bearbeiten.

Auf Ordnerebene können Sie auch Websicherheit für mobile Prisma Access-Benutzer, Remote-Netzwerke oder Dienstverbindungen aktivieren.

# Workflows: Prisma SD-WAN-Einrichtung

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma SD-WAN | ❑ Prisma SD-WAN-Lizenz |

Sie können Zweigstellen, Rechenzentrumsstandorte und ION-Geräte in Prisma SD-WAN mit Strata Cloud Manager einrichten.

Wählen Sie **Workflows** > **Einrichtung Prisma SD-WAN** aus.

Sie können Workflows für Folgendes einrichten:

- Zweigstellen

  Richten Sie mithilfe der Registerkarte **Zweigstellen** Zweigstellen in Ihrem Netzwerk ein. Ein Unternehmen kann innerhalb eines Netzwerks über eine oder mehrere Zweigstellen verfügen. Wenn Sie eine Zweigstelle erstellen, können Sie eine Standarddomäne und einen Satz von Richtlinienregeln auswählen und WAN-Netzwerke, Schaltkreiskategorien, Schaltkreisbezeichnungen und Schaltkreisspezifikationen konfigurieren.

- Rechenzentren

  Richten Sie mithilfe der Registerkarte **Rechenzentren** Rechenzentrumsstandorte in Ihrem Netzwerk ein. Rechenzentrumsstandorte sind mit Zweigstellen verbunden; Sie können Unternehmensanwendungen und -dienste in einem Rechenzentrum hosten.

- Geräte

  Richten Sie mithilfe der Registerkarte **Geräte** ION-Geräte in Ihrem Netzwerk ein. ION-Geräte können in einer Zweigstelle oder an einem Rechenzentrumsstandort bereitgestellt werden. Diese sind als Hardware- und Software-Varianten verfügbar, die den Anforderungen jedes Standorts und jedes Bereitstellungsszenarios gerecht werden. Sie müssen die ION-Geräte für Ihre Zweigstellen- und Rechenzentrumsstandorte verbinden, beanspruchen, zuweisen und konfigurieren.

# Workflows: Prisma Access-Einrichtung

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | Prisma Access-Lizenz |

Wählen Sie **Workflows** > **Einrichtung Prisma Access**, um mit der Einrichtung von Prisma Access zu beginnen.

- Richten Sie die Serviceinfrastruktur ein, um die Kommunikation zwischen Remote-Netzwerkstandorten, mobilen Benutzern und dem Hauptsitz oder den Rechenzentren zu ermöglichen, die Sie über Dienstverbindungen mit Prisma Access verbinden möchten. Eine Dienstverbindung stellt die Verbindung zum Rechenzentrum her.
- Binden Sie mobile Benutzer ein und bestimmen sie, wie sie sich mit Prisma Access verbinden sollen.
- Binden Sie Remote-Netzwerke ein, um Remote-Netzwerkstandorte, wie z. B. Zweigstellen, und die Benutzer an diesen Standorten zu schützen. Eine NGFW oder ein IPSec-kompatibles Gerät eines Drittanbieters mit einem SD-WAN, das einen IPSec-Tunnel zum Dienst aufbauen kann, ist am Remote-Standort erforderlich.
- Fügen Sie Dienstverbindungen hinzu, um sowohl mobilen Benutzern als auch Benutzern in Ihren Zweigstellennetzwerken den Zugriff auf Ressourcen in Ihrem Hauptsitz oder Rechenzentrum zu ermöglichen. Neben dem Zugriff auf Unternehmensressourcen ermöglichen Dienstverbindungen Ihren mobilen Benutzern auch die Verbindung zu Zweigstellen.

# Workflows: Prisma Access

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | Prisma Access-Lizenz |

Bevor Sie Prisma Access zum Schutz Ihrer Remote-Netzwerke und mobilen Benutzer verwenden können, müssen Sie ein Infrastruktursubnetz konfigurieren.

Prisma Access verwendet das Subnetz, um den Netzwerk-Backbone für die Kommunikation zwischen Ihren Zweigstellennetzen, mobilen Benutzern und der Prisma Access-Sicherheitsinfrastruktur sowie für die Kommunikation mit den Hauptsitz- und Rechenzentrumsnetzen zu erstellen, die Sie über Dienstverbindungen mit Prisma Access verbinden möchten. Wenn Sie dynamisches Routing für Ihre Remote-Netzwerke oder Dienstverbindungen verwenden, müssen Sie auch eine RFC-6696-konforme private BGP-AS-Nummer konfigurieren.

Verwenden Sie die folgenden Empfehlungen und Anforderungen, wenn Sie ein Infrastruktursubnetz für Prisma Access hinzufügen.

- Verwenden Sie ein RFC-1918-konformes Subnetz. Prisma Access unterstützt zwar die Verwendung nicht RFC-1918-konformer (öffentlicher) IP-Adressen, dies wird aber aufgrund möglicher Konflikte mit dem öffentlichen IP-Adressraum des Internets nicht empfohlen.

- Geben Sie keine Subnetze an, die sich mit 169.254.169.253, 169.254.169.254 und dem Subnetzbereich 100.64.0.0/10 überschneiden, da Prisma Access diese IP-Adressen und Subnetze für den internen Gebrauch reserviert. Dieses Subnetz ist eine Erweiterung Ihres bestehenden Netzwerks und darf sich daher nicht mit IP-Subnetzen überschneiden, die Sie innerhalb Ihres Unternehmensnetzwerks verwenden, oder mit den IP-Adresspools, die Sie Prisma Access für Benutzer oder Prisma Access für Netzwerke zuweisen. Da die Dienstinfrastruktur eine große Anzahl von IP-Adressen benötigt, müssen Sie ein /24-Subnetz zuweisen (z. B. 172.16.55.0/24).
- Geben Sie ein Infrastruktursubnetz ein, mit dem Prisma Access die Kommunikation zwischen Remote-Netzwerkstandorten, mobilen Benutzern und dem Hauptsitz oder den Rechenzentren ermöglicht, die Sie über Dienstverbindungen mit Prisma Access verbinden möchten. Verwenden Sie ein RFC-1918-konformes Subnetz als Infrastruktursubnetz.

Weitere Informationen finden Sie unter Prisma Access-Einrichtung.

### DNS-Einrichtung für die Infrastruktur

Mit Prisma Access können Sie DNS-Server (Domain Name System) angeben, um sowohl organisationsinterne als auch -externe Domänen aufzulösen. Prisma Access proxyt die DNS-Anfrage basierend auf der Konfiguration Ihrer DNS-Server.

Durch die Einrichtung des Infrastruktur-DNS wird der Zugriff auf Dienste in Ihrem Unternehmensnetzwerk wie LDAP und DNS-Server ermöglicht – insbesondere wenn Sie Dienstverbindungen einrichten möchten, um am Hauptsitz oder in Rechenzentren Zugriff auf diese Art von Ressourcen bereitzustellen. DNS-Abfragen für Domänen in der internen Domänenliste werden an Ihre lokalen DNS-Server gesendet, um sicherzustellen, dass Ressourcen für Prisma Access-Remote-Netzwerk- und mobile -Benutzer verfügbar sind.

Hierdurch werden interne Domänenlisten eingerichtet, die für den gesamten Datenverkehr gelten. Falls gewünscht, können Sie im Administratorhandbuch nachlesen, wie Sie interne Domänenlisten erstellen, die nur für bestimmte Mobile-Benutzer-Bereitstellungen oder Remote-Netzwerkstandorte gelten.

Die DNS-Einrichtung für die Infrastruktur hat mehrere Vorteile:

- Prisma Access kann Ihre internen Domänen auflösen.
- Richten Sie DNS ein, um sowohl interne als auch externe Domänen aufzulösen.
- Verwenden Sie einen Platzhalter (*) vor den Domänen in der Domänenliste, zum Beispiel *.acme.local oder *.acme.com.

Weitere Informationen finden Sie unter DNS für Prisma Access.

## Workflows: Mobile Benutzer

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | ☐ Prisma Access-Lizenz<br>☐ Strata Logging Service-Lizenz |

Stellen Sie vor der Konfiguration mobiler Benutzer sicher, dass Sie über die erforderlichen Lizenzen verfügen (Prisma Access-Lizenz für mobile Benutzer und eine Strata Logging Service-

Lizenz mit entsprechendem Firewall-Speicherplatz). Wenn mobile Benutzer eine Verbindung zu anderen verbundenen Netzwerken herstellen, benötigen Sie entweder eine ZTNA- (Zero Trust Network Access) oder eine Enterprise Edition Prisma Access-Lizenz, die den für die Verbindung erforderlichen Corporate Access Node (CAN) bereitstellt.

Sie wählen zuerst Ihren Verbindungstyp aus – Sie können GlobalProtect, einen expliziten Proxy oder beides verwenden. Für beide Verbindungsarten sind nur wenige Einstellungen erforderlich, die Sie vornehmen müssen, damit Prisma Access die Umgebung Ihrer mobilen Benutzer bereitstellen kann.

1. Stellen Sie eine Verbindung zu Prisma Access her.

   Legen Sie fest, wie mobile Benutzer am Standort, den Sie einrichten, eine Verbindung zu Prisma Access herstellen sollen. Sie können Ihre Mobile-Benutzer-Lizenz zwischen GlobalProtect und explizitem Proxy aufteilen: Einige Benutzer können sich über GlobalProtect und andere über einen expliziten Proxy verbinden.

   Die auf mobilen Benutzergeräten installierte GlobalProtect-App sendet Datenverkehr an Prisma Access.
2. Richten Sie die Infrastruktur ein.

   Richten Sie grundlegende Infrastruktureinstellungen ein und konfigurieren Sie dann die Infrastruktureinstellungen, die für Ihren Verbindungstyp (GlobalProtect oder expliziter Proxy) spezifisch sind.

   Eine Proxy-Autokonfigurationsdatei (PAC) auf mobilen Benutzergeräten leitet den Browserdatenverkehr zu Prisma Access um.
3. Wählen Sie den Prisma Access-Standort aus.

   Die Karte zeigt die globalen Regionen, in denen Sie Prisma Access für Benutzer bereitstellen können: Nordamerika, Südamerika, Europa, Afrika, Naher Osten, Asien, Japan und ANZ (Australien und Neuseeland). Darüber hinaus bietet Prisma Access mehrere Standorte innerhalb der einzelnen Regionen, um sicherzustellen, dass Ihre Benutzer eine Verbindung zu einem Standort herstellen können, der eine auf den Standort des Benutzers zugeschnittene Benutzererfahrung bietet. Wählen Sie „Alle auswählen“, um die beste Leistung zu erzielen. Wählen Sie alternativ bestimmte Standorte innerhalb der einzelnen ausgewählten Regionen aus, für die Ihre Benutzer Zugriffsrechte benötigen. Indem Sie Ihre Bereitstellung auf eine einzelne Region beschränken, können Sie die von Ihnen bereitgestellten Regionen genauer steuern und Regionen ausschließen, wenn Ihre Richtlinien oder Branchenvorschriften dies erfordern.
4. Fügen Sie die Prisma Access-Standorte hinzu.

   Konfigurieren Sie die Einstellungen, um die Prisma Access-Standorte hinzuzufügen, an denen Sie Ihre Benutzer unterstützen möchten.
5. Authentifizieren Sie mobile Benutzer.

   Richten Sie die Benutzerauthentifizierung ein, damit nur legitime Benutzer Zugriff auf Ihre Dienste und Anwendungen erhalten. Um Ihr Setup zu testen, können Sie Benutzer hinzufügen, die Prisma Access lokal authentifiziert. Alternativ können Sie direkt mit der Einrichtung der Authentifizierung auf Unternehmensebene fortfahren.

Nachdem Sie Ihre anfängliche Konfiguration an Prisma Access übertragen haben, beginnt Prisma Access mit der Bereitstellung der Umgebung Ihrer mobilen Benutzer. Dies kann bis zu 15 Minuten dauern. Sobald die Standorte Ihrer mobilen Benutzer eingerichtet sind, können Sie diese auf der

Einrichtungsseite für mobile Benutzer, auf der Übersichtsseite und innerhalb von Prisma Access Insights einsehen.

Hier finden Sie weitere Informationen zu mobilen Prisma Access-Benutzern.

## Workflows: Remote-Netzwerke

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | Prisma Access-Lizenz |

Wenn Sie die Verbindung von Remote-Netzwerken mit Prisma Access vorbereiten, müssen Sie wissen, wie viele Standorte Sie einbinden möchten. Mithilfe dieser Informationen können Sie die Verbindungsanforderungen ermitteln, beispielsweise wie der Datenverkehr über Prisma Access weitergeleitet wird. Wenn Sie die Bereitstellung Ihres Remote-Netzwerks planen, müssen Sie wissen, welche Anwendungen Prisma Access durchlaufen, um die optimalen Sicherheitsrichtlinienregeln entsprechend zu konfigurieren. Ebenso wichtig ist es, Ihre Bedrohungsprofil-Konfiguration einzurichten. Darüber hinaus sollten Sie im Rahmen einer konsequenten Strategie zur Bedrohungsminderung die Anwendung einheitlicher Bedrohungs-, URL- und WildFire-Scans auf alle Regeln in Betracht ziehen.

Weitere Informationen finden Sie unter Prisma Access-Remote-Netzwerke.

## Workflows: Dienstverbindungen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | Prisma Access-Lizenz |

Dienstverbindungen ermöglichen sowohl mobilen Benutzern als auch Benutzern in Ihren Zweigstellennetzwerken den Zugriff auf Ressourcen in Ihrem Hauptsitz oder Rechenzentrum. Neben dem Zugriff auf Unternehmensressourcen ermöglichen Dienstverbindungen Ihren mobilen Benutzern auch die Verbindung zu Zweigstellen.

Wählen Sie **Workflows** > **Einrichtung Prisma Access** > **Dienstverbindungen** aus, um eine Dienstverbindung hinzuzufügen.

Der erste Tunnel, den Sie erstellen, ist der primäre Tunnel für die Dienstverbindung. Wiederholen Sie diesen Workflow, um optional einen sekundären Tunnel einzurichten. Wenn beide Tunnel aktiv sind, hat der primäre Tunnel Vorrang vor dem sekundären Tunnel. Wenn der primäre Dienstverbindungstunnel ausfällt, wird die Verbindung auf den sekundären Tunnel umgestellt, bis der primäre Tunnel wieder verfügbar ist. Abhängig vom IPSec-Gerät, das Sie zum Aufbau des Tunnels verwenden, bietet Prisma Access integrierte, empfohlene IKE- und IPSec-Sicherheitseinstellungen. Sie können die empfohlenen Einstellungen für den Einstieg verwenden oder sie nach Bedarf an Ihre Umgebung anpassen.

Weitere Informationen finden Sie unter Prisma Access-Dienstverbindungen.

# Workflows: Remote-Browser-Isolation

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access 5.0 Innovation<br>❑ Prisma Access-Lizenz mit dem Lizenzabonnement für mobile Benutzer oder Remote-Netzwerke<br>❑ Remote-Browser-Isolation-Lizenz |

Remote-Browser-Isolation (RBI) von Palo Alto Networks ist eine Lösung, die alle Browseraktivitäten von den verwalteten Geräten und Unternehmensnetzwerken Ihrer Benutzer isoliert und an eine externe Entität überträgt, wie z. B. Prisma Access, das potenziell schädlichen Code und Inhalt innerhalb ihrer Plattform isoliert und Sie so davor schützt.

RBI ist nativ in Prisma Access integriert und ermöglicht es Ihnen, Isolationsprofile problemlos auf vorhandene Sicherheitsrichtlinien anzuwenden. Der gesamte Datenverkehr wird isoliert analysiert und einer Bedrohungsabwehr unterzogen, die von Cloud-Delivered Security Services (CDSS) wie Fortschrittliche Bedrohungsabwehr, Advanced WildFire, Erweiterte URL-Filterung, DNS Security und SaaS-Sicherheit bereitgestellt wird.

Überlegen Sie bei der Vorbereitung des Benutzer-Onboardings in RBI, welche URL-Kategorien Sie für das isolierte Webbrowsing Ihrer Benutzer aktivieren möchten. Überlegen Sie, welche Browseraktionen Sie Ihren Benutzern verbieten möchten, etwa Kopier- und Einfügefunktionen, Tastatureingaben und Freigabeoptionen wie das Hochladen, Herunterladen und Drucken von Dateien.

Weitere Informationen finden Sie unter Remote-Browser-Isolation.

# Workflows: Software-Upgrades

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• NGFW (Managed by Strata Cloud Manager) | • Mindestens eine dieser Lizenzen ist erforderlich, um Ihre Konfiguration mit Strata Cloud Manager zu verwalten; für die einheitliche Verwaltung von NGFWs und Prisma Access benötigen Sie sowohl NGFW- als auch Prisma Access-Lizenzen:<br>❑ Prisma Access-Lizenz<br>❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>❑ Strata Cloud Manager Pro |

Verwenden Sie Strata Cloud Manager zur Planung und Verwaltung Ihrer Software-Upgrades für NGFW und Prisma Access. Dies sind die Workflows, die Sie ausführen können:

- Upgrade-Empfehlungen: Erstellen Sie Empfehlungen, um die beste Softwareversion für Ihre Geräte zu ermitteln, auf die sie aktualisiert werden können. Die Funktion „Empfehlungen zum Software-Upgrade“ analysiert die auf Firewalls aktivierten Funktionen und bietet eine individuelle Empfehlung.
- Prisma Access-Upgrade-Dashboard Wählen Sie ein bevorzugtes Zeitfenster für bestimmte Prisma Access-Upgrades aus.
- NGFW – Zeitplaner: Planen Sie ein PAN-OS-Softwareupdate, um Ihre Firewalls zu einem Datum und Zeitpunkt Ihrer Wahl auf eine PAN-OS-Zielversion zu aktualisieren oder herunterzustufen.
- NGFW
- Prisma Access

## Software-Upgrades (NGFW)

Wählen Sie **Workflows** > **Software-Upgrades** > **Empfehlungen für Upgrade** aus, um die Upgrades Ihrer Geräte zu planen, indem Sie sie analysieren und Empfehlungen für Upgrades erstellen.

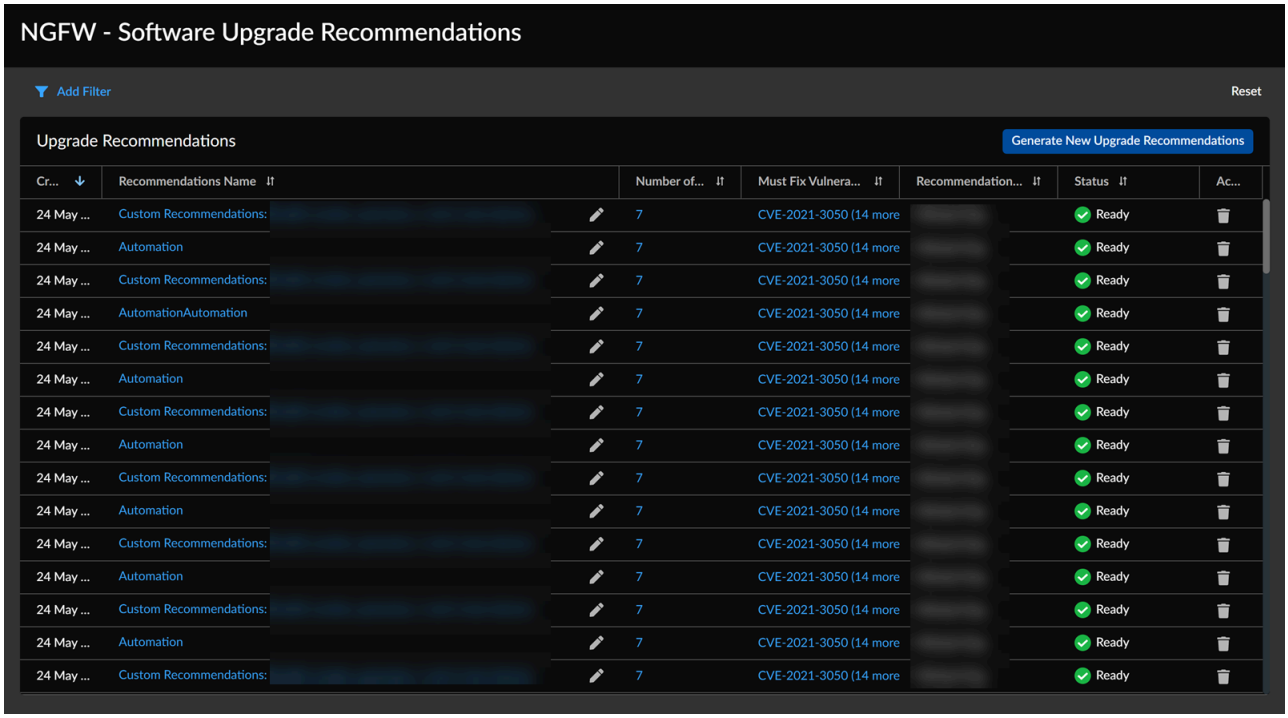
### Empfehlungen für Upgrade

Unter **Workflows** > **Software-Upgrades** > **Empfehlungen für Upgrade** können Sie Empfehlungen erstellen, um die beste Softwareversion für Ihre Geräte zu ermitteln, auf die sie aktualisiert werden können. Die Funktion „Empfehlungen zum Software-Upgrade“ analysiert die auf Firewalls aktivierten Funktionen und bietet eine individuelle Empfehlung, die Folgendes umfasst:

- beste Softwareversion für Ihre Geräte, auf die sie aktualisiert werden können
- Informationen zu neuen Funktionen, Verhaltensänderungen, Sicherheitslücken und Softwareproblemen in jeder empfohlenen Softwareversion

Die verschiedenen Arten der Upgrade-Empfehlungen lauten:

- systemgenerierte Empfehlungen, die jede Woche generiert werden und die vorgeschlagenen Upgrade-Optionen enthalten
- benutzerdefinierte Empfehlungen, die basierend auf den ausgewählten Geräten für bestimmte CVEs in der Zusammenfassung der Sicherheitsempfehlung generiert werden
- benutzergenerierte Empfehlungen, die auf Grundlage einer hochgeladenen TSF-Datei (Tech Support File) einer Firewall generiert werden




Für jeden Plan in **Empfehlungen für Upgrade** haben Sie folgende Möglichkeiten:

- Zeigen Sie die Anzahl der Geräte, die ein Upgrade erfordern, und die Sicherheitslücken an, die behoben werden müssen.
- Bearbeiten Sie den Namen eines Empfehlungsberichts, um benutzerdefinierte Berichte zu unterscheiden.
- Filtern Sie die Empfehlungsberichte nach Erstellungsdatum, Planname und generierten Empfehlungen.
- Löschen Sie eine Upgrade-Empfehlung, die fehlgeschlagen oder nicht mehr erforderlich ist.

Klicken Sie auf einen Empfehlungsbericht, um den detaillierten Bericht mit den Upgrade-Optionen für die Geräte anzuzeigen. Wählen Sie eine Upgrade-Option aus, um Details zu **neuen Funktionen**, **bekannten Sicherheitslücken in PAN-OS**, **Verhaltensänderungen** und **bekannten Probleme in PAN-OS** anzuzeigen. Bei einem bekannten Problem unter **Bekannte Probleme in PAN-OS** wird der Wert unter **Zugehörige Fallzahl** anhand der Anzahl der Kunden ermittelt, die dieses Problem gemeldet haben.

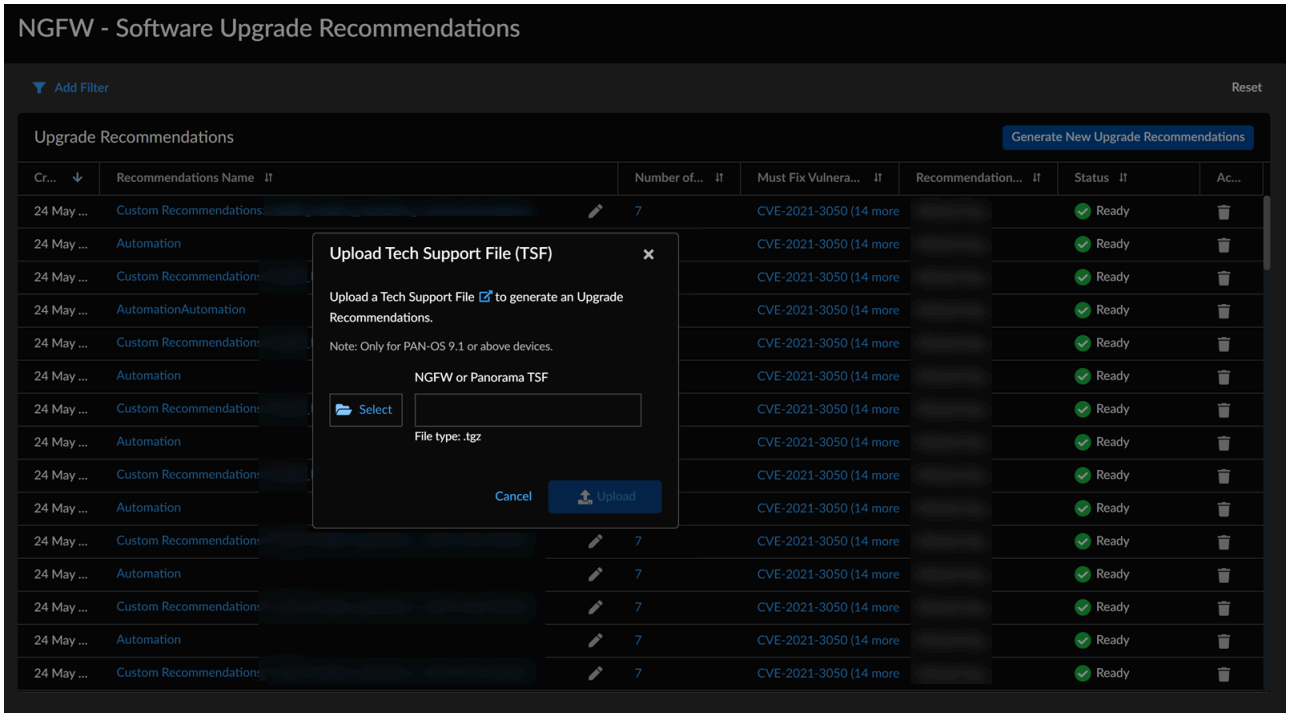
Klicken Sie auf **Exportieren**, um diesen Bericht im CSV-Format herunterzuladen.

### Generieren von On-Demand-Empfehlungen für Software-Upgrades

1. Navigieren Sie zu **Workflows > Software-Upgrades > Empfehlungen für Upgrade**.
2. Wählen Sie **Neue Upgrade-Empfehlungen generieren**.
3. Wählen Sie über **Auswählen** eine TSF-Datei (Tech Support Datei) aus und wählen Sie **Upload** aus.

   - *Sie können jeweils eine TSF-Datei von nur einem Gerät hochladen und die TSF-Datei muss im .tgz-Dateiformat vorliegen.*
   - *Die Funktion „Empfehlungen zum Software-Upgrade“ unterstützt bei der Berichterstellung TSF-Dateien von Geräten mit PAN-OS-Version 9.1 oder höher.*




4. Zeigen Sie Empfehlungen für Software-Upgrades an, nachdem der Status als **Bereit** angezeigt wird. Sie können auch in der Spalte **Status** nachsehen, ob Fehler im Zusammenhang mit dem Upload, Dateiformat oder der Verarbeitung der TSF-Datei aufgetreten sind.

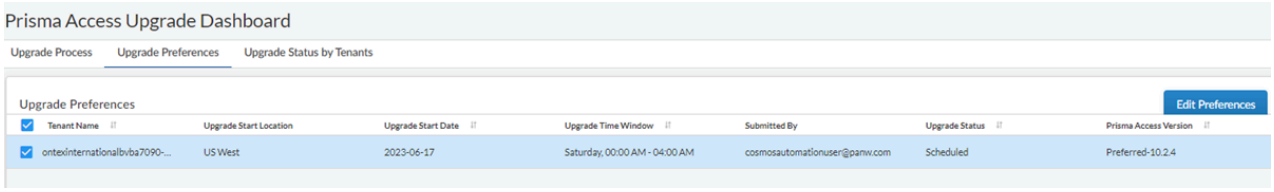
## Software-Upgrades (Prisma Access)

Wählen Sie **Workflows** > **Software-Upgrades** > **Prisma Access**, um Informationen zum Dataplane-Upgrade-Prozess von Prisma Access anzuzeigen.

Mögliche Aktionen:

- Verstehen Sie den Dataplane-Upgrade-Prozess von Prisma Access.
- Wählen Sie Ihre Upgrade-Einstellungen:




Wählen Sie einen Mandantennamen aus, um Ihre Upgrade-Einstellungen auszuwählen. Weitere Informationen finden Sie unter Auswählen eines bevorzugten Zeitfensters für bestimmte Prisma Access-Upgrades.

# Workflows: Prisma Access Browser

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access mit Bundle-Lizenz für Prisma Access Browser<br>❑ Superuser- oder Prisma Access Browser-Rolle |

Wählen Sie **Workflows** > **Einrichtung Prisma Access** > **Prisma Access Browser** aus, um mit dem Onboarding von Prisma Access Browser zu beginnen.

Prisma Access Secure Enterprise Browser (Prisma Access Browser) ist die einzige Lösung, die sowohl verwaltete als auch nicht verwaltete Geräte über einen nativ integrierten Unternehmensbrowser schützt, der den Schutz auf nicht verwaltete Geräte ausweitet. Siehe Was ist der Prisma Access Browser?.

Das Onboarding umfasst eine Reihe von Schritten, in denen Sie die folgenden Elemente konfigurieren:

- Benutzerauthentifizierung und Gruppen
- Prisma Access-Integration
- Routing
- Durchsetzen von SSO-Anwendungen
- Herunterladen und Verteilen
- Browserrichtlinie

Binden Sie Prisma Access Browser in Strata Cloud Manager ein.

# Berichte: Strata Cloud Manager

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)*<br>• NGFWs<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)*<br>• Prisma SD-WAN | ❑ Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>❑ Prisma Access<br>❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>❑ Strata Cloud Manager Essentials<br>❑ Strata Cloud Manager Pro<br>❑ Prisma SD-WAN<br>❑ Software-NGFW-Credits<br>*(für Software-NGFWs der VM-Series)*<br>❑ Lizenz für WAN Clarity-Bericht<br>❑ Eine Rolle, die zum Herunterladen, Freigeben und Planen von Berichten berechtigt ist. |

Erhalten Sie Berichte zu Netzwerkverkehrsmustern, Bandbreitennutzung und Ihren Sicherheitsabonnementdaten in Strata Cloud Manager. Berichte bieten aussagekräftige Einblicke in Ihr Netzwerk, die Sie für Planungs- und Überwachungszwecke verwenden können. Berichte werden in bestimmten Prisma Access- und NGFW-Dashboards, in der Activity Insights-Übersicht sowie in Prisma SD-WAN unterstützt. Prisma Access- und NGFW-Benutzer, die vollen Zugriff auf das Dashboard haben, können Dashboard-Daten als PDF herunterladen, den Bericht innerhalb ihrer Organisation freigeben und Berichte planen, damit sie in regelmäßigen Abständen an ihren E-Mail-Posteingang gesendet werden. Berichte sind ein lizenzierter Abonnementdienst in Prisma SD-WAN. Sie können Berichte von Controllern sowie über Standorte und Schaltungen hinweg in Prisma SD-WAN herunterladen und anzeigen.

Folgende Berichte können Sie in Strata Cloud Manager anzeigen:

- Prisma Access und NGFW – Sie können Berichte aus den Prisma Access- und NGFW-Dashboards und Activity Insights generieren. Diese Symbole  oben rechts im Dashboard weisen darauf hin, dass Berichte für dieses Dashboard unterstützt werden. Sie können Berichte auch direkt über das Menü **Berichte** Berichte generieren, herunterladen, freigeben und planen.
- Prisma SD-WAN – Sehen Sie sich die folgenden WAN Clarity-Berichte an:
  - WAN Clarity-Zweigstellenberichte
  - WAN Clarity-Rechenzentrumsberichte
  - Berichte zur aggregierten Bandbreitennutzung
- Prisma Access und NGFW

- Prisma SD-WAN

# Berichte (Prisma Access und NGFW)

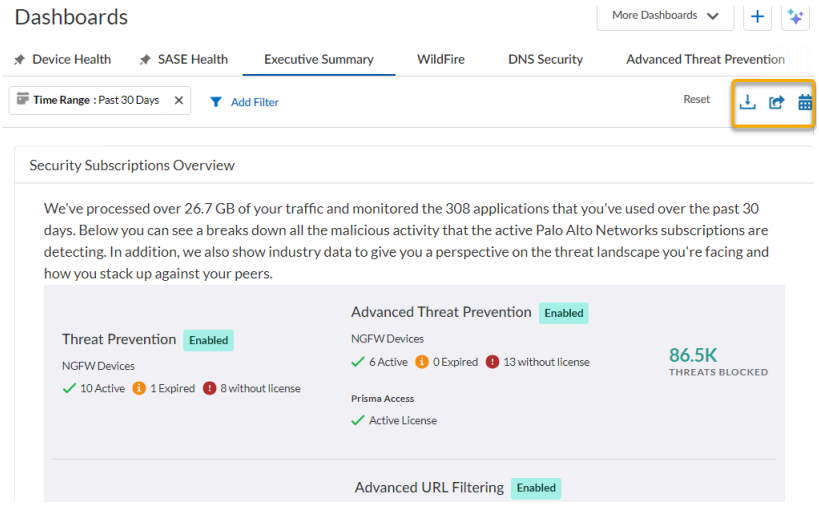
Die Dashboards und die Zusammenfassung der Activity Insights können innerhalb Ihrer Organisation als PDF-Berichte geteilt werden. Außerdem können Sie Berichte so planen, dass sie in regelmäßigen Abständen (täglich, wöchentlich oder monatlich) an Ihren E-Mail-Posteingang – und an die Postfächer Ihrer Kollegen – gesendet werden.

Damit Sie Berichte problemlos mit Personen in Ihrer Organisation teilen können, richten Sie die Cloud Identity Engine (Verzeichnissynchronisierung) für diese App ein. Die Cloud Identity Engine gewährt Apps schreibgeschützten Zugriff auf Ihre Active Directory-Informationen. Wenn die Cloud Identity Engine eingerichtet ist, können Sie einem geplanten Bericht problemlos Empfänger hinzufügen. Ihre Berichtsempfänger werden mit der Cloud Identity Engine abgeglichen. Wenn keine Übereinstimmung gefunden wird, wird ein zusätzlicher Validierungsschritt ausgeführt, indem ihre E-Mail-Domäne mit den E-Mail-Domänen abgeglichen wird, die Ihrem Supportkonto zugeordnet sind. Diese Prüfungen stellen sicher, dass keine Berichte außerhalb Ihrer Organisation gesendet werden.

Sie können Berichte direkt über das Menü **Berichte**, über die jeweilige **Dashboard**-Seite oder über die Seite **Insights** > **Activity Insights** > **Übersicht** herunterladen, freigeben oder planen. Berichte werden als PDFs geteilt und heruntergeladen.

So laden Sie einen Bericht herunter, geben ihn frei oder planen ihn:

**STEP 1 |** Klicken Sie auf eines der Symbole auf der **Dashboard**-Seite oder auf der Seite **Insights** > **Activity Insights** > **Übersicht**.

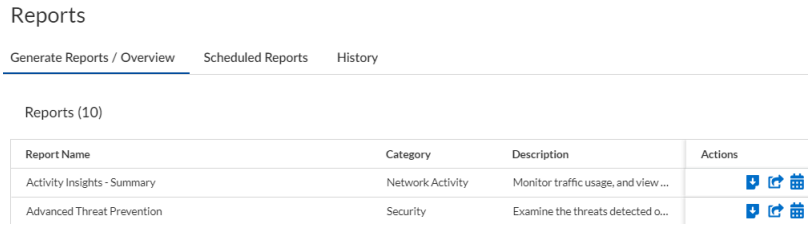



Oder

Klicken Sie auf **Strata Cloud Manager** > **Berichte** > **Berichte/Übersicht generieren** und wählen Sie eines dieser Symbole aus der Liste der Berichtsformate aus. Standardmäßig werden Berichte mit den Daten der letzten 24 Stunden oder 30 Tage erstellt, je nach Art des

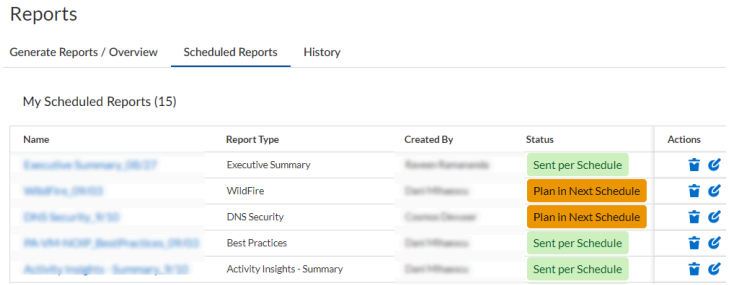
Dashboards, für das Sie den Bericht erstellen. Sie können den Zeitraum, für den Sie im Bericht Daten erfassen möchten, beim Planen des Berichts anpassen.




**STEP 2 |** Wenn Sie einen Bericht planen, müssen Sie weiterhin die Berichtsparameter definieren, darunter:

- **Zeitraum**, für den Daten gesammelt werden sollen
- **Wiederholung**, also die Häufigkeit, mit der der Bericht gesendet werden soll (täglich, wöchentlich oder monatlich)

Sie können alle geplanten Berichte auf der Registerkarte **Strata Cloud Manager** > **Berichte** > **Geplante Berichte** anzeigen, bearbeiten oder löschen.




**Der Verlauf** zeigt alle in den letzten 30 Tagen heruntergeladenen Berichte.

# Berichte (Prisma SD-WAN)

Prisma SD-WAN WAN Clarity-Berichte bieten eine Gesamtansicht der Verkehrsverteilung und Bandbreitennutzung in Ihrem Netzwerk. Sie können das gesamte Berichtspaket herunterladen oder die Berichte vom Prisma SD-WAN-Controller anzeigen. Das ermöglicht wöchentliche Trendvergleiche sowie Vergleiche zwischen Standorten und Schaltkreisen.

Berichte stehen zur sofortigen Verwendung als lizenzierter Abonnementdienst zur Verfügung. Wenden Sie sich an das Prisma SD-WAN-Vertriebsteam, um das Abonnement zu aktivieren.

Der Prisma SD-WANWAN Clarity-Berichte umfassen:

- WAN Clarity-Zweigstellenberichte
- WAN Clarity-Rechenzentrumsberichte
- Berichte zur aggregierten Bandbreitennutzung

So zeigen Sie Berichte an:

**STEP 1 |** Wählen Sie **Berichte** > **Prisma SD-WAN** aus.

**STEP 2 |** Klicken Sie unter **WAN Clarity-Berichte** auf **Berichte anzeigen**.

**STEP 3 |** Wählen Sie einen **Zeitbereich** aus und wählen Sie im Feld **Bericht für** eine der folgenden Optionen aus.

- **Zweig**
- **Rechenzentrum**
- **Aggregierte Bandbreitennutzung**

# Favoriten: Strata Cloud Manager

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)*<br>• NGFWs<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)* | ❑ Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>❑ Prisma Access<br>❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>❑ Strata Cloud Manager Essentials<br>❑ Strata Cloud Manager Pro<br>❑ jede von Mandant oder Mandanten-Dienstgruppe (TSG) unterstützte Anwendung<br>❑ eine Rolle, die Ihren Anforderungen entspricht |

Mit der Favoriten-Funktion können Sie interessante Elemente speichern und dann bei Bedarf an jedem Ort in Strata Cloud Manager schnell darauf zugreifen. Sie können die Namen Ihrer bevorzugten Menüelemente in Ihrer eigenen privaten Liste personalisieren, indem Sie den Inhalt Ihrer Liste organisieren, bearbeiten und löschen.

Verwalten Sie Favoriten wie folgt:

- Favoriten hinzufügen
- Favoriten anzeigen
- Favoriten bearbeiten
- Favoriten löschen

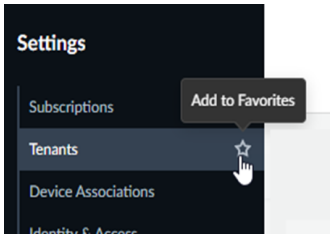
# Favoriten hinzufügen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)*<br>• NGFWs<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)* | ❑ Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>❑ Prisma Access<br>❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>❑ Strata Cloud Manager Essentials<br>❑ Strata Cloud Manager Pro<br>❑ jede von Mandant oder Mandanten-Dienstgruppe (TSG) unterstützte Anwendung<br>❑ eine Rolle, die Ihren Anforderungen entspricht |

Wenn Sie Menüpunkte oder Seiten in Strata Cloud Manager haben, die Sie immer wieder aufrufen müssen, Sie aber nicht mehr suchen oder dorthin navigieren möchten, können Sie diese in einer Favoritenliste speichern.

**STEP 1 |** Navigieren Sie zu dem Menüpunkt oder der Seite, den oder die Sie speichern möchten.

**STEP 2 |** Bewegen Sie den Mauszeiger über das Element, um das Sternsymbol anzuzeigen.




**STEP 3 |** Wählen Sie den Stern aus, um dieses Element zu Ihren **Favoriten** hinzuzufügen.

*Die Menüelemente der obersten Ebene können nicht als Favoriten hinzugefügt werden. Nur Untermenüs können als Favoriten hinzugefügt werden.*

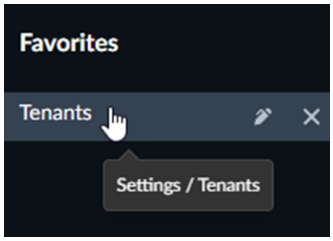
# Favoriten anzeigen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)*<br>• NGFWs<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)* | ❑ Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>❑ Prisma Access<br>❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>❑ Strata Cloud Manager Essentials<br>❑ Strata Cloud Manager Pro<br>❑ jede von Mandant oder Mandanten-Dienstgruppe (TSG) unterstützte Anwendung<br>❑ eine Rolle, die Ihren Anforderungen entspricht |

Nachdem Sie Favoriten hinzugefügt haben, können Sie Ihre Favoriten und deren ursprüngliche Standorte anzeigen.

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

**STEP 2 |** Bewegen Sie den Mauszeiger über das entsprechende Element, um das Standortsymbol anzuzeigen.




**STEP 3 |** Der Pfad zum aktuellen Standort sowie der Menüname werden angezeigt.

*Wenn Sie auf das Element in Ihrer Favoritenliste klicken, gelangen Sie zum ursprünglichen Standort.*

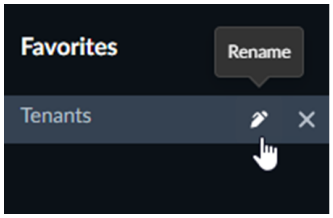
# Favoriten bearbeiten

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)*<br>• NGFWs<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)* | ❑ Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>❑ Prisma Access<br>❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>❑ Strata Cloud Manager Essentials<br>❑ Strata Cloud Manager Pro<br>❑ jede von Mandant oder Mandanten-Dienstgruppe (TSG) unterstützte Anwendung<br>❑ eine Rolle, die Ihren Anforderungen entspricht |

Nachdem Sie Favoriten hinzugefügt haben, können Sie Ihre Favoriten bearbeiten, um sie zu personalisieren.

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

**STEP 2 |** Bewegen Sie den Mauszeiger über das Element, um das Bearbeitungssymbol anzuzeigen.




**STEP 3 |** Benennen Sie das Element um.

*Durch das Umbenennen des Elements in Ihrer Favoritenliste wird das ursprüngliche Element an seinem ursprünglichen Standort nicht umbenannt.*

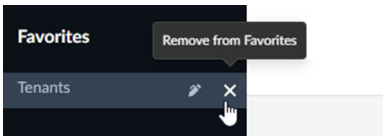
# Favoriten löschen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)*<br>• NGFWs<br>*(mit Strata Cloud Manager- oder Panorama-Konfigurationsmanagement)* | ❑ Jede dieser Lizenzen beinhaltet Zugriff auf Strata Cloud Manager:<br>❑ Prisma Access<br>❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app)<br>❑ Strata Cloud Manager Essentials<br>❑ Strata Cloud Manager Pro<br>❑ jede von Mandant oder Mandanten-Dienstgruppe (TSG) unterstützte Anwendung<br>❑ eine Rolle, die Ihren Anforderungen entspricht |

Nachdem Sie Favoriten hinzugefügt haben, können Sie Favoriten aus Ihrer Liste löschen.

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

**STEP 2 |** Bewegen Sie den Mauszeiger über das Element, um das Symbol „Löschen“ anzuzeigen.




**STEP 3 |** Klicken Sie auf das Symbol, um den Favoriten aus der Liste zu löschen.

*Durch das Löschen des Elements aus Ihrer Favoritenliste wird das ursprüngliche Element nicht von seinem ursprünglichen Speicherort entfernt.*

# Einstellungen: Strata Cloud Manager

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager) | ☑ jede von Mandant oder Mandanten-Dienstgruppe (TSG) unterstützte Anwendung<br>☐ eine Rolle, die Ihren Anforderungen entspricht<br>☐ Strata Logging Service zur Verwaltung von Protokollen |

In den **Einstellungen** können Sie die Prozesse verwalten, die sich auf alle in Strata Cloud Manager angebotenen Dienste beziehen. Zu diesen Prozessen gehören:

#### Abonnements

Zeigen Sie die genehmigten Abonnements für Ihr Produkt an.

Verwalten Sie Abonnements.

#### Device Associations

**Device Associations** wird am häufigsten beim Geräte- und Anwendungs-Onboarding verwendet und ermöglicht Ihnen Folgendes:

- neue Geräte einem Mandanten zuordnen
- Apps Ihren Geräten zuordnen
- Geräte- und App-Zuordnungen verwalten

Erste Schritte mit Gerätezuordnungen.

#### Produkte

Wenn Sie über eine Ein-Mandanten-Umgebung verfügen, können Sie Ihre Produkte anzeigen, starten und verwalten:

- Produktinformationen anfordern
- Instanz umbenennen
- Freigabe verwalten
- Mandanten hinzufügen

Erste Schritte mit der Produktverwaltung.

**Mandanten**

Wenn Sie ein Managed Security Service Provider (MSSP) oder ein verteiltes Unternehmen sind, können Sie eine Hierarchie aus Geschäftsorganisationen und -einheiten erstellen und verwalten, die durch Mandanten dargestellt wird. Unter **Mandanten** haben Sie folgende Möglichkeiten:

- Mandanten hinzufügen
- Mandanten bearbeiten
- Mandantenlizenzen verwalten
- Mandanten löschen
- von einer Ein-Mandaten- zu einer Mehrmandanten-Bereitstellung wechseln

Erste Schritte mit der Mandantverwaltung.

**Identität und Zugriff“ aus?**

Kontrollieren Sie die Authentifizierung und Autorisierung von Benutzerrollen und -berechtigungen für alle Anwendungen und den API-basierten Zugriff. Über „Identität und Zugriff“ können Sie Folgendes verwalten:

- Benutzerzugriff
- Dienstkonten
- Rollen
- Integration externer Identitätsanbieter

Erste Schritte mit Identität und Zugriff.

**Auditierungslog**

Zeigen Sie alle Aktionen an, die von Strata Cloud Manager-Benutzern initiiert wurden.

Zeigen Sie Auditierungslogs an.

**ION-Lizenzverwaltung**

Generieren Sie Autorisierungstoken für virtuelle ION-Geräte. Dies bietet eine Reihe von Kontrollen, um das unbefugte Hinzufügen virtueller Geräte zu einer Umgebung zu verhindern.

Verwalten Sie ION-Lizenzen.

**Benutzereinstellungen**

Passen Sie Ihre Einstellungen Ihren Bedürfnissen an. Wählen Sie beispielsweise Ihren Anzeigemodus aus.

Konfigurieren Sie Benutzereinstellungen.

**Liste vertrauenswürdiger IP-Adressen**

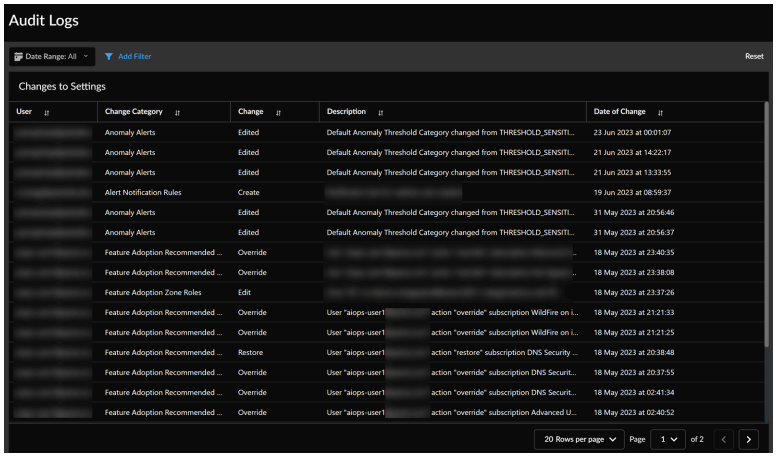
Verwenden Sie vertrauenswürdige IP-Listen, um den Zugriff auf Ihre Anwendungen einzuschränken, indem Sie pro Mandant zulässige IP-Adressen angeben.

Konfigurieren Sie eine Liste vertrauenswürdiger IP-Adressen.

# Einstellungen: Auditierungslog

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Strata Cloud Manager | ❑ Eine der folgenden Komponenten:<br>• AIOps for NGFW Free-App<br>• AIOps for NGFW Premium (verwenden Sie die Strata Cloud Manager-App)<br>• Strata Cloud Manager Essentials<br>• Strata Cloud Manager Pro<br>❑ Eine der folgenden vordefinierten Rollen: Auditor, Geschäftsadministrator, Datensicherheitsadministrator, Bereitstellungsadministrator, IAM-Administrator, Mehrmandanten-IAM-Administrator, Mehrmandanten-Verwaltungsbenutzer, Mehrmandanten-Monitorbenutzer, Mehrmandanten-Superuser, Netzwerkadministrator, Sicherheitsadministrator, SOC-Analyst, Superuser, Tier-1-Support, Tier-2-Support, Administrator mit schreibgeschütztem Zugriff |

Unter **Einstellungen > Auditierungslogs** können Sie eine Liste der von Strata Cloud Manager-Benutzern eingeleiteten Aktionen sehen. Hier finden Sie Protokolle der vorgenommenen Änderungen, den Eigentümer der Änderung, das Datum und die Uhrzeit der Änderung sowie eine Beschreibung der Änderung. Sie können diese Protokolle zu Compliance- und Fehlerbehebungszwecken verwenden. Sie können die Auditierungslogs nach Datumsbereich, Benutzer, Kategorie und Änderungstyp filtern.



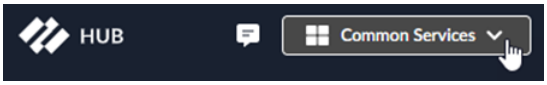
# Einstellungen: Liste vertrauenswürdiger IP-Adressen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Strata Cloud Manager | ❑ IAM-Rolle „Superuser“, „Mehrmandanten-Superuser“, „Mehrmandanten-IAM-Administrator“ oder eine beliebige benutzerdefinierte Rolle mit dem Berechtigungssatz „Liste vertrauenswürdiger IP-Adressen“ |

Über die Cloud bereitgestellte Anwendungen bieten den Vorteil, dass sie von jedem Ort der Welt aus zugänglich sind. Allerdings besteht dabei das Risiko, dass Benutzer mit gestohlenen Anmeldedaten auf Anwendungen zugreifen oder dass Wörterbuchangriffe oder andere Formen von Brute-Force-Angriffen auftreten.

Zwar mindert Identitäts- und Zugriffsmanagement einige dieser Risiken, doch mithilfe vertrauenswürdiger IP-Listen können Sie den Zugriff auf Ihre Anwendungen zusätzlich einschränken, indem Sie IP-Adressen angeben, die pro Mandant zulässig sind.

Beim Erstellen eines neuen Mandanten kann standardmäßig jede IP-Adresse auf die Weboberfläche und die API zugreifen. Die Liste vertrauenswürdiger IP-Adressen ist eine Liste von IP-Adressen, die auf Ihren Mandanten zugreifen dürfen. Sie können eine vertrauenswürdige IP-Liste verwenden, um den Zugriff auf einen einzelnen Mandanten zu beschränken oder um den Zugriff auf einen übergeordneten Mandanten und seine untergeordneten Elemente in einer mandantenübergreifenden Hierarchie zu beschränken. Wenn Sie in einer Hierarchie mit mehreren Mandanten dem übergeordneten Mandanten eine Liste vertrauenswürdiger IPs hinzufügen, wird die Liste vom übergeordneten Mandanten an seine untergeordneten Mandanten vererbt und von oben nach unten durchgesetzt.

| So verwalten Sie eine Liste vertrauenswürdiger IP-Adressen über Strata Cloud Manager | So verwalten Sie eine Liste vertrauenswürdiger IP-Adressen den hub |
|---|---|
| Um eine Liste vertrauenswürdiger IP-Adressen über Strata Cloud Manager zu verwalten, wählen Sie **Einstellungen** > **Liste vertrauenswürdiger IP- Adressen** aus.<br>  <br>Sie können Listen vertrauenswürdiger IP-Adressen über Strata Cloud Manager verwalten. Hierdurch gewähren die Strata Cloud Manager-Weboberfläche und -API nur vertrauenswürdigen IP-Adressen Zugriff. | Um eine Liste vertrauenswürdiger IP-Adressen im hub zu verwalten, wählen Sie **Hub-Mandantenansicht** > **Allgemeine Dienste** > **Liste vertrauenswürdiger IP-Adressen** aus.<br>  <br>Sie können Listen vertrauenswürdiger IP-Adressen im hub verwalten. Der hub selbst ist jedoch von der Durchsetzung vertrauenswürdiger IP-Adressen ausgenommen, sodass der Zugriff auf den hub nicht auf vertrauenswürdige IP-Adressen beschränkt ist. Wenn Ihre IP-Adresse von |

| So verwalten Sie eine Liste vertrauenswürdiger IP-Adressen über Strata Cloud Manager | So verwalten Sie eine Liste vertrauenswürdiger IP-Adressen den hub |
|---|---|
| | einem Mandanten in Strata Cloud Manager blockiert wird, auf den Sie eigentlich Zugriff haben sollten, können Sie zum hub wechseln und den Zugriff freischalten, sofern Sie über die aufgeführten Berechtigungen verfügen. |

- Hinzufügen vertrauenswürdiger IPs
- Löschen vertrauenswürdiger IPs
- Freischalten des Zugriffs

## Vertrauenswürdige IPs hinzufügen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Strata Cloud Manager | ☐ IAM-Rolle „Superuser“, „Mehrmandanten-Superuser“, „Mehrmandanten-IAM-Administrator“ oder eine beliebige benutzerdefinierte Rolle mit dem Berechtigungssatz „Liste vertrauenswürdiger IP-Adressen“ |

Nachdem Sie Ihre Lizenz aktiviert und Ihre Mandanten erstellt haben und den Benutzerzugriff auf Strata Cloud Manager verwalten, können Sie den Zugriff auf Ihre Mandanten weiter einschränken, indem Sie einer Liste vertrauenswürdiger IPs vertrauenswürdige IP-Adressen hinzufügen. Standardmäßig erhält jede IP-Adresse Zugriff.

Fügen Sie vertrauenswürdige IPs mit Strata Cloud Manager hinzu.

**STEP 1 |** Wählen Sie **Einstellungen** > **Liste vertrauenswürdiger IPs**.

**STEP 2 |** Suchen oder scrollen Sie, um Ihren Mandanten zu finden und auszuwählen.

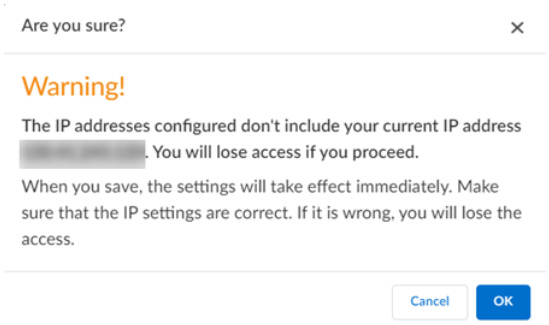
**STEP 3 |** Wählen Sie **Neue Quelle hinzufügen**.

**STEP 4 |** Geben Sie eine **IP-Adresse** ein, die auf diesen Mandanten zugreifen kann.

- Das Feld unterstützt die CIDR-Notation. Nur IPv4-Adressen sind zulässig.
- Sie können eine einzelne IP-Adresse verwenden oder einen Bereich mit einer Subnetzmaske wie 12.12.12.1/30 angeben.
- IP und Bereich werden validiert, wobei Fehler für nicht unterstützte Elemente angezeigt werden.
- Das Feld **Hingefügt von** wird automatisch ausgefüllt.


**STEP 5 |** Klicken Sie auf **Speichern**.

*Die Änderung tritt sofort in Kraft; stellen Sie also sicher, dass Ihre IP-Adresse korrekt ist, da Sie ansonsten den Zugriff auf den Mandanten verlieren können.*




**STEP 6 |** Nachdem Sie dem übergeordneten Mandanten eine Liste vertrauenswürdiger IPs hinzugefügt haben, wird die Liste vom übergeordneten Mandanten an seine untergeordneten Mandanten vererbt und von oben nach unten durchgesetzt. Untergeordnete Mandanten können auch eine eigene Liste hinzufügen.

## Löschen vertrauenswürdiger IPs

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Strata Cloud Manager | ☐ IAM-Rolle „Superuser“, „Mehrmandanten-Superuser“, „Mehrmandanten-IAM-Administrator“ oder eine beliebige benutzerdefinierte Rolle mit dem Berechtigungssatz „Liste vertrauenswürdiger IP-Adressen“ |

Nachdem Sie einer Liste vertrauenswürdiger IPs für Ihren Mandanten vertrauenswürdige IPs hinzugefügt haben, können Sie die Zugriffseinschränkung aufheben, indem Sie die vertrauenswürdigen IP-Adressen löschen.

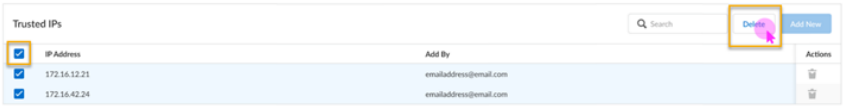
Löschen Sie vertrauenswürdige IPs mit Strata Cloud Manager.

**STEP 1 |** Wählen Sie **Einstellungen** > **Liste vertrauenswürdiger IPs**.

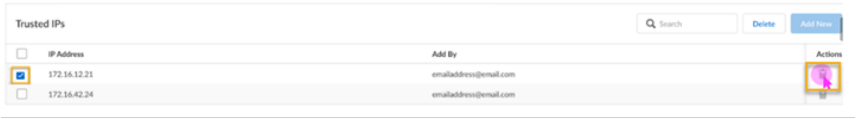
**STEP 2 |** Suchen oder scrollen Sie, um Ihren Mandanten zu finden und auszuwählen.

**STEP 3 |** Verwenden Sie eine der folgenden Optionen:

- Mehrere IPs löschen – Aktivieren Sie das Kontrollkästchen **IP-Adresse**, um alle IP-Adressen gleichzeitig zu markieren, und aktivieren Sie dann die Schaltfläche **Löschen**.




- Eine einzelne IP löschen – Aktivieren Sie das individuelle Kontrollkästchen der entsprechenden IP und wählen Sie dann **Aktionen** > **Löschen** aus.




*Wenn Sie eine vertrauenswürdige IP-Liste von einem übergeordneten Mandanten geerbt haben, können Sie sie nicht von einem untergeordneten Mandanten löschen. Sie können eine vertrauenswürdige IP-Liste eines Untermandanten nur löschen, wenn Sie sie direkt auf Untermandantenebene hinzugefügt haben.*

**STEP 4 |** Wählen Sie in der Eingabeaufforderung **OK** aus.

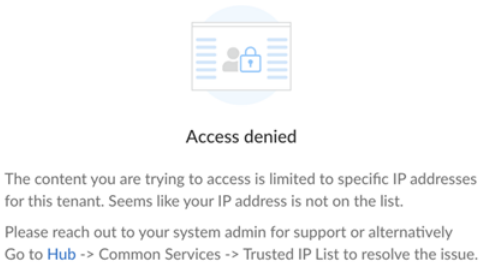
Die Änderung wird sofort wirksam. Wenn Sie alle vertrauenswürdigen IPs löschen, wird der IP-Zugriff auf **Beliebige** zurückgesetzt.

## Freischalten des Zugriffs

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Strata Cloud Manager | ❑ IAM-Rolle „Superuser“, „Mehrmandanten-Superuser“, „Mehrmandanten-IAM-Administrator“ oder eine beliebige benutzerdefinierte Rolle mit dem Berechtigungssatz „Liste vertrauenswürdiger IP-Adressen“ |

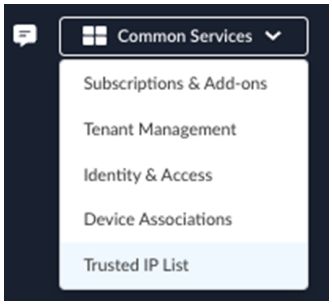
Nach dem Hinzufügen vertrauenswürdiger IPs zu einer Liste vertrauenswürdiger IP-Adressen für Ihren Mandanten wird der entsprechende Zugriff durch Strata Cloud Manager durchgesetzt. Wenn Ihre IP-Adresse nicht in der Liste vertrauenswürdiger IP-Adressen für den Mandanten enthalten ist, wird beim Versuch, darauf zuzugreifen, die Meldung „Zugriff verweigert“ angezeigt.




Wenn Ihre IP-Adresse von einem Mandanten blockiert wird, auf den Sie eigentlich Zugriff haben sollten, können Sie zum hub wechseln und den Zugriff freischalten, sofern Sie über die aufgeführten Berechtigungen verfügen.

**STEP 1 |** Wählen Sie im hub **Hub-Mandantenansicht** > **Allgemeine Dienste** > **Liste vertrauenswürdiger IP-Adressen**aus.




**STEP 2 |** Fügen Sie Ihre IP-Adresse hinzu zur Liste der vertrauenswürdigen IP-Adressen.

# Einstellungen: Benutzereinstellungen

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Strata Cloud Manager | Eine der folgenden Komponenten:<br>❑ AIOps for NGFW Free- oder AIOps for NGFW Premium-Lizenz<br>❑ Strata Cloud Manager Essentials<br>❑ Strata Cloud Manager Pro |

Unter **Einstellungen > Benutzereinstellungen** können Sie Strata Cloud Manager anpassen, um ihn auf Ihre speziellen Bedürfnisse zuzuschneiden, indem Sie die `Benutzereinstellungen` ändern. Zu diesen Einstellungen gehört Folgendes:

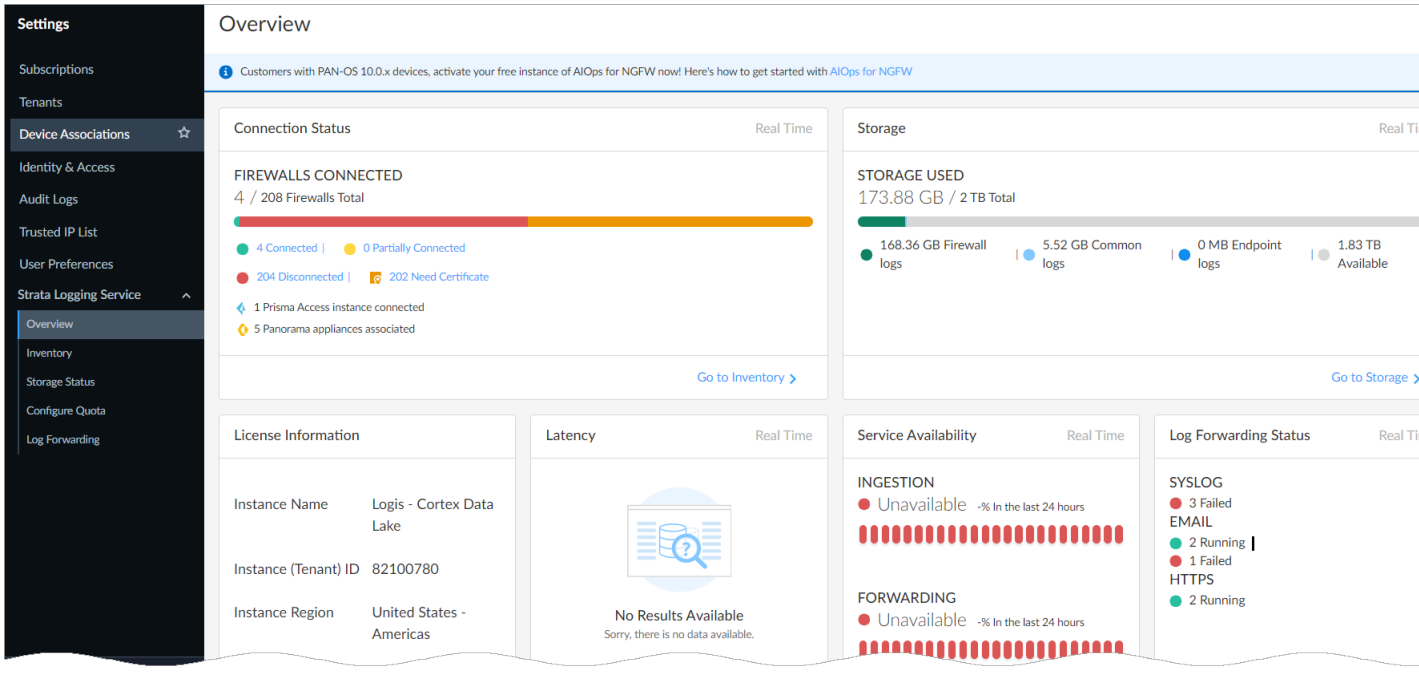
- **Heller/Dunkler/Systemmodus** – Wählen Sie zwischen dem dunklen und dem hellen Anzeigemodus oder folgen Sie Ihren eigenen Systemeinstellungen.

# Einstellungen: Strata Logging Service

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>• NGFW (Managed by PAN-OS or Panorama)<br>• NGFW (Managed by Strata Cloud Manager) | ☐ Strata Logging Service |

Strata Logging Service (früher Cortex Data Lake) ist ein cloudbasiertes Protokollierungssystem, das kontextreiche, erweiterte Netzwerkprotokolle speichert, die von unseren Sicherheitsprodukten generiert werden, darunter unsere NGFWs, Prisma Access und Cloud-NGFWs für AWS. Mit Strata Logging Service können Sie immer größere Datenmengen erfassen, ohne lokale Rechenleistung und Speicherung einplanen zu müssen – und er ist von Anfang an skalierbar. Erfahren Sie, wie Sie den Strata Logging Service in Ihrem Produkt aktivieren und bereitstellen.

*Darüber hinaus können Sie Protokolle auch mit der Strata Logging Service-App abrufen und verwalten, die im Hub verfügbar ist. Die Protokolldaten in der Strata Logging Service-App und in Strata Cloud Manager sind gleich, mit Ausnahme der Unterschiede in der Weboberfläche.*




Verwenden Sie Strata Logging Service für Folgendes:

- Überprüfung des Status einer Strata Logging Service-Instanz – Klicken Sie auf **Strata Logging Service** > **Übersicht**
- Anzeige und Onboarding von Firewalls, Cloud-NGFW, Prisma Access oder Panorama-Geräten – Klicken Sie auf **Strata Logging Service** > **Inventar**
- Anzeigen des zugewiesenen Protokollspeicherkontingents, des verfügbaren Speicherplatzes und der Anzahl der Tage, für die die Protokolle aufbewahrt werden (basierend auf Ihrer eingehenden Protokollrate) – Klicken Sie auf **Strata Logging Service** > **Speicherstatus**
- Konfigurieren des Protokollspeicherkontingents – Klicken Sie auf **Strata Logging Service** > **Kontingent konfigurieren**
- Suchen, Filtern und Exportieren von Protokolldaten – Klicken Sie auf **Vorfälle und Benachrichtigungen** > **Protokoll-Viewer**. Der Protokoll-Viewer hat dieselben Funktionen wie „Erkunden“ in der Strata Logging Service-App.
- Leiten Sie Protokolldaten weiter an externe Server zur Langzeitspeicherung, für SOC oder interne Audits. Klicken Sie auf **Strata Logging Service** > **Protokollweiterleitung**

# Anwendungserfahrung

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | Eine dieser Lizenzen:<br>❑ Prisma Access-Lizenz<br>❑ ADEM Observability-Lizenz oder AI-Powered ADEM-Lizenz |

Verwenden Sie die Seite **Anwendungserfahrung**, um Ihre Autonomous DEM-Benutzer und Remote-Standorte zu verwalten. Sehen Sie sich die Auditierungslogs an, um zu sehen, welche Administratoren sich während des ausgewählten **Zeitbereichs** bei Prisma Access authentifiziert haben.

Weitere Informationen zu den **Upgrade-Optionen** finden Sie unter Verwalten von Upgrades für Autonomous DEM-Agent.

## Endpunkt-Agent-Verwaltung

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | Eine dieser Lizenzen:<br>❑ Prisma Access-Lizenz<br>❑ ADEM Observability-Lizenz oder AI-Powered ADEM-Lizenz |

Über diese Registerkarte erhalten Sie Informationen zu allen registrierten ADEM-Benutzern, darunter, ob der Benutzer online (das Benutzergerät sendet Keep-alive-Nachrichten an den ADEM-Dienst) oder offline ist (der ADEM-Dienst hat in den letzten zehn Minuten keine Keep-alive-Nachricht vom Benutzergerät erhalten), wann das Benutzergerät zuletzt gesehen wurde, den Benutzernamen, den Gerätetyp und den Hostnamen des ADEM-Benutzers sowie Informationen dazu, welche ADEM-Agent-Version ausgeführt wird.

Jede Zeile der Tabelle in dieser Registerkarte stellt eindeutige Benutzer in einer separaten Zeile dar. Jede Benutzer-/Gerätekombination wird als eindeutiger Benutzer betrachtet. Wenn z. B. zwei Benutzer auf jeweils drei Geräten angemeldet sind, beträgt die Anzahl der eindeutigen Benutzer 6. Daher könnte ein Benutzername über mehrere Zeilen hinweg doppelt vorkommen – abhängig von der Anzahl der Geräte, bei denen er angemeldet ist.

Im Titel der Tabelle in diesem Widget gibt der Wert unter **Gesamte Endpunkt-Agents** die Gesamtzahl der überwachten Geräte an. Der Wert unter **Benutzer** ist die Gesamtzahl der Benutzer, unabhängig von der Anzahl der Geräte, bei denen sie angemeldet sind. Denn der Lizenzverbrauch basiert auf der Gesamtanzahl der Benutzer, unabhängig davon, bei wie vielen Geräten jeder Benutzer angemeldet ist.

Verwenden Sie die Kontrollkästchen links neben dem **zuletzt angemeldeten Benutzer**, um eine Massenkonfiguration vorzunehmen, indem Sie die Zeile für die Endpunkte auswählen. Wenn Sie einen Eintrag löschen, indem Sie ihn aus der Tabelle „Endpunkt-Agent-Verwaltung“ auswählen, wird der Lizenzeintrag freigegeben.

| Spaltenname | Beschreibung |
|---|---|
| Zuletzt angemeldeter Benutzer | Bei einem Gerät können sich mehrere Benutzer anmelden. Diese Spalte listet die Benutzer-ID des letzten Benutzers auf, der sich mit diesem Gerät bei GlobalProtect angemeldet hat. |
| Gerät | Das Betriebssystem, das auf diesem Gerät ausgeführt wird. |
| Hostname | Der Hostname des Geräts. |
| Zuletzt gesehen | Die letzte Nachricht, die vom Gerät an den DEM-Server gesendet wurde. |
| Zum ersten Mal gesehen | Die erste Nachricht, die von diesem Gerät vom DEM-Server empfangen wurde. |
| Benutzerstatus | Verbindungsstatus des aktuellen Benutzers. |
| Prüfzustand | Informationen dazu, ob Anwendungstests auf dem Gerät laufen. |
| Endpunkt-Agent-Version | Die auf dem Gerät installierte Version des ADEM-Agents. |

## Remote-Standort-Agent-Verwaltung

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | Eine dieser Lizenzen:<br>❑ Prisma Access-Lizenz<br>❑ ADEM Observability-Lizenz oder AI-Powered ADEM-Lizenz |

Auf dieser Registerkarte finden Sie Details zu den Prisma SD-WAN-ION-Zweigstellengeräten, die für Digital Experience Management aktiviert sind. Verwenden Sie diese Registerkarte, um Details zu all Ihren registrierten ADEM-Remote-Standorten abzurufen, z. B. Gerätemodell, Hostname, Standortstatus, Überwachungsstatus (ob die Überwachung für den Standort aktiviert ist), Hostname des Hochverfügbarkeitsservers (sofern vorhanden) und Version des Remote-Standort-Agents.

| Spaltenname | Beschreibung |
|---|---|
| Name des Remote-Standorts | Pisma SD-WAN-Zweigstelle. |
| Gerätemodell | Modellnummer des Prisma SD-WAN-ION-Geräts. |
| Hostname | Hostname des ION-Geräts. |
| HA-Peer-Hostname | Ob an diesem Standort ein hochverfügbares Standby-ION-Gerät konfiguriert wurde. |
| Zuletzt gesehen | Die letzte vom ION-Gerät an den DEM-Server gesendete Nachricht. |
| Zum ersten Mal gesehen | Die erste vom ION-Gerät beim DEM-Server eingegangene Nachricht. |
| Standortstatus | Verbindungsstatus zwischen Standort-ION-Geräts und DEM-Agent. |
| Prüfzustand | Ob der Standort zum Ausführen von Anwendungstests konfiguriert ist. |
| Remote-Standort-Agent-Version | Die Version des auf dem ION-Gerät installierten ADEM-Agents. |

## Zustandsscoreprofile

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | Eine dieser Lizenzen:<br>❑ Prisma Access-Lizenz<br>❑ ADEM Observability-Lizenz oder AI-Powered ADEM-Lizenz |

Auf dieser Registerkarte können Sie Details zum Domänen-Zustandsscore anzeigen.

| Spaltenname | Beschreibung |
|---|---|
| Name der Domänen-Zustandsscoremetrik | Listet die Domänen auf, für die Zustandsscoremetriken berechnet werden. Klicken Sie in dieser Spalte auf einen Domänennamen, um entsprechende Metriken anzuzeigen, wie z. B. den unteren und oberen Schwellenwert sowie die Auswirkungen (Prozentsatz des Gesamt-Erfahrungsscores) |

| Spaltenname | Beschreibung |
|---|---|
| | auf den Gesamtscore, wenn die Zahlen den Schwellenwert überschreiten. Derzeit sind diese Metriken schreibgeschützt und wie vom Administrator festgelegt. Sie können nicht geändert werden. |
| Typ | Domänentyp |
| Verknüpfter Anwendungsfall | Das Dashboard oder Widget, auf dem der berechnete Erfahrungsscore angezeigt wird. |

# ADEM-Auditierungslogs

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | Eine dieser Lizenzen:<br>❑ Prisma Access-Lizenz<br>❑ ADEM Observability-Lizenz oder AI-Powered ADEM-Lizenz |

Sehen Sie sich die Auditierungslogs für alle Ereignisse an, die aufgrund von API-Aufrufen ausgelöst wurden.

| Spaltenname | Beschreibung |
|---|---|
| Ereigniszeit | Der Zeitpunkt, zu dem das Ereignis ausgelöst wurde, das zur Erstellung des Logs geführt hat. |
| E-Mail | E-Mail-Adresse der Person, die bei der Erstellung des Logs benachrichtigt wurde. |
| Beschreibung | Der API-Aufruf, durch den das Ereignis ausgelöst wurde, wodurch das Protokoll erstellt wurde. |