Launch Week: Überblick über die Produkt-Releases

Early Access und allgemeine Verfügbarkeit (Oktober 2025 bis März 2026)

Diese Informationen und die darin enthaltenen Empfehlungen stellen keine Rechts-, Datenschutz-, Sicherheits-, Compliance oder Geschäftsberatung dar. Dieses Dokument dient nur zu allgemeinen Informationszwecken und gibt womöglich nicht den aktuellen Stand aller relevanten Fragen wieder. Es liegt in Ihrer Verantwortung, sich mit Blick auf die Rechtslage, den Datenschutz, die Sicherheit, die Compliance und das Business beraten zu lassen. Stützen Sie sich nicht allein auf die enthaltenen Empfehlungen. Okta übernimmt keine Haftung für Verluste oder Schäden, die sich potenziell aus der Umsetzung der Empfehlungen in diesen Materialien ergeben. Okta gibt keine Zusicherungen, Garantien oder sonstigen Zusicherungen in Bezug auf den Inhalt dieser Materialien. Informationen zu den vertraglichen Zusicherungen von Okta an seine Kunden finden Sie unter okta.com/agreements.

Safe harbor

Diese Präsentation enthält „zukunftsgerichtete Aussagen“ im Sinne der „Safe Harbor“-Bestimmungen des Private Securities Litigation Reform Act von 1995, einschließlich, aber nicht ausschließlich Aussagen zu unseren finanziellen Perspektiven, den Unternehmensstrategien und -plänen, Markttrends und Marktgröße sowie Geschäftschancen und Positionierung. Diese zukunftsgerichteten Aussagen basieren auf aktuellen Erwartungen, Schätzungen, Prognosen und Vorhersagen. Mit der Verwendung von Worten wie „erwarten“, „beabsichtigen“, „planen“, „vorhersehen“, „davon ausgehen“, „glauben“, „potenziell“ und ähnlichen Formulierungen werden zukunftsgerichtete Aussagen gekennzeichnet, auch wenn nicht alle zukunftsgerichteten Aussagen diese Worte enthalten. Diese zukunftsgerichteten Aussagen sind von einer Vielzahl von Risiken und Unsicherheiten abhängig, einschließlich Faktoren oder Umständen, die nicht von uns zu vertreten sind. Beispielsweise haben weltweite wirtschaftliche Rahmenbedingungen in der Vergangenheit die Nachfrage nach unseren Produkten sinken lassen und könnten das auch in der Zukunft wieder tun. Ebenso haben wir und unsere externen Service Provider in der Vergangenheit Cybersicherheitsvorfälle verzeichnet, was sich wiederholen könnte. Es könnte dazu kommen, dass unser Unternehmen das bisher verzeichnete Wachstum nicht aufrecht erhalten kann. Ebenso ist es nicht ausgeschlossen, dass unsere finanziellen Ressourcen nicht ausreichen, um unsere Wettbewerbsposition zu halten oder zu verbessern. Wir könnten nicht im Stande sein, neue Kunden zu gewinnen oder unsere Bestandskunden zu halten bzw. ihnen zusätzliche Produkte zu verkaufen. Der Kundenzuwachs ist in der letzten Zeit zurückgegangen und könnte sich in der Zukunft weiter verlangsamen.

Es könnte zu Ausfällen oder Leistungsproblemen bei unserer Technologie, einschließlich einem Service-Ausfall, kommen. Wir und unsere externen Service Provider haben bereits bzw. haben in der öffentlichen Wahrnehmung gegen verschiedene für uns geltende Datenschutz- und Sicherheitsvorschriften verstoßen, solche Vorfälle könnten in der Zukunft erneut auftreten. Möglicherweise werden nicht die erwarteten Synergien und Effizienzsteigerungen durch kürzliche Akquisen oder Unternehmenszusammenschlüsse erzielt, und es könnte dazu kommen, dass wir die erworbenen Unternehmen nicht vollständig integrieren können. Und es könnte vorkommen, dass wir unsere Anleihen bei Fälligkeit nicht begleichen können. Weitere Informationen zu Faktoren, die unsere Finanzergebnisse beeinflussen können, finden Sie in unserem aktuellsten Form 10-Q-Quartalsbericht und in anderen Berichten an die US-Behörde für die Kontrolle des Wertpapierhandels (SEC). Die zukunftsgerichteten Aussagen in dieser Präsentation stellen die Ansichten zum Zeitpunkt der Präsentation dar. Okta beabsichtigt keine Aktualisierung dieser zukunftsgerichteten Aussagen und lehnt jedwede entsprechende Verpflichtung ab.

Alle in dieser Präsentation genannten Produkte, Funktionen, Zertifizierungen, Autorisierungen oder Bestätigungen, die derzeit noch nicht allgemein verfügbar sind, noch nicht verkauft wurden oder derzeit nicht gepflegt werden, werden möglicherweise nicht zum angekündigten Zeitpunkt oder überhaupt nicht bereitgestellt bzw. verkauft. Produkt-Roadmaps stellen keine Zusage, keine Verpflichtung und kein Versprechen dar, ein Produkt, eine Funktion, eine Zertifizierung oder eine Bestätigung bereitzustellen. Sie sollten sich bei Ihren Kaufentscheidungen nicht auf sie verlassen.

Weitere Informationen zu den neuesten Innovationen und geplanten Funktionen von Okta

Webseite zur Launch Week

Hier können Sie sich über die neuesten Innovationen informieren, Aufzeichnungen von der Showcase ansehen und weiterführende Materialien finden.

Hier können Sie unser Vertriebsteam kontaktieren.

Webinar zur Launch Week

Eine kurze Vorschau auf kommende Produkt-Releases.

Hier können Sie sich für die Webinare zu Okta-Produkten registrieren.

Willkommen bei der Release-Übersicht der Okta Platform

4. Quartal 2025 bis 1. Quartal 2026

Herzlich Willkommen zur ersten Release-Übersicht von Okta für 2026. Dieses Jahr hat bereits viele spannende Neuigkeiten gebracht. Wir möchten Ihnen alle Innovationen vorstellen, die wir in der letzten Zeit veröffentlicht haben.

Erfahren Sie, wie Okta Workforce Identity die Sicherheit für menschliche Benutzer, Geräte und KI-Agenten verbessert.

Überblick über diese Präsentation

Der Überblick über die Produkt-Releases ist in zwei Teile mit folgenden Inhalten unterteilt:

Okta Workforce Identity

- Überblick über Okta Workforce Identity
- Spotlights
- Übersicht über die Produkt-Releases
- Entwicklerressourcen

Okta Customer Identity

- Überblick über Okta Customer Identity
- Spotlights
- Übersicht über die Produkt-Releases

Okta Workforce Identity

Kunden können mit Okta Workforce Identity die Identity-Sicherheit verbessern, Unternehmenswachstum durch Automatisierung ermöglichen und die IT modernisieren, um die Effizienz der Geschäftsprozesse zu steigern.

Die Releases dieses Quartals konzentrieren sich auf unser Versprechen, Kunden bei der Verbesserung ihrer Sicherheitslage und Governance für Geräte, privilegierte Benutzer und KI-Agenten zu unterstützen.

Spotlights

Okta Workforce Identity

- Okta for AI Agents
- Okta for US Military
- Verbesserungen beim Customer Identity-Schutz
- Gerätegebundenes Single Sign-On

Alle Funktionen

- KI-Agenten
- Identity Security Posture Management (ISPM)
- Zugriffsmanagement
- Identity-Management
- Identity Governance
- Platform Services

Entwicklerressourcen

Die Okta Platform erweckt den Identity Security Fabric zum Leben

Secure Identity-Produkte

Posture Management	Governance	PAM	Zugriffsmanagement	Okta Device Access	Identity Threat Protection
Identity-Konfigurationsfehler	Richtlinienverstöße	Ressourcenzugriff	Gemeinsame Nutzung von Risikoindikatoren	Indikatoren für die Gerätesicherheit	Ökosystem-Indikatoren + Universal Logout

Secure Identity-Orchestrierung

Secure Identity-Integrationen

Infrastruktur	Anwendungen	APIs	Identitäten
IaaS, On-Premise-Server	Cloud-Anwendungen, On-Premise-Anwendungen	Öffentlich, Privat	Directories, Maschinen/KI-Agenten

99,99 % Verfügbarkeit. Dutzende Milliarden Logins pro Monat. Keine planmäßigen Ausfallzeiten.

okta

Early Access

Spotlight: Okta for AI Agents

Ihre KI-Strategie beginnt mit Identity-Management

Was ist das?

KI-Agenten sind Ihre neuesten digitalen Mitarbeiter. Die meisten von ihnen arbeiten aber momentan noch im Dunkeln.

Okta for AI Agents bietet eine Identity-Ebene für das Zeitalter der Agenten. Wir integrieren jeden KI-Agenten in Ihren Identity Security Fabric – damit Sie KI im vollen Umfang sehen, verwalten und kontrollieren können. Lassen Sie Ihre KI-Strategie nicht zu Ihrem größten Sicherheitsrisiko werden.

Herausforderungen bei Kunden:

- KI-Agenten werden in Unternehmen schnell und isoliert bereitgestellt – ohne zentrale Informationsquelle für Transparenz und Berechtigungen.
- Die Agenten handeln schnell, im Namen der Benutzer oder autonom und sind oft überprivilegiert.
- Viele Governance- und Sicherheitstools können mit der anwendungsübergreifenden Echtzeit-Agilität von KI-Agenten nicht mithalten.

Vorteile

KI-Agenten verhalten sich nicht wie menschliche Benutzer und integrieren sich nicht nahtlos in traditionelle Identity-Modelle. Dadurch entstehen große Sicherheitslücken mit diesen Folgen:

- **Erhöhtes Risiko:** Eine versehentliche Offenlegung von Daten kann schwerwiegende Datenschutz- und Sicherheitsverletzungen nach sich ziehen. Fehlende Audit-Trails können Compliance- und Audit-Ziele gefährden.
- **Verbreiteter Wildwuchs bei Anmeldedaten:** KI-Agenten werden oft standardmäßig zu „Superadministratoren“. Sie verlassen sich auf riskante, langlebige Token, die ein großes und schwer zu verteidigendes Ziel für Angriffe auf Anmeldedaten darstellen.
- **Wachsende Governance-Lücke:** 91 % der Unternehmen nutzen zwar KI, aber 44 % haben keine Governance-Struktur. Menschen als Überwachungsinstanz können mit der Geschwindigkeit der Agenten nicht Schritt halten. Dies hemmt Innovationen und lässt Wertpotenzial ungenutzt.*

* Okta: *AI at Work 2025: Absicherung der KI-unterstützten Belegschaft*, 12. August 2025

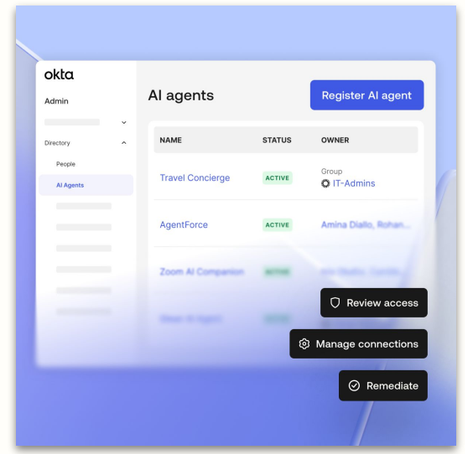
Installation

Im Early Access verfügbar ab **6. Februar 2026**.

Okta for AI Agents-SKU: Bietet die Vorteile der Okta Platform for AI Agents.

Nur für die OIE-Plattform (Okta Identity Engine) verfügbar.

Mehr dazu im Blog.



Post-Audit

Spotlight: Okta for US Military (IL5- und NSS-Bereitschaft)

Missionskritisches Identity-Management in relevanter Geschwindigkeit

Was ist das?

Okta for US Military, die vorläufige Sicherheitsfreigabe (PA) des Kriegsministeriums (DoW) der USA für Okta, wird von der Behörde des US-Verteidigungsministeriums für IT-Sicherheit und Infrastruktur (DISA) auf Sicherheitsstufe 5 (IL5) voraussichtlich verlängert.

Die erwartete PA wird es Okta ermöglichen, Workloads und Anwendungen bis IL5 in unserer Okta for US Military-Umgebung zu betreuen.

Herausforderungen bei Kunden:

Legacy- und On-Premise-Lösungen, die missionskritische Funktionen nicht mehr effektiv unterstützen oder die Streitkräfte des Landes nicht mehr mit der besten Technologie ausstatten können.

Vorteile

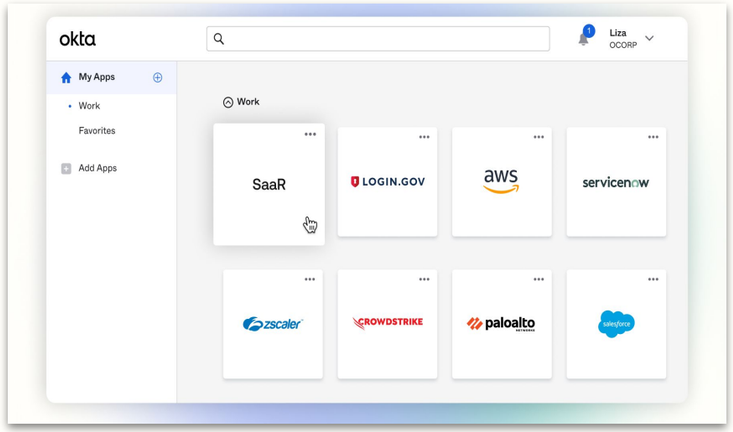
- Okta wird nicht-öffentliche, keiner Geheimhaltungsstufe unterliegende Daten von nationalen Sicherheitssystemen (NSS) oder nicht-öffentliche, keiner Geheimhaltungsstufe unterliegende Daten betreuen, bei denen die unbefugte Offenlegung von Informationen voraussichtlich schwerwiegende negative Auswirkungen auf organisatorische Abläufe, Assets oder Personen haben könnte.
- Mit einer einzigen Cloud für IL4- und IL5-Anwendungen und -Workloads beseitigt Okta den Zusatzaufwand für die Verwaltung fragmentierter Identity-Stacks und verlagert den Fokus von der Infrastruktur auf die Innovation.
- Okta kombiniert die IL5-Datenverarbeitung mit Workflows auf Attributebene, um Rechteausweitungen zu verhindern und die zentralen Zero-Trust-Vorgaben zu erfüllen.

Installation

Die Verlängerung der PA für Okta wird voraussichtlich im 2. Quartal des Kalenderjahres 2026 verfügbar sein.

Cell Add-on: Okta for US Military (bestehende SKU) sowie die bestehende Produktverfügbarkeit und -bewertung bleiben unverändert.

Erfahren Sie, wie ein IL4-Identity-Anbieter erfolgreich IL5-Umgebungen betreut.



okta

Spotlight: Anwendungsbereiche für den Identity Security Fabric

Fabric wird mit Threads für die End-to-End-Absicherung aller Identitäten verwoben

Was ist das?

Moderne Sicherheit erfordert einen einheitlichen Identity Security Fabric. Okta implementiert diesen Fabric durch miteinander verbundene Anwendungsbereiche (unsere Threads), die auch die schwierigsten Sicherheitsherausforderungen bewältigen. Zusammen bietet Okta umfassende Identity-Sicherheit für alle Identitäten, Anwendungsfälle und Ressourcen, einschließlich:

- Schutz für Hybrid- und On-Premise-Umgebungen (allgemein verfügbar*)
- Sicherheitsorientierte Governance (allgemein verfügbar*)
- Sicheres Onboarding für Mitarbeiter (allgemein verfügbar*)

Herausforderungen bei Kunden:

- **Komplexe hybride Umgebungen** erweitern die Angriffsfläche von Unternehmen; fragmentierte Sicherheitstools schränken Transparenz und Kontrolle ein.
- **Legacy Governance** erzeugt Isolation und führt zu reaktiven Korrekturen, blinden Genehmigungen und mangelnder Transparenz.
- **Identity-Sicherheitslücken während des Onboardings** können sich schnell zu Sicherheitsverletzungen und operativen Risiken ausweiten und das Onboarding in einen Bedrohungsvektor verwandeln.

* Bestimmte Funktionen befinden sich im Early Access.

Vorteile

Sichere Hybrid- und On-Premise-Umgebungen

- Bessere Sicherheitslage Ihrer Hybridumgebung
- Zentrale Verwaltung für On-Premise-Ressourcen
- Beschleunigung der Cloud-Journey

Sicherheitsorientierte Governance

- Triage von Sicherheitsvorfällen durch Zugriffsprüfung unmittelbar nach einem Hochrisiko-Ereignis
- Echtzeitunterbindung toxischer Zugriffskombinationen
- Verhinderung dauerhafter Benutzerberechtigungen für sensible Ressourcen

Sicheres Mitarbeiter-Onboarding

- Vertrauensbildung von der ersten Interaktion an
- Sichere Provisionierung von Geräten und Authentifizierungsfaktoren
- Verwaltung der Provisionierung von Birthright-Anwendungen

Installation

Verfügbar als Bestandteil von Okta Workforce Identity Cloud. Der Identity Security Fabric ist Oktas moderner Ansatz für die Identity-Architektur. Es handelt sich nicht um ein einzelnes Produkt, das man kaufen kann.

Ressourcen: Landing-Page, Demo zum Durchklicken, Blog „Sichere Hybrid- und On-Premise-Umgebungen“, Blog „Sicherheitsorientierte Governance“, Blog und Demo „Sicheres Mitarbeiter-Onboarding“.

Early Access

Spotlight: Gerätegebundenes Single Sign-On

So erreichen Ihre Mitarbeiter einfacher und sicherer ihr Ziel – beginnend mit der Geräteanmeldung

Was ist das?

Gerätegebundenes Single Sign-On (SSO) initiiert eine Hardware-geschützte SSO-Session für den nahtlosen Zugriff auf Ihre nachgelagerten Anwendungen, nachdem sich ein Gerät auf macOS- und Windows-Geräten mit Okta Device Access angemeldet hat. Diese Funktion stoppt die Wiederholung von Okta-Sessions und sorgt für eine optimierte Login-Experience.

Herausforderungen bei Kunden:
Mitarbeiter benötigen immer und überall sicheren Zugriff auf ihre benötigten Anwendungen und Tools. Eines ist jedoch klar: Herkömmliches SSO und MFA reichen nicht aus. Benutzer ärgern sich nicht nur über wiederholte Authentifizierungsaufforderungen. Hinzu kommt, dass diese Standardschutzmaßnahmen möglicherweise nicht zuverlässig vor raffinierten Identity-basierten Angriffen schützen.

Vorteile

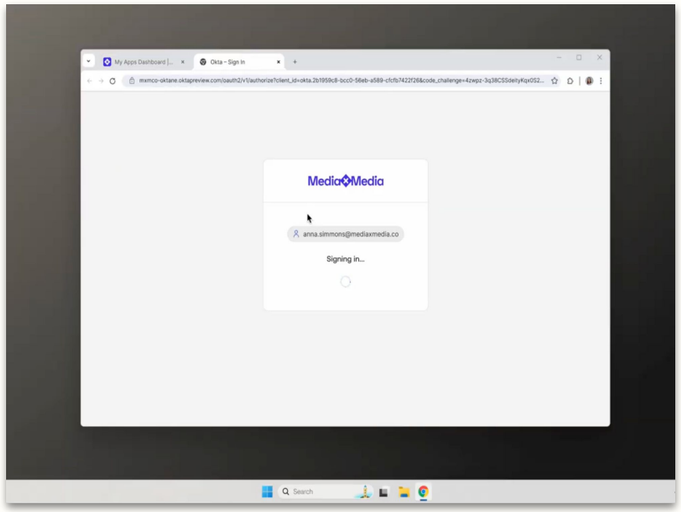
- **Optimierte Sicherheitslage:**
  Hardware-geschützte und kryptografisch sichere Session, die Identity-basierte Angriffe deutlich erschwert, weil der Zugriff nicht nur an den Benutzer, sondern auch an dessen Gerät gebunden ist. Angreifer können eine gestohlene aktive Okta SSO-Session nicht auf einem Gerät anderen nutzen.

- **Nahtloser Zugriff auf nachgelagerte Anwendungen:**
  Nutzung einer erfolgreichen Geräteanmeldung bei Okta Device Access für den Zugriff auf nachgelagerte Ressourcen, die das gleiche Sicherheitsniveau erfordern. Diese Funktion sorgt dafür, dass Mitarbeiter nicht mehr so oft zur Authentifizierung aufgefordert werden, und reduziert damit mögliche Einfalltore für Angreifer.

Installation

Gerätegebundenes SSO ist eine neue Funktion von Okta Device Access. Für diese Funktion benötigen Sie Okta Device Access und Okta Adaptive MFA.

Mehr dazu im Blog.



Okta Workforce Identity-Releases

Okta Workforce Identity vereinheitlicht die Identity-Sicherheit, indem die Lösung Compliance-Risiken identifiziert und behebt, starke Authentifizierung und Governance durchsetzt sowie Bedrohungen bei allen Benutzern, Ressourcen und Geräten erkennt.

Informieren Sie sich über die neuesten Funktionen, die im 4. Quartal 2025 und 1. Quartal 2026 veröffentlicht wurden.

Finden Sie ganz einfach die Technologie, die im jeweiligen Release verfügbar ist:

Classic

Okta Identity Engine (OIE)

* **Unterstützt für FedRAMP Moderate/High/DOD IL4:** Dieses Produkt funktioniert wie erwartet und wird vollständig im Okta Public Sector-Portfolio unterstützt.

* **Autorisiert für FedRAMP Moderate/High/DOD IL4:** Dieses Produkt bzw. diese Funktion ist verfügbar, vollständig unterstützt und für FedRAMP bzw. DISA autorisiert.

KI-Agenten

Early Access

Okta for AI Agents

Funktion von Okta for AI Agents

- **Erkennung von KI-Agenten:** Führen Sie die KI aus dem Schatten ins Licht – mit kontinuierlicher Erkennung und zentralisierter Verwaltung für jede Agenten-Identität.
- **Verwaltung und Standardisierung des anwendungsübergreifenden Zugriffs:** Verwalten und vereinheitlichen Sie den Zugriff auf KI-Agenten über SaaS- und Legacy-Systeme hinweg auf einer einzigen Kontrollebene, um konsistente Richtlinien, das Least-Privilege-Prinzip und ein kontinuierliches Identity-Standing über komplexe Workflows hinweg zu gewährleisten.
- **Schutz und Rotation von Anmeldedaten:** Sichern Sie die „Generalschlüssel“, indem Sie Anmeldedaten in einem Vault speichern und kontextbezogene Least-Privilege-Richtlinien für Agenten durchsetzen, die mit Maschinengeschwindigkeit handeln.
- **Lebenszyklusverwaltung von Agenten:** Schließen Sie die Lücke in der KI-Governance, indem Sie autonome Agenten in Standard-Zertifizierungsworkflows integrieren, um sicherzustellen, dass Aktionen auf menschliche Absichten zurückführbar sind.

Mehr erfahren

OIE

Okta for AI Agents

Identity Security Posture Management (ISPM)

Allgemein verfügbar

Rollenbasierte Zugriffskontrolle – Verwaltung von Anwendungen und Integration von Quellen

Classic OIE

Funktion von ISPM

Anwendungsverantwortliche (z. B. der Salesforce.com-Administrator) erhalten begrenzten Zugriff auf ISPM und können nur ausgewählte Datenquellen anzeigen, sodass Security-Teams die Problemlösung an diese Anwendungsverantwortlichen delegieren können.

Geografische Expansion

Classic OIE

Funktion von ISPM

ISPM wird sowohl in EMEA als auch in APJ verfügbar sein, um Datenresidenzvorschriften zu unterstützen.

Nicht-menschliche Identitäten: Workload-App-Identitäten

Classic OIE

Funktion von ISPM

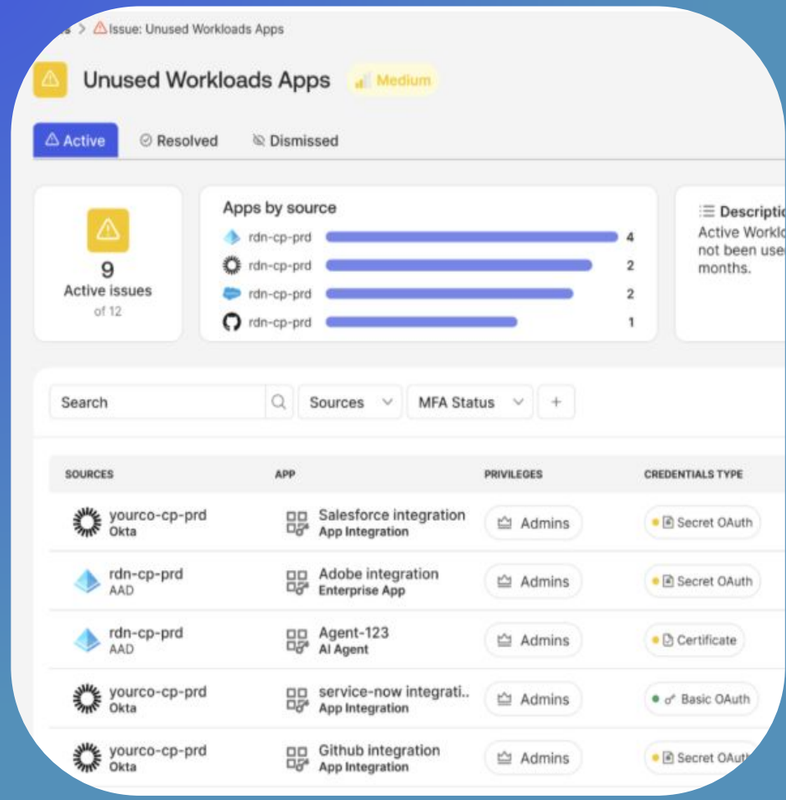
Verbesserte Transparenz und Risikoerkennungen für OAuth-Token, die KI-Agenten, Anwendungen und Drittanbieterprodukte unterstützen.

Workday-Integrationen

Classic OIE

Funktion von ISPM

Zentraler Überblick über alle Workday-Identitäten, einschließlich nicht-menschlicher Identitäten, privilegierter und lokaler Accounts. Erkennung damit verbundener Risiken wie veraltete Identitäten und schwache MFA.



Workload-App-Identitäten

Identity Security Posture Management (ISPM)

Allgemein verfügbar

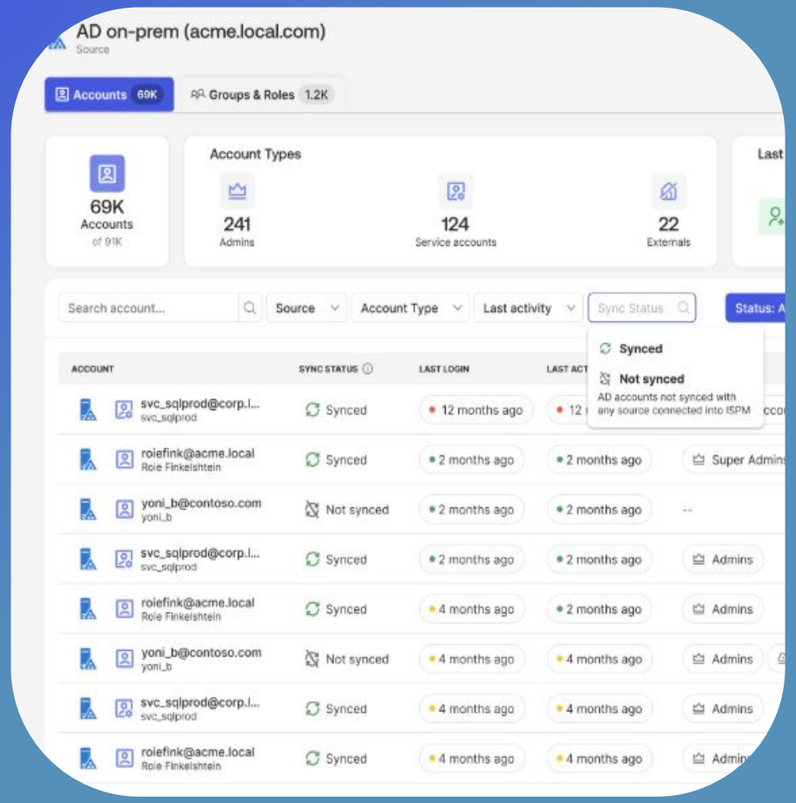
On-Premise-Integration für Active Directory

Funktion von ISPM

Umfassende Transparenz in Bezug auf Active Directory-Accounts, Gruppen und deren Risiken, um die Angriffsfläche mithilfe des Okta AD-Agenten zu reduzieren.

Classic

OIE



On-Premise-Integration für Active Directory

Identity Security Posture Management (ISPM)

Early Access

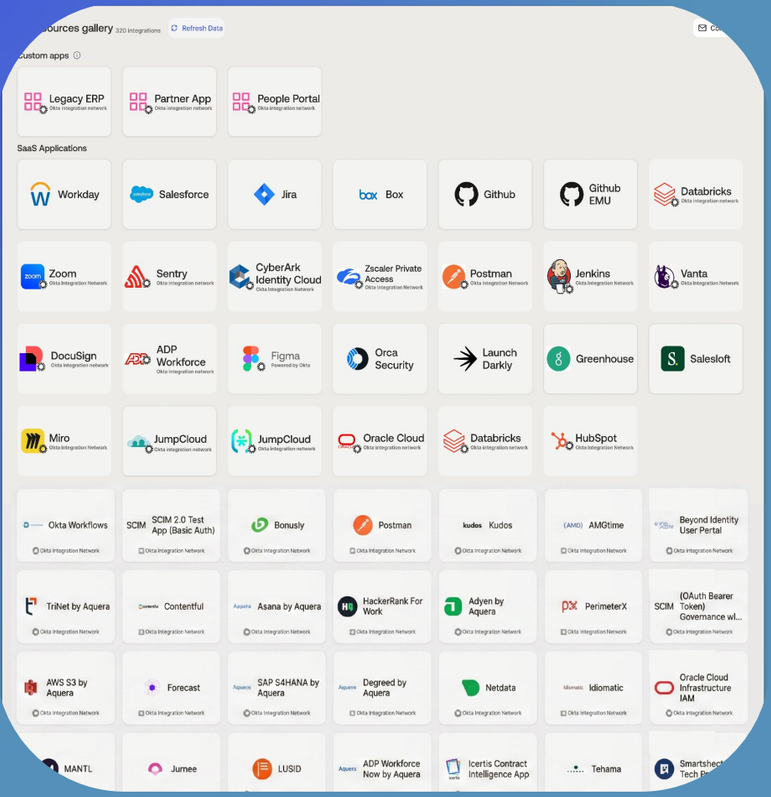
300 neue Integrationen – basierend auf Okta SCIM

Funktion von ISPM

Ermöglichen Transparenz in Bezug auf die am häufigsten nachgefragten Anwendungen, z. B. Datadog, Databricks, Oracle Cloud, Jenkins, Zoom. Erkennung und Priorisierung lokaler Accounts.

Classic

OIE



300 neue SCIM-Integrationen

Zugriffsmanagement

Allgemein verfügbar

Device Assurance: Richtlinienoption für dynamische Betriebssystemversionen

Verfügbar in AMFA-ASSO ‖ Autorisiert für FedRAMP Moderate/High/DOD IL4

Nutzen Sie eine flexiblere, weniger aufwändige Richtlinienkonfiguration, die den Zugriff dynamisch auf der Basis minimaler Betriebssystem-Versionen regelt, um festzulegen, dass Geräte über die neuesten Betriebssystem-Updates verfügen.

Mehr erfahren

OIE

Übergangsfrist für die Device Assurance-Compliance

Verfügbar in AMFA/ASSO ‖ Autorisiert für FedRAMP Moderate/High/DOD IL4

Gewähren Sie Endbenutzern für konfigurierbare Zeiträume ununterbrochenen Zugriff auf wichtige Ressourcen, damit sie etwaige Geräte-Compliance-Probleme selbst beheben können, bevor sie ausgesperrt werden.

Mehr erfahren

OIE

Anbieter von Informationen zum Gerätestatus

Verfügbar in AMFA-ASSO ‖ Autorisiert für FedRAMP Moderate/High/DOD IL4

Administratoren können Device Assurance-Richtlinien mit Signalen zum Gerätestatus anreichern, die von kundeneigenen Compliance-Services stammen und per SAML-Assertions bereitgestellt werden.

Mehr erfahren

OIE

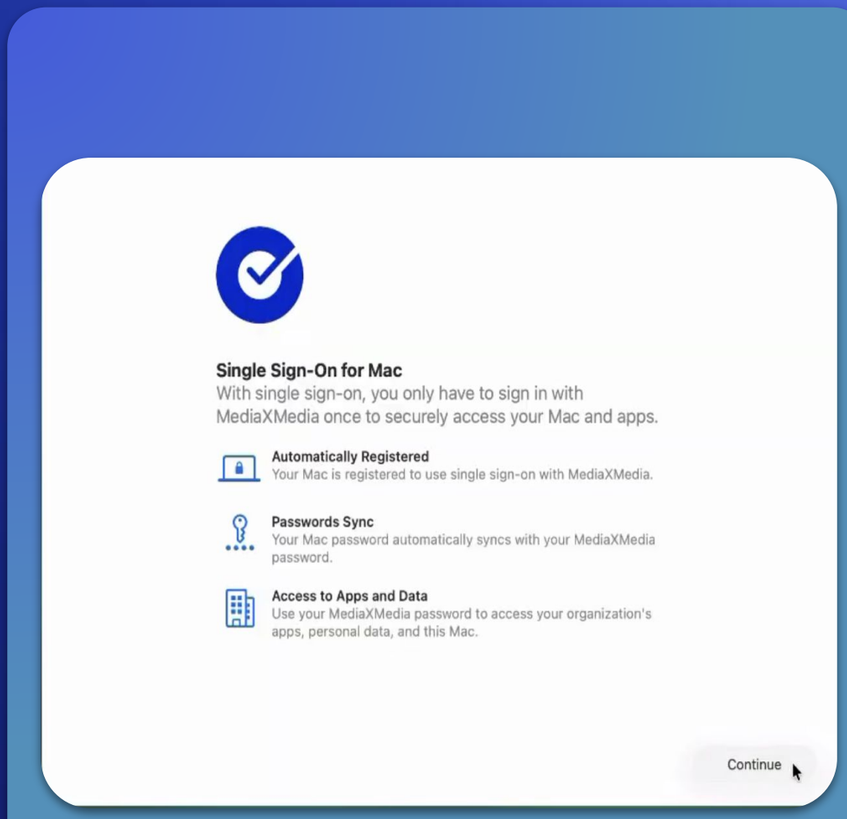
SSO-Support der Plattform im macOS Setup Assistant

Funktion von Okta Device Access ‖ Autorisiert für FedRAMP Moderate/High/DOD IL4

Bieten Sie eine optimierte Geräte-Onboarding-Experience, bei der mithilfe der Benutzerprofil-Attribute und Anmeldedaten von Okta automatisch ein lokaler, bei der Desktop-Passwortsynchronisation registrierter macOS-Account erstellt wird.

Mehr erfahren

OIE



SSO-Support der Plattform im macOS Setup Assistant

Zugriffsmanagement

Allgemein verfügbar

Benutzerdefinierte Administratorberechtigungen für Zugriffsrichtlinien

Verfügbar in allen SKUs || Autorisiert für FedRAMP Moderate/High/DOD IL4

Benutzerdefinierte Administratorberechtigungen, die eine konsistente, granulare Kontrolle über die Zugriffsrichtlinien (Authentifizierungs-, Session- und Account Management-Richtlinien) ermöglichen.

Mehr erfahren

OIE

OEL für Passwortkomplexität (ehemals Höhere Sicherheit für Anmeldedaten)

Verfügbar in allen SKUs || Autorisiert für FedRAMP Moderate/High/DOD IL4

Verwenden Sie Okta Expression Language (OEL), um benutzerdefinierte Anforderungen an die Passwortkomplexität für Endbenutzer zu definieren, die Passwörter erstellen.

Mehr erfahren

OIE

APIs für OAG-Automatisierung

Funktion von Okta Access Gateway || Unterstützt für FedRAMP Moderate/High/DOD IL4

Kunden können jetzt Anwendungs- und Identity-Anbieterkonfigurationen in Okta Access Gateway (OAG) über RESTful API-Aufrufe automatisieren.

Mehr erfahren

Classic

OIE

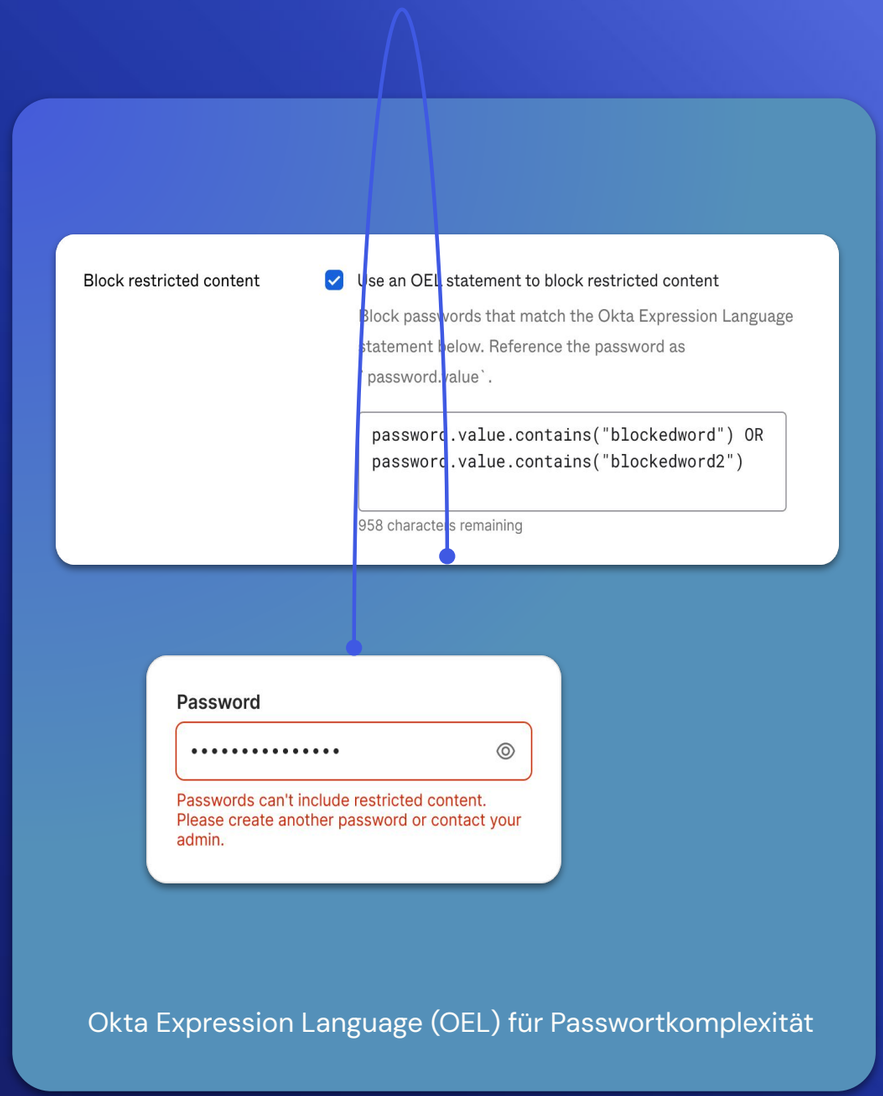
Einheitliche Claims-Generierung für per Okta föderierte Anwendungen

Verfügbar in allen SKUs || Autorisiert für FedRAMP Moderate/High/DOD IL4

Ermöglichen Sie erstklassige, personalisierte Experiences für Verbundanwendungen mit einer optimierten Schnittstelle für die Konfiguration von SAML-Attributen und OIDC-Claim-Typen.

Mehr erfahren

OIE



Okta Expression Language (OEL) für Passwortkomplexität

Zugriffsmanagement

Allgemein verfügbar

OIDC-Token-Verschlüsselung

Classic OIE

Verfügbar in allen SKUs || Autorisiert für FedRAMP Moderate/High/DOD IL4

Ein standardbasierter Ansatz zur Verschlüsselung von OIDC ID-Token, der JSON Web Encryption zwischen einem Okta-Identity-Anbieter und einer Relying Party (RP) nutzt.

Mehr erfahren

Unterstützung von Okta Account Management-Richtlinien für Passwort-Ablauf

OIE

Verfügbar in allen SKUs || Autorisiert für FedRAMP Moderate/High/DOD IL4

Erweiterung des Schutzes für Passwort-Ablauf-Prozesse in der OAMP-Richtlinie, was größere Kontrolle über Sicherheitsanforderungen ermöglicht.

Mehr erfahren

Vom Administrator ausgewählter Faktor für User Enumeration Prevention (UEP)-Sicherheitsabfrage

OIE

Verfügbar in allen SKUs || Autorisiert für FedRAMP Moderate/High/DOD IL4

Durchsetzung stärkerer Faktoren (z. B. Okta Verify-Push, FastPass) für UEP-Sicherheitsabfragen, um die Offenlegung von Benutzerinformationen zu verhindern und passwortlose Authentifizierungabläufe zu optimieren.

Mehr erfahren

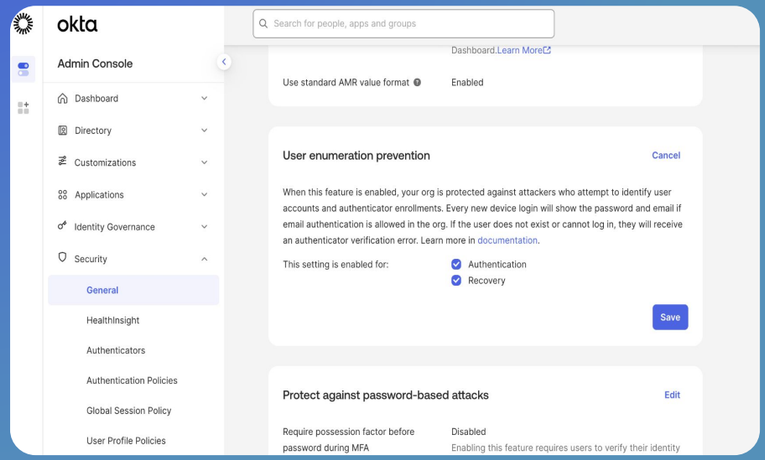
Zusätzliche biografische Attribute für die ID-Verifizierung

OIE

Funktion von MFA/AMFA || Autorisiert für FedRAMP Moderate/High/DOD IL4

Erlaubt die Zuordnung zusätzlicher biografischer Daten (z. B. Geburtsdatum, E-Mail-Adresse, Telefon) während der Identity-Verifizierung, um die Benutzerzuordnung und Sicherheit zu verbessern.

Mehr erfahren



User Enumeration Prevention (UEP)-Sicherheitsabfrage

Zugriffsmanagement

Allgemein verfügbar

Unterstützung für hochsichere Zertifikate von Zertifizierungsstellen

Verfügbar in allen SKUs ‖ Autorisiert für FedRAMP Moderate/High/DOD IL4

Verwendung von Okta Custom Domains mit sichereren Verschlüsselungsoptionen für Zertifikate (SHA-384 und SHA-512), um höhere Authentizität und Integrität zu garantieren.

Mehr erfahren

OIE

Netzwerkbeschränkungen für Token Endpoint

Verfügbar in allen SKUs ‖ Autorisiert für FedRAMP Moderate/High/DOD IL4

Verbesserte Sicherheit dank Allow-Listen für Netzwerk-Zonen, Einschränkung von Token-Anfragen auf vertrauenswürdige IP-Adressen und Schutz vor Replay-Attacken, Token-Diebstahl, DoS und Rate Limit-Missbrauch.

Mehr erfahren

OIE

Neue EDNZ-IP-Kategorien für Residential Proxies und Blockchain-VPNs

Funktion von AMFA ‖ Autorisiert für FedRAMP Moderate/High/DOD IL4

Ermöglicht das Zulassen oder Verweigern des Zugriffs basierend darauf, ob eine IP-Adresse mit einem kommerziellen VPN-Anbieter, Anonymisierungsproxys, dem Tor-Netzwerk etc. verbunden ist.

Mehr erfahren

Classic

OIE

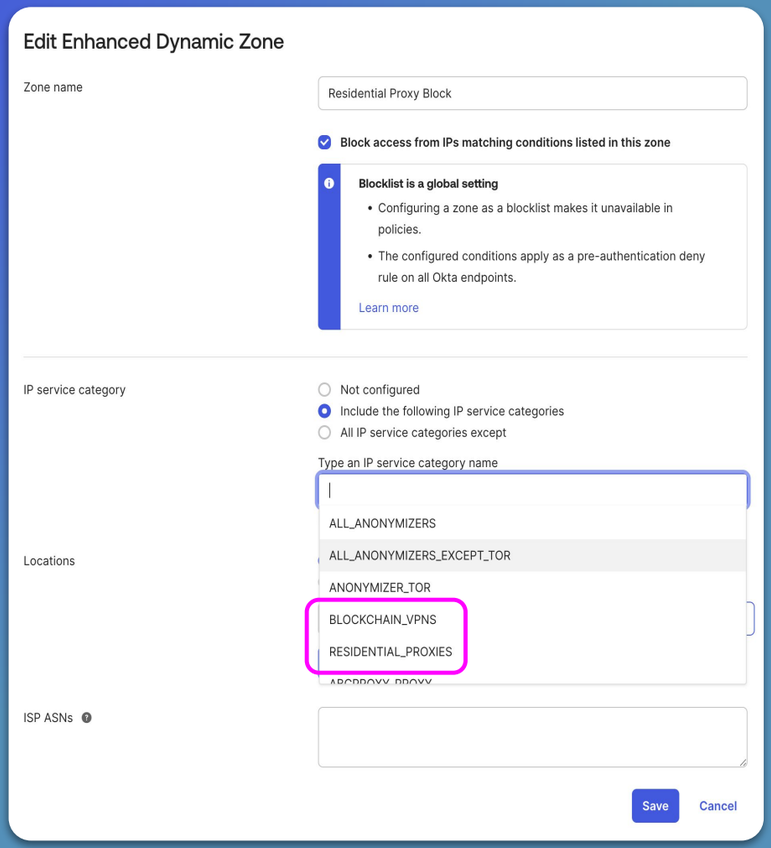
Benutzerdefinierte Administratorrollen für Identity Threat Protection

Funktion von Identity Threat Protection ‖ Autorisiert für FedRAMP Moderate/High, unterstützt für DOD IL4

Durchsetzung von Least-Privilege-Zugriff mit präzisen Administratorberechtigungen mit festgelegten Berechtigungsbereichen für die Verwaltung von ITP-Konfigurationen, z. B. wer Benutzer-Sessions verwalten, Risikorichtlinien konfigurieren oder SSF-Integrationen (Shared Signals Framework) einrichten kann.

Mehr erfahren

OIE



Neue EDNZ-IP-Kategorien für Residential Proxies und Blockchain-VPNs

Zugriffsmanagement

Allgemein verfügbar

Landing-Page für Identity Threat Protection (ITP)

Funktion von Identity Threat Protection || Autorisiert für FedRAMP High, unterstützt für FedRAMP Moderate/High, unterstützt für DOD IL4

Einheitliche Experience zur einfachen Navigation zu allen ITP-Funktionen. Einfaches Kennenlernen neuer Funktionen, Verstehen von Konfigurationen und Optimieren von Steuerelementen, um die eigene Bereitstellung zu optimieren und die Sicherheitslage zu verbessern.

Mehr erfahren

OIE

Verdächtige Anmeldung von einer IP-Adresse, die von FastPass gekennzeichnet wurde

Funktion von Identity Threat Protection || Autorisiert für FedRAMP Moderate/High, unterstützt für DOD IL4

Diese Erkennung zeigt an, dass ein Anmelde-Ereignis von einer IP-Adresse aus stattgefunden hat, die Okta FastPass bei einem Phishing-Ereignis gekennzeichnet hat.

Mehr erfahren

OIE

Verdächtige Anmeldung von einer IP-Adresse, die bei einem Anmeldedaten-Angriff gekennzeichnet wurde

Funktion von Identity Threat Protection || Autorisiert für FedRAMP Moderate/High, unterstützt für DOD IL4

Diese Erkennung zeigt an, dass ein erfolgreiches Anmelde-Ereignis von einer IP-Adresse aus stattgefunden hat, bei der auch mehrere Anmelde-Fehler aufgetreten sind.

Mehr erfahren

OIE

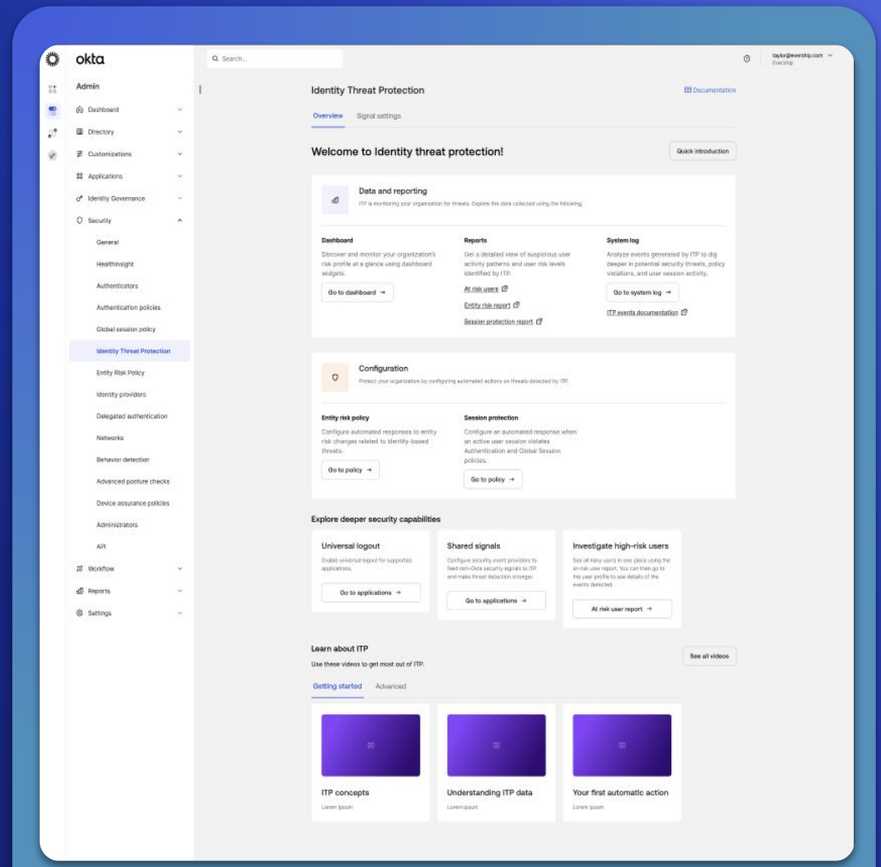
Kompromittierte Anmeldedaten erkannt

Funktion von Identity Threat Protection || Autorisiert für FedRAMP Moderate/High, unterstützt für DOD IL4

Diese Erkennung zeigt an, dass eine Benutzername-Passwort-Kombination Ihrer Org in einer Drittanbieter-Liste mit öffentlichen Datenschutzverletzungen aufgeführt ist.

Mehr erfahren

OIE



Landing-Page für ITP

Zugriffsmanagement

Allgemein verfügbar

Verwendung eines eigenen Anbieters für Identitätsprüfungen

Funktion von MFA/AMFA || Autorisiert für FedRAMP Moderate/High/DOD IL4

Möglichkeit, für Onboarding, Authentifizierung, Account-Wiederherstellung und Helpdesk-Support einen eigenen Anbieter zur Identitätsprüfung oder eine eigenentwickelte interne Lösung zu verwenden.

Mehr erfahren

OIE

Native Passkey-Unterstützung

Funktion von MFA / AMFA || Autorisiert für FedRAMP Moderate

Ermöglicht sichere und benutzerfreundliche Experiences dank nahtloser Passkey-Authentifizierung direkt in nativen Mobilgeräte-Apps, sodass kein Webbrowser notwendig ist.

Mehr erfahren

OIE

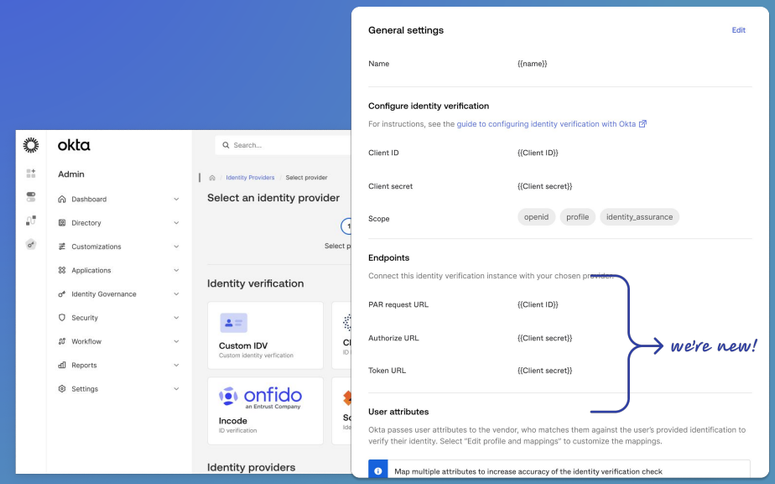
Passkey für mehrere Subdomains

Funktion von MFA/AMFA || Autorisiert für FedRAMP Moderate/High/DOD IL4

Ermöglicht die Konfiguration der Relying Party ID (rpID), die Passkey-Registrierung und Authentifizierung in mehreren Subdomains erlaubt.

Mehr erfahren

OIE



Verwendung eines eigenen Anbieters für Identitätsprüfungen

Zugriffsmanagement

Allgemein verfügbar

Temporary Access Code (TAC)

Funktion von MFA/AMFA

Fügt einen neuen Authentifikator hinzu, mit dem IT-Support-Administratoren einmalig oder mehrmals nutzbare Codes für Endbenutzer erstellen können, die nur temporär Zugriff benötigen.

Mehr erfahren

OIE

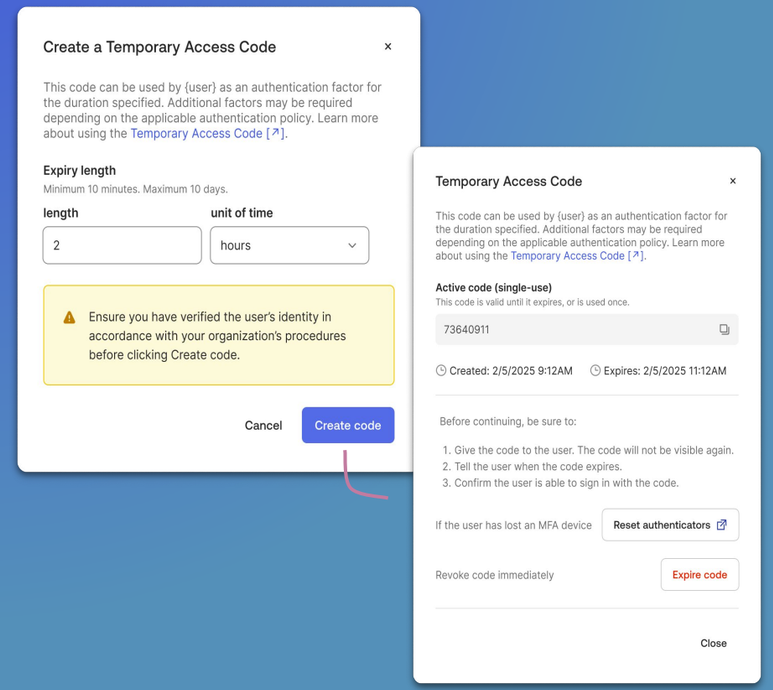
Benutzerdefinierte AAGUID

Funktion von MFA/AMFA || Autorisiert für FedRAMP Moderate/High/DOD IL4

Beschränkt die Authentifikator-Registrierung durch Endbenutzer ausschließlich auf zulässige Authentifikatoren und Passwortmanager.

Mehr erfahren

OIE



Temporary Access Code (TAC)

Zugriffsmanagement

Early Access

Gerätebedingungen in OAMP

Verfügbar in allen SKUs || Autorisiert für FedRAMP Moderate/High/DOD IL4

Ermöglicht Administratoren, Account Management-Aktivitäten wie Self-Service-Passwortrücksetzungen und die Registrierung neuer Authentifizierungsfaktoren auf registrierte/verwaltete Geräte zu beschränken.

Mehr erfahren

OIE

OAG-Offline-Zugriff

Funktion von Okta Access Gateway || Unterstützt für FedRAMP Moderate/High/DOD IL4

Wenn Okta Access Gateway (OAG) die Verbindung zu Okta verliert, können Benutzer weiterhin auf lokale Anwendungen zugreifen.

Classic

OIE

Eigenen Telefonieanbieter verwenden

Verfügbar in allen SKUs

Binden Sie Ihren Telefonieanbieter unkompliziert über die vereinfachte Einrichtung von Okta ein und wickeln Sie die Abrechnung Ihrer Nutzung direkt mit Ihrem Anbieter ab.

Mehr erfahren

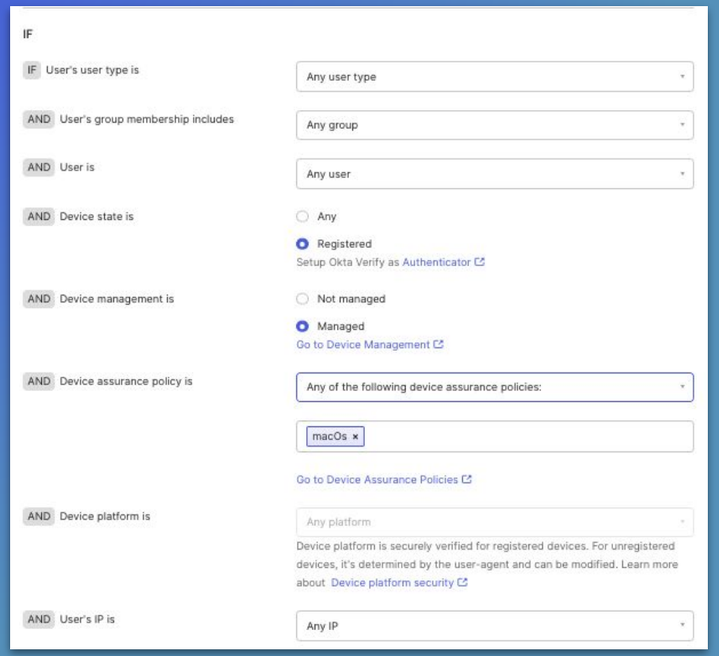
OIE

Erneute Authentifizierung bei Identity-Anbietern

Verfügbar in allen SKUs

Mechanismus, um Verbundbenutzer zu zwingen, sich bei ihrem externen Identity-Anbieter erneut zu authentifizieren und dabei jede aktive Identity-Anbieter-Session zu umgehen.

OIE



Gerätebedingungen in OAMP

Zugriffsmanagement

Early Access

Gerätegebundenes Single Sign-On (Windows und macOS)

Funktion von Okta Device Access ‖ Unterstützt für FedRAMP Moderate/High/DOD IL4

Ermöglicht Hardware-geschützte Sessions, die die Okta-Session-Wiedergabe stoppen und den Zugriff auf nachgelagerte Anwendungen nach der Geräteanmeldung vereinfachen.

Mehr erfahren

OIE

Erweiterte Compliance-Prüfungen (Windows und macOS)

Verfügbar in AMFA ‖ Autorisiert für FedRAMP Moderate/High/DOD IL4

Erfassung und Bewertung des Gerätekontexts (basierend auf beliebigen Windows- oder macOS-Geräteattributen bzw. Sicherheitseinstellungen), sodass Sie die Zero-Trust-Sicherheit während der Authentifizierung weiter stärken können.

Mehr erfahren

OIE

Okta als Fallback-Identity-Anbieter bei Routing-Regeln

Verfügbar in allen SKUs ‖ Autorisiert für FedRAMP Moderate/High/DOD IL4

Führt einen konfigurierbaren Fallback-Mechanismus ein, der Benutzer an den Okta-Identity-Anbieter weiterleitet, wenn ein externer Identity-Drittanbieter während der Anmeldung ausfällt.

Mehr erfahren

OIE

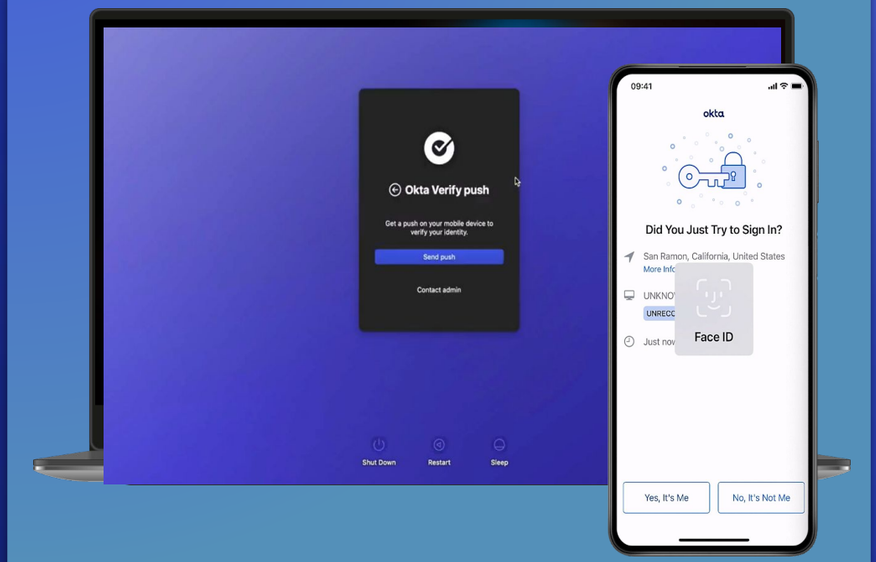
Support des SHA256-Digests in SAML-AuthN-Anfragen

Verfügbar in allen SKUs ‖ Autorisiert für FedRAMP Moderate/High/DOD IL4

Aktualisiert die SAML-Implementierung von Okta, um den sicheren SHA-256-Digest-Algorithmus anstelle des veralteten SHA-1-Standards zu verwenden.

Mehr erfahren

OIE



Gerätegebundenes Single Sign-On

Zugriffsmanagement

Early Access

Erkenntnisse zu Authentifikator-Rollouts

Funktion von MFA/AMFA || Autorisiert für FedRAMP Moderate/High/DOD IL4

Mit dieser Erweiterung des Berichts zu Authentifizierungsaktivitäten sieht der Administrator genau, wie Okta FastPass und andere Faktoren genutzt werden – nach Gerätetyp, Anmeldemethode, Verwaltungsstatus und Registrierungsstatus aufgeschlüsselt.

Mehr erfahren

OIE

Verbesserungen bei der Threat Intelligence-Erkennung

Funktion von Identity Threat Protection || Autorisiert für FedRAMP High, unterstützt für FedRAMP Moderate/High, unterstützt für DOD IL4

Anreicherung der Threat Intelligence-Erkennung von Okta mit IOC-Informationen wie IP-Adresse und ASN.

OIE

Bot-Schutz mit Okta AI

Funktion von Identity Threat Protection || Autorisiert für FedRAMP High, unterstützt für FedRAMP Moderate/High, unterstützt für DOD IL4

Verbesserte Sicherheit bei automatisierten Bot-Angriffen, wie sie häufig bei Credential Stuffing, Brute-Force-Angriffen und Account-Hacking-Versuchen auftreten. Weniger betrügerische Anmeldungen und Authentifizierungsereignisse bei gleichzeitiger Verbesserung der User Experience für legitime Benutzer.

OIE

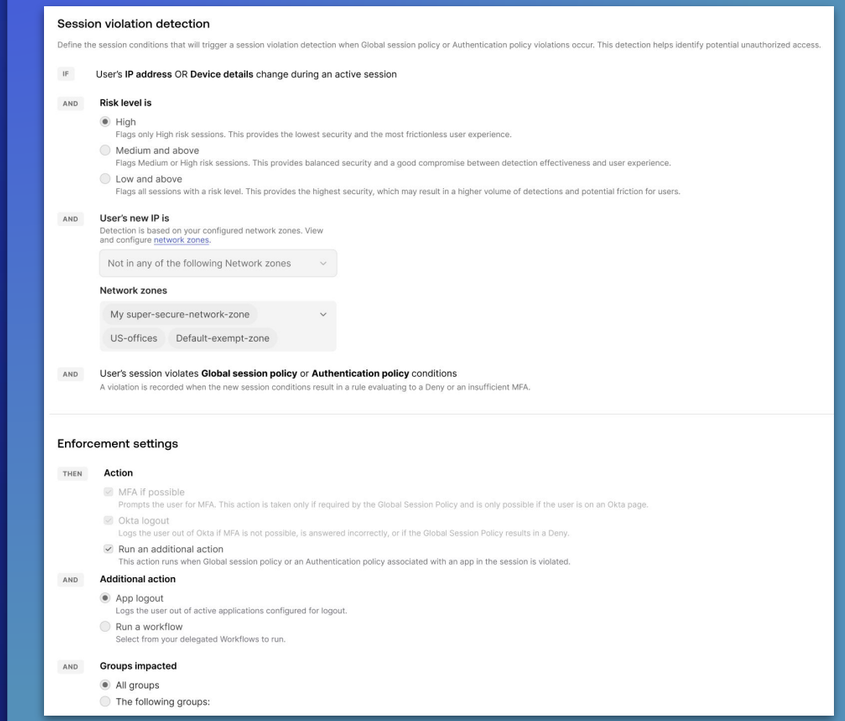
Verbesserte Session-Schutzkontrollen

Funktion von Identity Threat Protection || Autorisiert für FedRAMP Moderate/High, unterstützt für DOD IL4

Administratoren können konfigurieren, welche Änderungen des Session-Kontexts eine erneute Überprüfung der Richtlinie auslösen sollen, und ermöglichen damit eine granulare Kontrolle basierend auf der Risikotoleranz des Unternehmens.

Mehr erfahren

OIE



Verbesserte Session-Schutzkontrollen

Zugriffsmanagement

Early Access

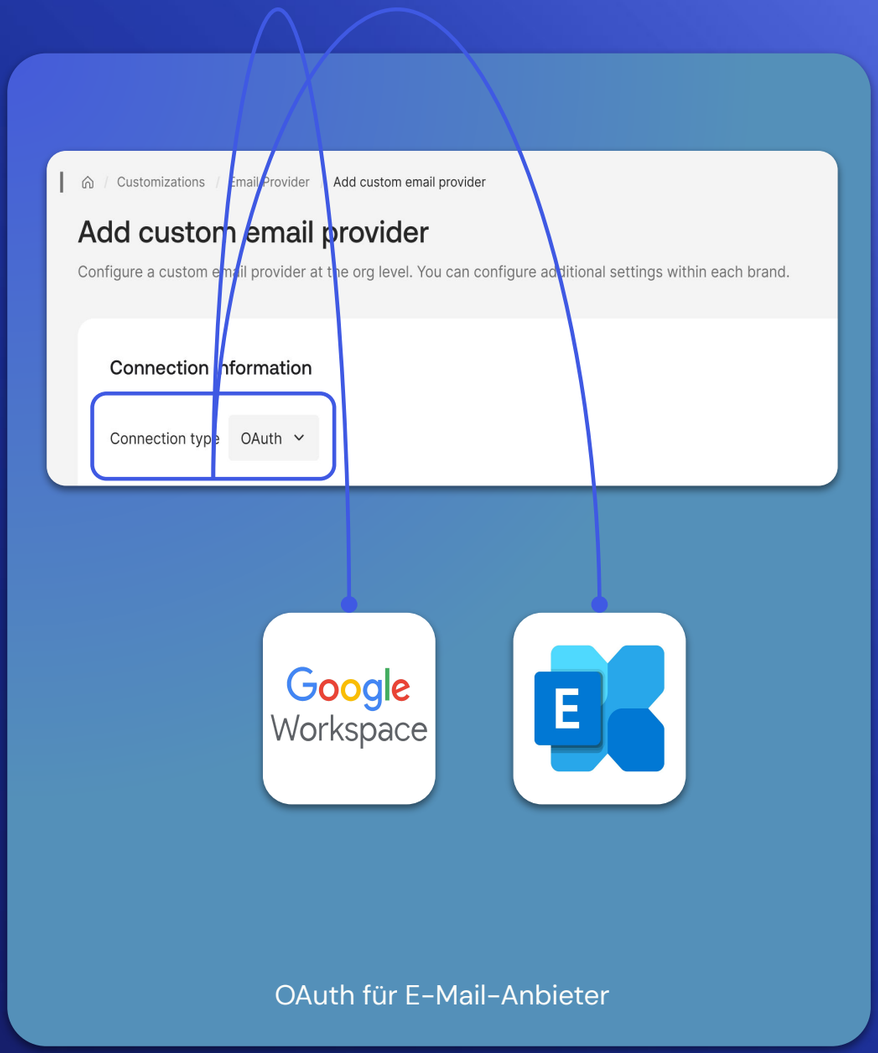
OAuth für E-Mail-Anbieter

Verfügbar in allen SKUs

Kunden, die den E-Mail-Anbieter für eigenes SMTP verwenden, können sich mit der OAuth-Authentifizierung verbinden, um die Sicherheit der Standardauthentifizierung zu erhöhen.

Mehr erfahren

OIE



OAuth für E-Mail-Anbieter

Identity-Management

Allgemein verfügbar

Sicherheitszugriffsprüfung

Verfügbar in OIG ‖ Autorisiert für FedRAMP High/DOD IL4[1], unterstützt für FedRAMP Moderate

Führt insbesondere nach Sicherheitsvorfällen eine benutzerzentrierte Zugriffsprüfung für Endbenutzer durch, um die Benutzerzugriffsebenen zu evaluieren.

Mehr erfahren

Classic OIE

Upgrade von LDAPi auf OIDC

Verfügbar in UD ‖ Autorisiert für FedRAMP High/Moderate/DOD IL4

Verlagert den LDAPi-Ansatz für Superadministratoren und Manager aus dem Directory Integration- zu einem Anwendungsinstanz-Modell.

OIE

Profilbearbeitungen für deaktivierte Benutzer

Verfügbar in UD ‖ Autorisiert für FedRAMP High/Moderate/DOD IL4

Ermöglicht Administratoren die Bearbeitung von Okta-Profilattributen für deaktivierte Benutzer. Dadurch sind Profilaktualisierungen möglich, ohne dass ein Benutzer reaktiviert werden muss.

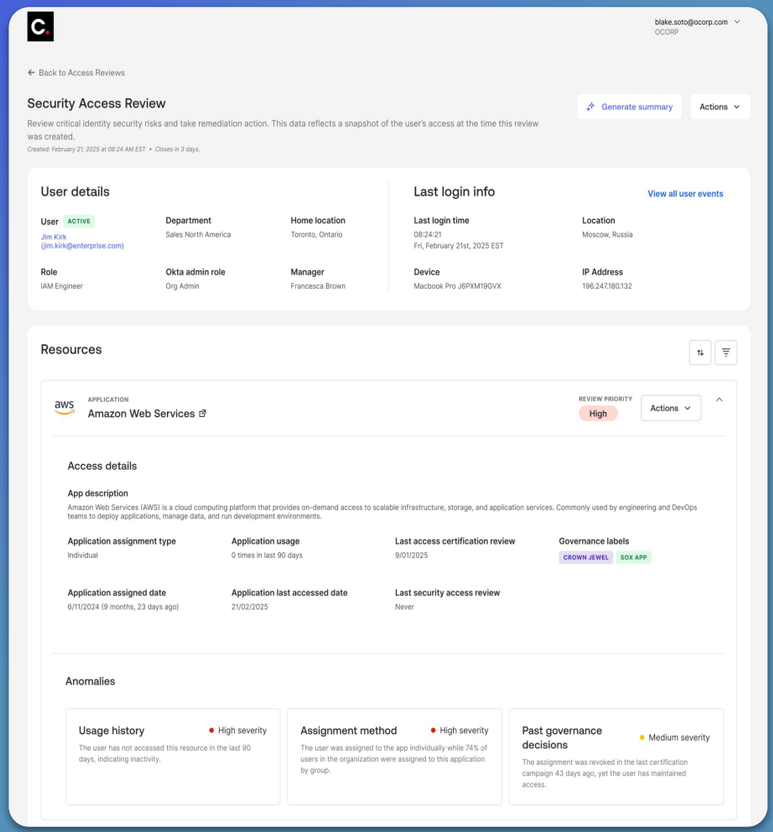
Classic OIE

Verbesserungen bei der Automatisierung von Zugriffsanfragen

Verfügbar in OIG ‖ Autorisiert für FedRAMP High/DOD IL4, unterstützt für FedRAMP Moderate

Gibt die für Benutzer sichtbare Anfrage-ID über Get-Request-APIs zurück. Übergibt die Anfrage-ID als „Aufruferkontext“ in der Delegated Workflows V1-Integration.

Classic OIE



Sicherheitszugriffsprüfung[1]

1. Durch KI/LLM generierte Zusammenfassungen sind in unseren FedRAMP- und DoD-autorisierten Cloud-Angeboten nicht verfügbar, werden aber auf ihre Aufnahme geprüft.

Identity-Management

Allgemein verfügbar

Benachrichtigungen über gewährten und widerrufenen Zugriff

Classic OIE

Verfügbar in OIG ‖ Autorisiert für FedRAMP High/DOD IL4[1], unterstützt für FedRAMP Moderate

Informiert die Benutzer von Anfragen, wenn der Zugriff gewährt oder widerrufen wird, und erläutert den Zugriffsanforderungsprozess.

Export von OIG-Berichten im PDF-Format

Classic OIE

Verfügbar in OIG ‖ Autorisiert für FedRAMP High/DOD IL4, unterstützt für FedRAMP Moderate

Exportiert Berichte als PDF-Dateien für Prüfer und Kontrollanalysten, damit diese die Compliance-Nachweise prüfen können. PDF ist das bevorzugte Format von Prüfern und GRC-Mitarbeitern.

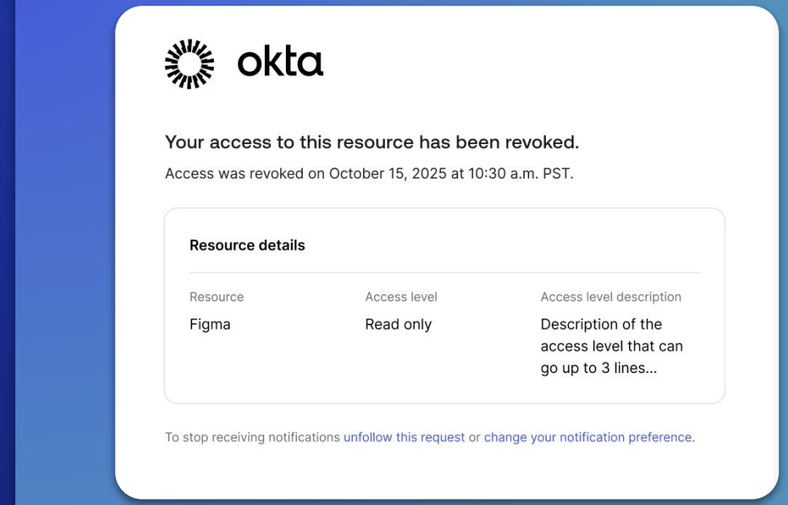
Governance-Kennzeichnungen

Classic OIE

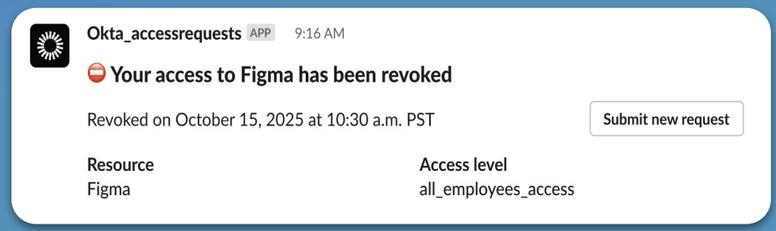
Verfügbar in OIG ‖ Autorisiert für FedRAMP High/DOD IL4, unterstützt für FedRAMP Moderate

Ermöglicht Administratoren das Hinzufügen von Kennzeichnungen zu Ressourcen in Okta und unterstützt damit OIG-Anwendungsfälle.

Mehr erfahren



Widerrufene Benachrichtigungen per E-Mail



Widerrufene Benachrichtigungen über Slack[1]

1. Von Slack generierte Benachrichtigungen sind derzeit nicht in unseren FedRAMP- und DoD-autorisierten Cloud-Angeboten verfügbar, werden aber auf ihre Aufnahme geprüft.

Identity-Management

Allgemein verfügbar

Berechtigungshistorie

Classic OIE

Verfügbar in OIG ‖ Autorisiert für FedRAMP High/DOD IL4, unterstützt für FedRAMP Moderate

Visualisiert die Veränderungen bei den Berechtigungszuweisungen für eine Anwendung im zeitlichen Verlauf. Einblicke in Zugriffsänderungen und Vereinfachung der Benutzerzugriffsprüfung für Superadministratoren und Prüfer.

Mehr erfahren

Office 365-Anwendung für die GCC-Umgebung

Classic OIE

Verfügbar in UD ‖ Autorisiert für FedRAMP High/Moderate/DOD IL4

Unterstützt die Office 365-Integration innerhalb der GCC-Umgebung von Microsoft. Diese Funktion wird von Administratoren verwaltet.

Bidirektionale LDAP-APIs

Classic OIE

Verfügbar in Okta Directory-Integrationen ‖ Autorisiert für FedRAMP High/Moderate

Einfaches Hinzufügen oder Entfernen von Benutzern in lokalen Gruppen auf der Basis von Triggern, die in Okta mit APIs für LDAP festgelegt werden.

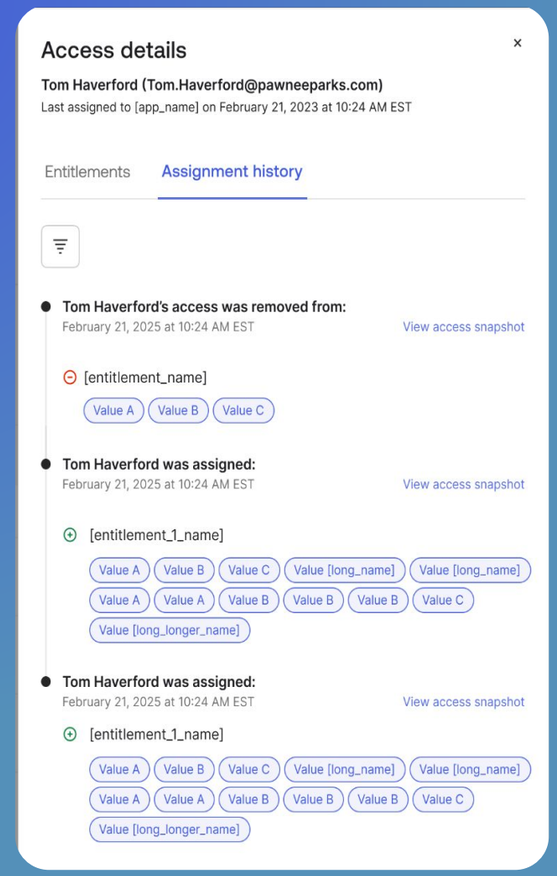
Ressourceninhaber

Classic OIE

Verfügbar in OIG ‖ Autorisiert für FedRAMP Moderate/High/DOD IL4

Steuert Richtlinien auf Basis von Ressourceneigenschaften und vereinfacht die Governance, indem verantwortlichen Ressourcenbesitzern Aufgaben zugewiesen werden.

Mehr erfahren



Berechtigungshistorie

Identity-Management

Allgemein verfügbar

Einheitliche Audit-Berichte in Access Certifications

Classic OIE

Verfügbar in OIG || Autorisiert für FedRAMP High/DOD IL4, unterstützt für FedRAMP Moderate

Generiert Compliance-Audit-Daten an einem zentralen Ort in Access Certifications für alle Berichtsanforderungen.

Mehr erfahren

Zugriffsanforderungen für Active Directory-Gruppen

Classic OIE

Verfügbar in OIG || Autorisiert für FedRAMP High/DOD IL4, unterstützt für FedRAMP Moderate

Fordert für Benutzer Zugriff auf Active Directory-Gruppen an und nutzt dabei die bidirektionale AD-Synchronisierung für das Hinzufügen von Benutzern und den zeitbasierten Widerruf.

Mehr erfahren

Zuweisen von Genehmigungen zu Ressourcenbesitzern

Classic OIE

Verfügbar in OIG || Autorisiert für FedRAMP High/DOD IL4, unterstützt für FedRAMP Moderate

Vereinfachung und Verringerung der Anzahl von Zugriffsanforderungssequenzen mithilfe generischer Besitzer, die an Ressourcen gebunden sind.

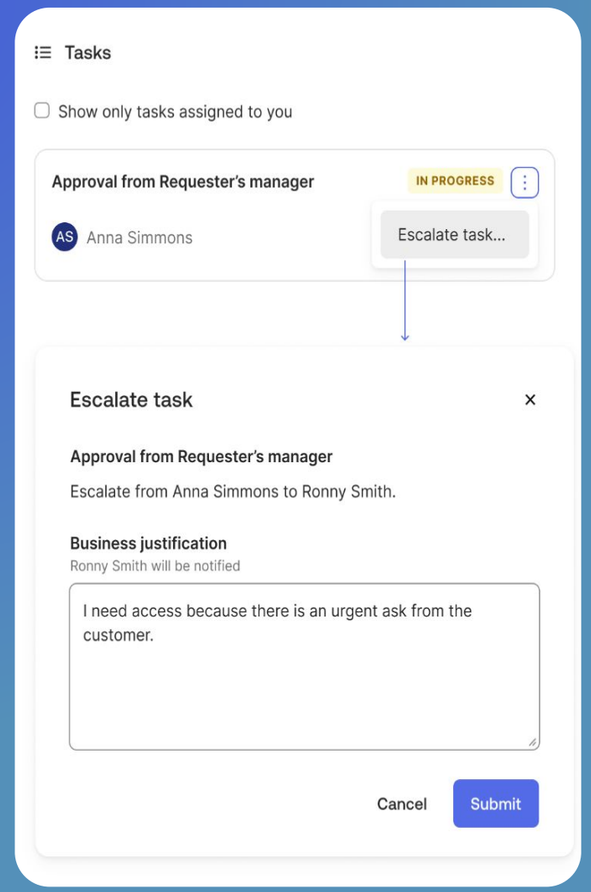
Eskalationen der Genehmigung

Classic OIE

Verfügbar in OIG || Autorisiert für FedRAMP High/DOD IL4, unterstützt für FedRAMP Moderate

Optimierung von Genehmigungen, indem Benutzern ermöglicht wird, ihre Anfragen zu eskalieren, wenn die zuständigen Genehmiger nicht im Büro oder nicht erreichbar sind.

Mehr erfahren



Eskalationen der Genehmigung

Identity-Management

Allgemein verfügbar

Anything-as-a-Source (XaaS): Gruppen

Classic OIE

Verfügbar in LCM || Autorisiert für FedRAMP Moderate/High/DOD IL4

Verwaltung von Gruppen und Gruppenmitgliedschaften mit Anything-as-a-Source-APIs.

Neue Integrationen für Provisionierung/Berechtigungen

Classic OIE

Funktion von OIG/LCM || OIG – Autorisiert für FedRAMP High/DOD IL4, unterstützt für FedRAMP Moderate.
LCM – Autorisiert für FedRAMP Moderate/High/DOD IL4

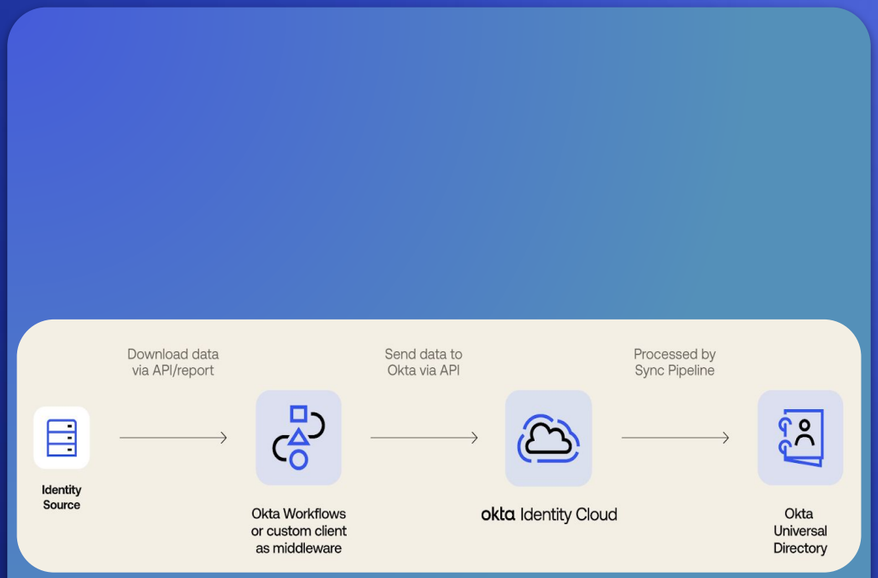
Neue Integrationen für Provisionierung/Berechtigungen für CrowdStrike, LucidChart, Netskope, Oracle IAM, SAP Analytics, SAP Concur, Trend Micro und Mimecast.

Verbesserungen des Import-Überblicks

Classic OIE

Verfügbar in LCM || Autorisiert für FedRAMP Moderate/High/DOD IL4

Mehr Einblicke für Administratoren in die Importschritte und den Fortschritt, sodass ihr Vertrauen in den Okta-Prozess durch Transparenz und Zuverlässigkeit gestärkt wird.



Anything-as-a-Source (XaaS): Gruppen

Identity-Management

Early Access

On-prem Connector: Generische Datenbank (JDBC)

Classic | OIE

Verfügbar in OIG

Bietet sofort einsatzbereite Verbindungen für die Provisionierung von Lifecycle Management (LCM) und das Berechtigungsmanagement für generische Datenbanken mit einem JDBC-Connector.

Zugriffszertifizierungen für Sammlungen

Classic + OIE

Verfügbar in OIG || Autorisiert für FedRAMP High/DOD IL4, unterstützt für FedRAMP Moderate

Durchführung von Zugriffszertifizierungskampagnen an Sammlungen für Superadministratoren.

Slack-Benachrichtigungen für Zugriffszertifizierungen

Classic | OIE

Verfügbar in OIG

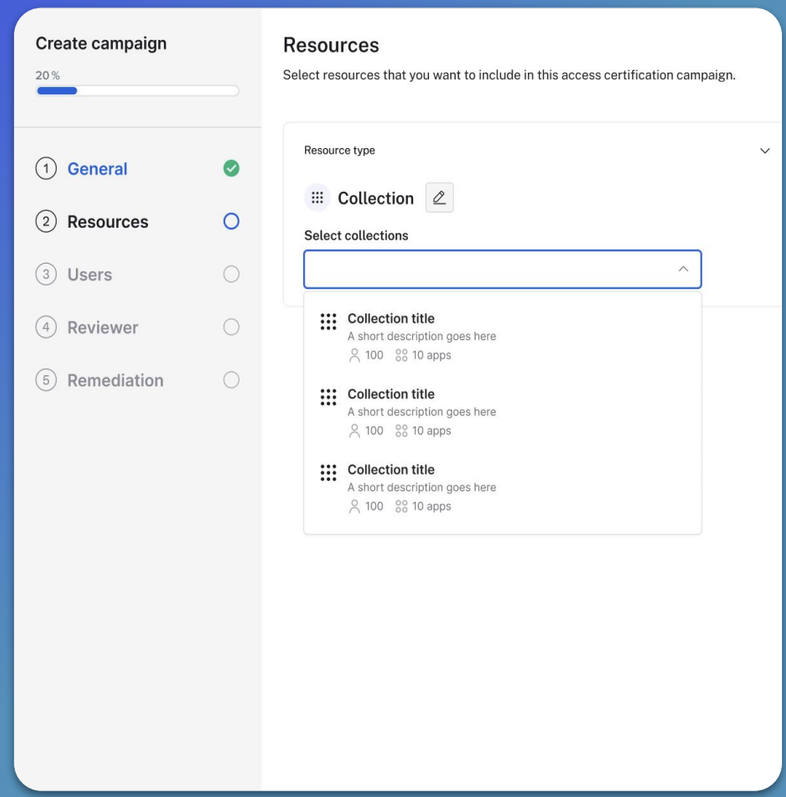
Integration von Slack mit Zugriffszertifizierungen, sodass zugewiesene Prüfer direkt über Slack Kampagnenerinnerungen erhalten können.

Flexible Berechtigungszuweisungen

Classic | OIE

Verfügbar in OIG || Autorisiert für FedRAMP High/DOD IL4, unterstützt für FedRAMP Moderate

Zuweisung von Berechtigungen für Benutzer ohne bestehende Zuweisungen, sodass Administratoren bei der Verwaltung von Zuweisungen mehr Flexibilität erhalten.



Zugriffszertifizierungen für Sammlungen

Identity-Management

Early Access

Workday: Inkrementelle Importe

Verfügbar in LCM ‖ Autorisiert für FedRAMP Moderate/High/DOD IL4

Ermöglicht den schnelleren Import geänderter Benutzeridentitäten und Zugriffsrechte aus Workday in Okta, sodass Administratoren schnell über die aktuellsten Benutzer- und Gruppendaten verfügen.

Classic

OIE

Zugriffszertifizierungen für Service-Accounts

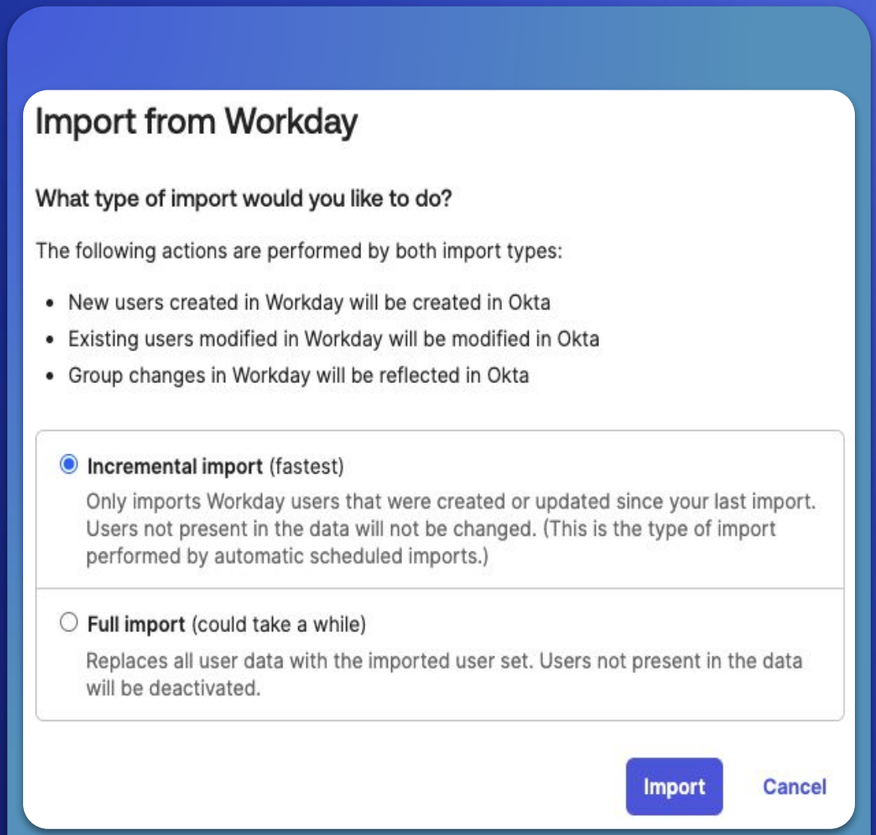
Verfügbar in OIG ‖ Autorisiert für FedRAMP High/DOD IL4, unterstützt für FedRAMP Moderate

Verwaltung von Zertifizierungskampagnen für Service-Accounts in Okta Privileged Access.

Mehr erfahren

Classic

OIE



Workday: Inkrementelle Importe

Privileged Access

Allgemein verfügbar

Japanische Produktionszelle

Funktion von Okta Privileged Access

Bietet Kunden in Japan eine Umgebung in der Region, die den lokalen Anforderungen an Datenresidenz und Datensouveränität entspricht.

Classic OIE

Workload Identity für DevOps: SSH-Automatisierung

Funktion von Okta Privileged Access || Verfügbar in allen kostenpflichtigen Tarifen

Der erste Anwendungsfall für einen neuen Ressourcentyp. Ermöglicht einer Workload, ihre Identität nachzuweisen und für die Automatisierung sicher OPA-geschützte Ressourcen/Anmeldedaten abzurufen.

Classic OIE

Offenlegung des Passworts für sicher verwahrte Accounts auf Servern

Funktion von Okta Privileged Access || Verfügbar in allen kostenpflichtigen Tarifen

Möglichkeit, das Passwort eines sicher verwahrten Accounts auf Servern offenzulegen. Neue Richtlinienberechtigung, um den Zugriff auf Passwörter nur denjenigen zu ermöglichen, die ihn benötigen.

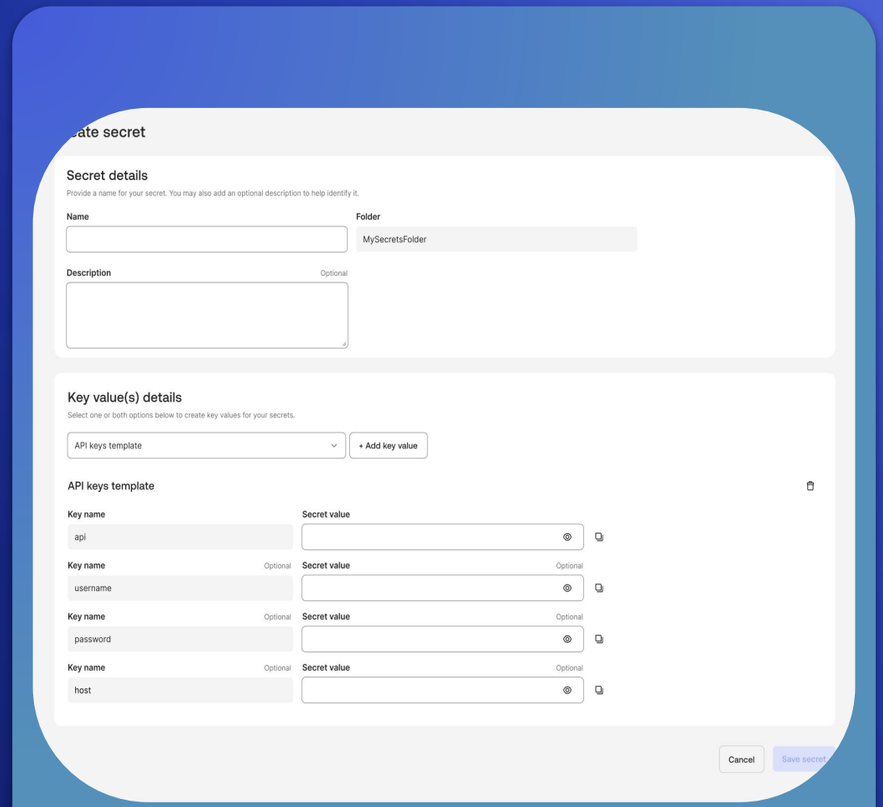
Classic OIE

Templates für Secrets

Funktion von Okta Privileged Access || Verfügbar in allen kostenpflichtigen Tarifen

Vordefinierte Secret-Vorlagen (z. B. API-Keys, Datenbank-Anmeldedaten), die die manuelle Schlüssel/Wert-Eingabe durch eine geführte Dropdown-Experience ersetzen.

Classic OIE



Templates für Secrets

Privileged Access

Early Access

OPA: AD-Accounts – Beim Import nicht rotieren

Classic OIE

Funktion von Okta Privileged Access ‖ Verfügbar in allen kostenpflichtigen Tarifen

Minimiert Unterbrechungen bei Abläufen, indem Endbenutzern die Möglichkeit gegeben wird, die Änderung des vorläufigen Passworts hinauszuzögern, damit sie ihren Account ohne unmittelbare Folgen für sich selbst oder ihre Anwendungen einrichten können.

OPA: SaaS-Accounts – Beim Import nicht rotieren

Classic OIE

Funktion von Okta Privileged Access ‖ Verfügbar in allen kostenpflichtigen Tarifen

Minimiert Unterbrechungen bei Abläufen, indem Endbenutzern die Möglichkeit gegeben wird, die Änderung des vorläufigen Passworts hinauszuzögern, damit sie ihren Account ohne unmittelbare Folgen für sich selbst oder ihre Anwendungen einrichten können.

Jetzt für Endbenutzer rotieren – AD-Accounts

Classic OIE

Funktion von Okta Privileged Access ‖ Verfügbar in allen kostenpflichtigen Tarifen

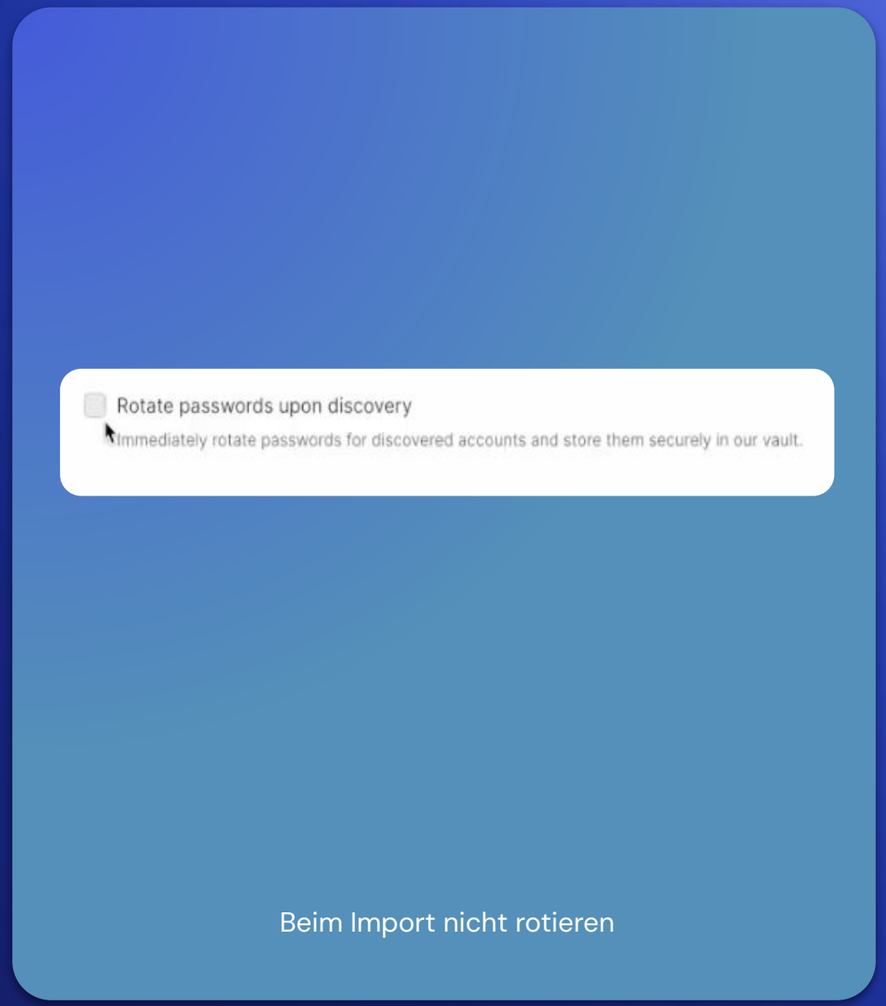
Gewährt dem Benutzer eines Accounts die Möglichkeit, das AD-Passwort sofort selbst (ohne die Hilfe eines Administrators) zu ändern.

Jetzt für Endbenutzer rotieren – SaaS-Service-Accounts

Classic OIE

Funktion von Okta Privileged Access ‖ Verfügbar in allen kostenpflichtigen Tarifen

Gewährt dem Benutzer eines SaaS-Service-Accounts die Möglichkeit, das Passwort sofort selbst (ohne die Hilfe eines Administrators) zu ändern.



Beim Import nicht rotieren

Privileged Access

Early Access

SaaS-Service-Account – benutzerdefinierte Passwort-Synchronisierung

Classic OIE

Funktion von Okta Privileged Access ‖ Verfügbar in allen kostenpflichtigen Tarifen

Ermöglicht die Rotation des „aktuellen + neuen“ Passworts für SCIM-basierte Anwendungen und ein „Sicherheitsventil“, um Vault-Aufzeichnungen manuell zu aktualisieren, wenn die Anmeldedaten mit den Zielsystemen nicht mehr synchron sind.

OPA: Vaulting für Okta-fähiges AD-basierte Accounts

Classic OIE

Funktion von Okta Privileged Access ‖ Verfügbar in allen kostenpflichtigen Tarifen

Ermöglicht, dass OPA-verwaltete AD-Accounts auch Okta-Benutzer sein können, und definiert das Okta-Benutzerstatusverhalten von OPA-AD-Account-Regeln.

OPA: Import-Filterung von Active Directory-Accounts

Classic OIE

Funktion von Okta Privileged Access ‖ Verfügbar in allen kostenpflichtigen Tarifen

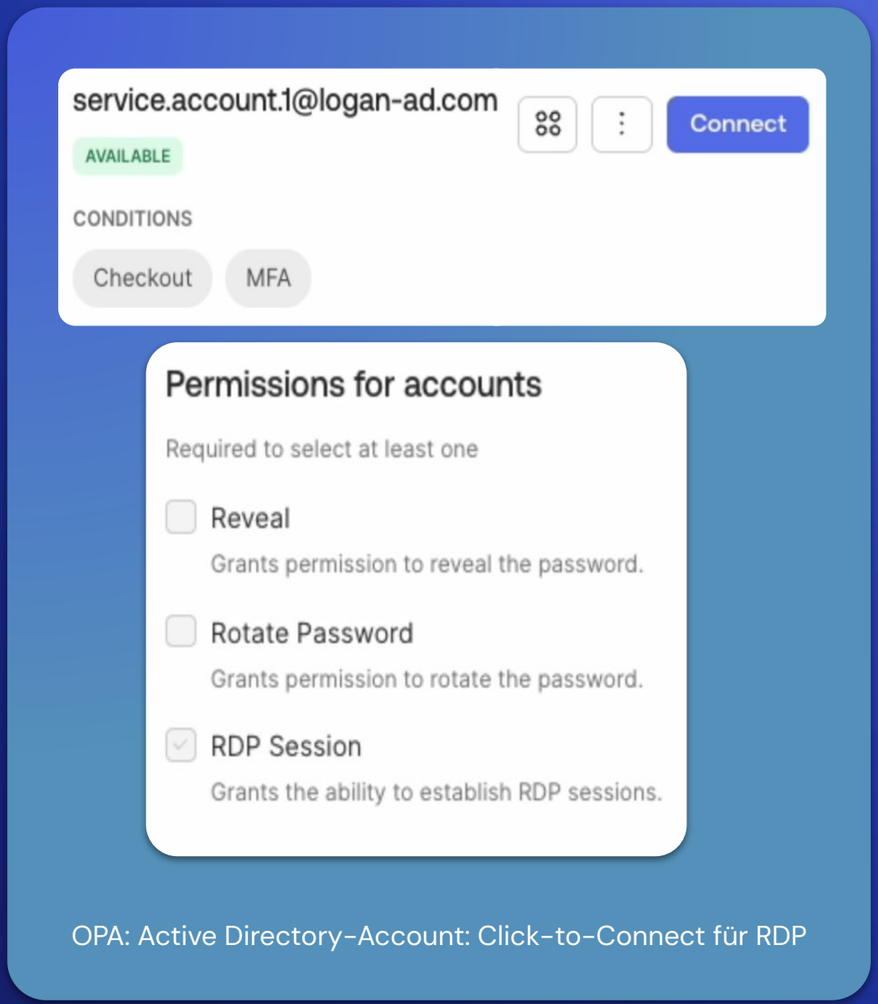
Möglichkeit zum Filtern von Accounts in der Organisationseinheit, die den Kriterien „beginnt mit“, „endet mit“, „enthält“ oder der Gruppe entsprechen.

OPA: Active Directory-Account: Click-to-Connect für RDP

Classic OIE

Funktion von Okta Privileged Access ‖ Verfügbar in allen kostenpflichtigen Tarifen

Click-to-Connect für RDP bei AD-Accounts unterstützt passwortlose Authentifizierung mit SSO für RDP.



OPA: Active Directory-Account: Click-to-Connect für RDP

Privileged Access

Early Access

OPA: Active Directory-Account: Click-to-Connect für SSH

Classic OIE

Funktion von Okta Privileged Access ‖ Verfügbar in allen kostenpflichtigen Tarifen

Ermöglicht nahtlosen, passwortlosen Click-to-Connect-SSH-Zugriff auf Ressourcen, die in Active Directory eingebunden sind.

OPA: Active Directory-Account: lokale Server-Berechtigung für RDP

Classic OIE

Funktion von Okta Privileged Access ‖ Verfügbar in allen kostenpflichtigen Tarifen

Ermöglicht die zentrale Kontrolle der lokalen Serverberechtigungen und eliminiert damit Standing Access. Berechtigungen werden just-in-time gewährt und nach Ende der Sessions wieder entfernt.

OPA: Active Directory-Account: RDP-Domain-Controller

Classic OIE

Funktion von Okta Privileged Access ‖ Verfügbar in allen kostenpflichtigen Tarifen

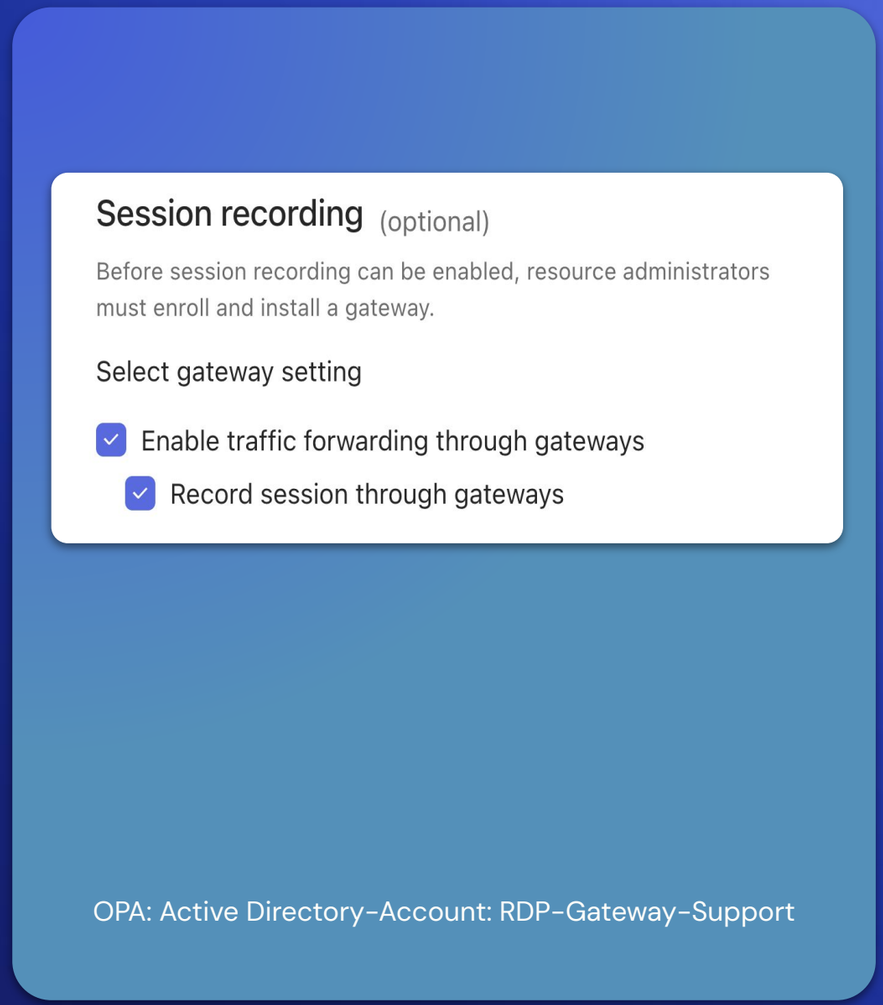
Schutz des RDP-Zugriffs auf Domain-Controller mit OPA, damit alle Windows Server-Typen geschützt sind.

OPA: Active Directory-Account: RDP-Gateway-Support

Classic OIE

Funktion von Okta Privileged Access ‖ Verfügbar in allen kostenpflichtigen Tarifen

Ermöglicht Zero-Trust-Netzwerkarchitektur, bei der nur authentifizierte und autorisierte Benutzer eine Verbindung zu Servern hinter Gateways herstellen können.



OPA: Active Directory-Account: RDP-Gateway-Support

Platform Services

Allgemein verfügbar

Übermittlung von Berechtigungsmanagement an OIN

Funktion von Okta Platform || Verfügbar in allen Tarifen

Ermöglicht es Integratoren, SCIM-basierte Berechtigungsmanagement-Integrationen zu erstellen, zu testen und an OIN zu übermitteln – schneller, sicherer und ohne manuelle Übergaben.

Classic OIE

Übermittlung von API-Service-Integrationen an OIN-Assistenten (SIE)

Funktion von Okta Platform || Verfügbar in allen Tarifen

Self-Service-Workflow, mit dem ISVs API-Service-Integrationen erstellen, testen und an OIN übermitteln können – schneller, sicherer und ohne manuelle Übergaben.

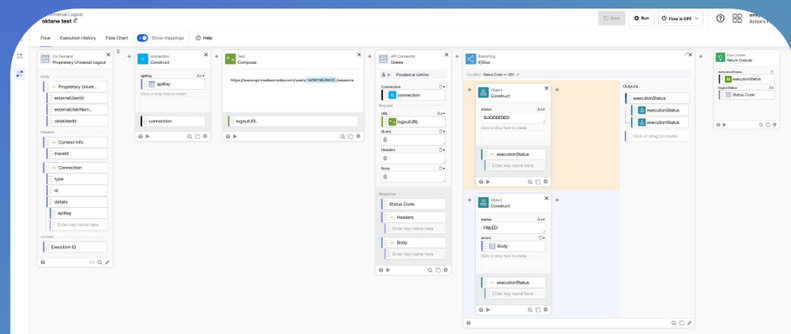
Classic OIE

Actions: API-Integrationen

Funktion von Okta Platform || Verfügbar in allen Tarifen

Low-Code-Builder, mit dem ISVs Okta-Integrationen (Provisionierung, Berechtigungen, Universal Logout, Workflows) erstellen können, die von Okta-Produkten nahtlos aufgerufen werden (z. B. Abruf und Aktualisierung von Berechtigungen oder Auslösung einer risikobasierten Abmeldung).

Classic OIE



Actions: API-Integrationen

Platform Services

Allgemein verfügbar

Identity Threat Protection, Okta Identity Governance und Workflows für US-amerikanischen öffentlichen Sektor

Classic

OIE

Funktion von Okta Platform || Identity Threat Protection – Autorisiert für FedRAMP Moderate/High, unterstützt für DOD IL4. Okta Identity Governance und Workflows – Autorisiert für FedRAMP High/DOD IL4, unterstützt für FedRAMP Moderate

Bietet eine einheitliche Grundlage für die Implementierung zentraler Sicherheitsprinzipien, die in Frameworks wie DoW Instruction 8520.04 („Identity Assurance“), DoW CIO Memorandum, „Modernizing SAAR and AAP through ICAM Workflows“ und anderen hervorgehoben werden.

Mehr erfahren

Okta Aerial für Multi-Org-Management

Classic

OIE

Funktion von Okta Platform || Verfügbar in Sandbox- und Multi-Org Platform-SKU

Zentrales Dashboard auf Account-Ebene, das Transparenz und Managementfunktionen für mehrere Okta Orgs innerhalb eines einzelnen Kunden-Accounts bietet.

Mehr erfahren

Neue Workflows-Konnektoren

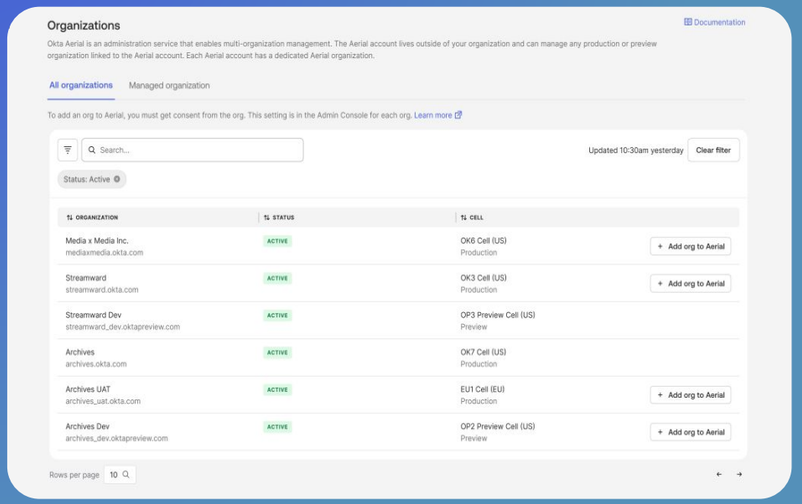
Classic

OIE

Funktion von Workflows || Verfügbar in allen Workflows-SKUs

Integration mit mehr Okta-APIs und gängigen Anwendungen (Checkpoint, LucidChart, Okta OIG, Snowflake, Tenable, Trend Micro) zur Verwaltung von Benutzern und Gruppen.

Mehr erfahren



Okta Aerial für Multi-Org-Management

Platform Services

Allgemein verfügbar

Globale Suche – Enthält

Funktion von Okta Platform || Verfügbar in allen Tarifen

Administratoren können über die globale Suchleiste nach Benutzern mit einem bestimmten Domain-Namen oder einer teilweisen Übereinstimmung eines Gruppennamens suchen, um die Notwendigkeit zu reduzieren, in der erweiterte Suche produktübergreifend zu navigieren.

Classic OIE

Verbesserungen des App-Umschalters

Funktion von Okta Platform || Verfügbar in allen Tarifen || Autorisiert für FedRAMP Moderate/High/DOD IL4

Okta-Benutzer ohne Administratorrechte können den App-Umschalter für die schnelle und nahtlose Navigation zwischen verschiedenen Okta-eigenen Anwendungen verwenden. Dem App-Umschalter wurden weitere Okta-Produkte hinzugefügt, um einen zentralen, praktischen Ort für den Zugriff auf Ihr Okta-Ökosystem zu schaffen.

Classic OIE

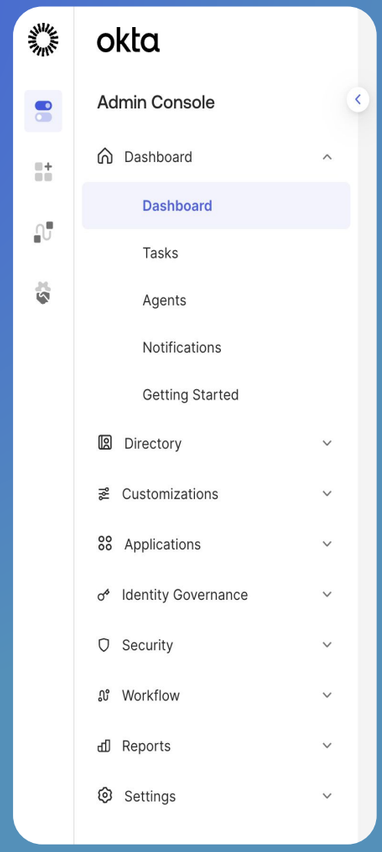
Zellerweiterungen – Kanada und Indien

Funktion von Okta Platform || Verfügbar in allen Tarifen

Ermöglicht es Kunden, Daten lokal in diesen Regionen zu hosten, um Datenresidenzanforderungen zu unterstützen und dynamische Anforderungen in den Bereichen Daten, Sicherheit und Compliance zu erfüllen.

Mehr erfahren

Classic OIE



Verbesserungen des App-Umschalters

Platform Services

Early Access

RBAC-Ordnerrollen

Classic

OIE

Funktion von Workflows || Autorisiert für FedRAMP High/DOD IL4, unterstützt für FedRAMP Moderate

Gewährt Benutzern Zugriff auf einzelne Ordner, in denen sie nur bestimmte Abläufe, Tabellen und Verbindungen verwenden und verwalten können. Ermöglicht es Kunden, die Nutzung von Workflows auch Benutzern zu erlauben, die nicht zum IT-Team gehören.

Mehr erfahren

Governance für Workflows

OIE

Funktion von Workflows || Autorisiert für FedRAMP High/DOD IL4, unterstützt für FedRAMP Moderate

Ermöglicht es Unternehmen, den Zugriff auf die Workflows-Plattform mithilfe von OIG Access Requests and Certifications sicher zu verwalten. Vereinfacht Rollenzuweisungen und gewährt zeitgebundene Zugriffsrechte mit benutzerdefinierten Zugriffsanforderungen.

Mehr erfahren

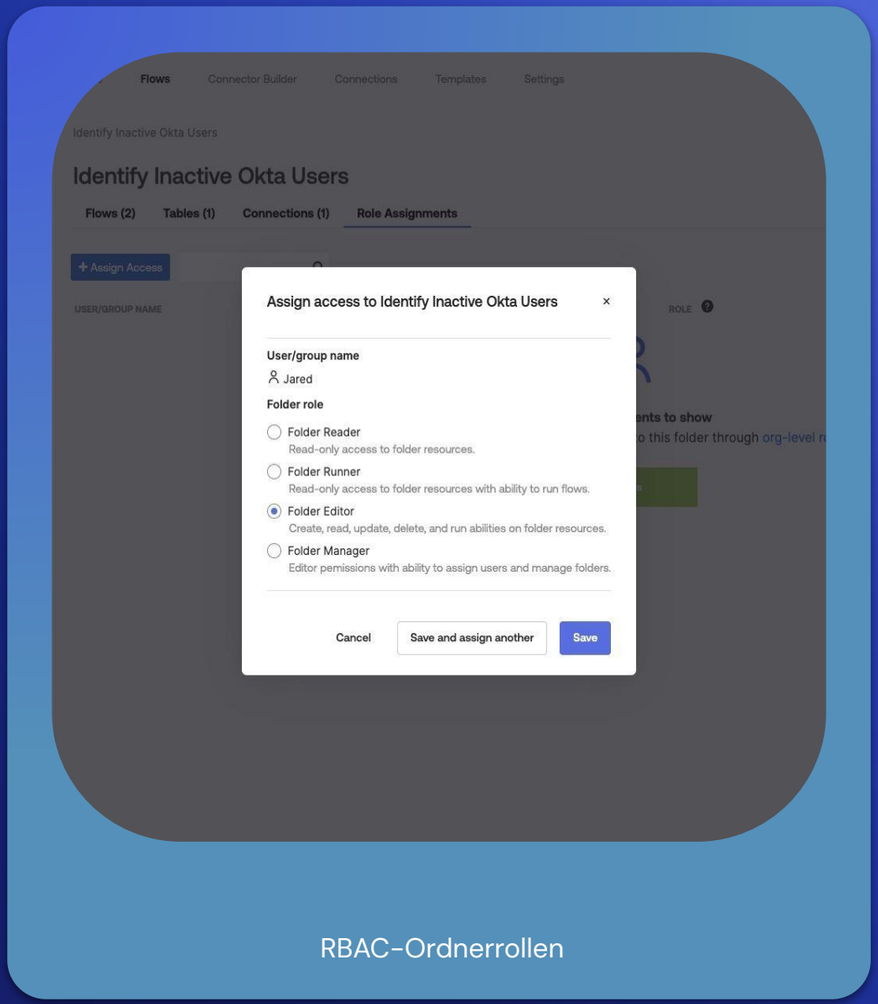
SKU für Workflows Dedicated Infrastructure Add-on

Classic

OIE

Funktion von Workflows || Verfügbar in Workforce/Customer Identity Workflows Dedicated Infrastructure Add-on

Unterstützt leistungsstärkere Anwendungsfälle mit höherer Zuverlässigkeit, insbesondere im Bereich des Niedriglatenzmodus und der Nutzung von Inline-Hooks, sowie ein höheres Volumen an Anfragen durch gelockerte Systemgrenzen.



RBAC-Ordnerrollen

Vereinheitlichung und Absicherung aller Identitäten mit Okta

Okta Platform

Okta Workforce Identity

Sie implementieren sicheren Zugriff für Ihre internen Benutzer mithilfe aller Identity-Tools, die Sie für End-to-End-Transparenz, Verwaltung und Governance benötigen.

- Posture Management
- Secure Partner Access
- PAM

Okta Customer Identity

Sie implementieren nahtlose und sichere Experiences für alle externen Identitäten, unabhängig davon, ob es sich um Kunden, Partner oder Lieferanten handelt.

- Erweiterte Verzeichnisverwaltung
- Social Login
- Lifecycle Management

Shared Identity Platform

Single Sign-On, passwortlose Authentifizierung, Adaptive MFA, Identity Threat Protection, Governance

Orchestrierung und Integration

- Automatisierte Workflows
- API-gestützte Verbindungen
- Nahtloser Anwendungszugriff

Skalierbarkeit und Zuverlässigkeit der Plattform

- Keine planmäßigen Ausfallzeiten
- Selbstheilende Nodes
- Granulare Anzahl-begrenzung
- Redundantes SaaS, PaaS und IaaS
- Datenresidenz
- >99,99 % Verfügbarkeit
- Stark skalierbar
- Mehrstufige Verschlüsselungs-architektur

Einhaltung von Compliance-Anforderungen

FR · CSA STAR Certification · HIPAA · PCI DSS Compliant · Sarbanes-Oxley Compliant · GDPR · AICPA SOC · VPAT Compliant

Einheitliche Identität für den Identity Security Fabric

- Bürger
- Mitarbeiter
- Auftragnehmer
- Verbraucher
- B2B-Kunden
- Partner
- ISVs
- KI-Agenten

Platform Services

Early Access

Self-Service-Failover – Erweiterte Disaster Recovery

Funktion von Okta Platform || Verfügbar in Enhanced Disaster Recovery

Ermöglicht es Kunden, über ein Self-Service-Portal oder eine API auf eine Disaster Recovery-Region zurückzugreifen oder ihre Okta Orgs in der primären Region wiederherzustellen.

Mehr erfahren

Classic

OIE

Okta Aerial: API zum Löschen von Orgs

Funktion von Okta Platform || Verfügbar in Sandbox- und Multi-Org Platform-SKU

Ermöglicht es Kunden, die Okta Aerial-API aufzurufen, um unerwünschte Orgs in einem Account zu löschen und zu entfernen. Hilft Kunden, eine aktuelle Liste aktiver Orgs zu führen und sich an DSGVO-Prozesse zu halten.

Mehr erfahren

Classic

OIE

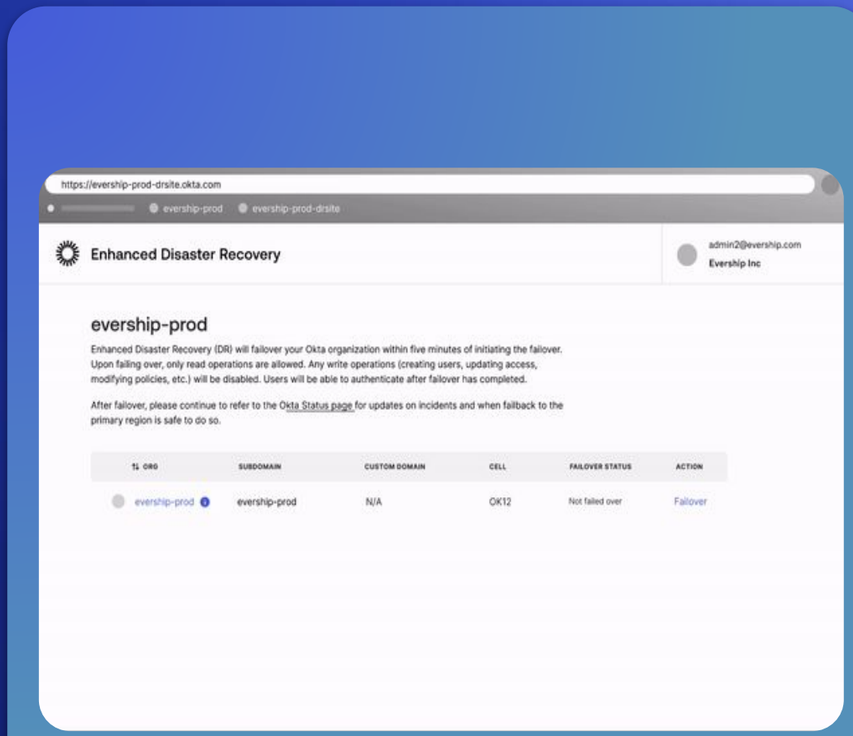
Erweiterungen der Administratorrolle und Prüferrolle

Funktion von Okta Platform || Verfügbar in allen Tarifen || Autorisiert für FedRAMP Moderate/High/DOD IL4

Ermöglicht es, Okta-Administratoren eine schreibgeschützte Version jeder standardmäßigen oder benutzerdefinierten Administratorrolle zuzuweisen. Setzt das Prinzip des Least-Privilege-Zugriffs für Benutzer- und API-Dienstintegrationen durch und ermöglicht gleichzeitig die Delegierung von Audit-Aufgaben.

Classic

OIE



Self-Service-Failover – Erweiterte Disaster Recovery

Okta Learning

Allgemein verfügbar

Schutz nicht-menschlicher Identitäten

Funktion von Produkt / Verfügbar in SKU

Dieser Lernpfad führt nicht-menschliche Identitäten ein, erklärt, wie man sie identifiziert, und stellt die ISPM- und OPA-Angebote von Okta für deren Verwaltung vor.

Mehr erfahren

Classic OIE

Branding Ihrer Okta Customer Identity-Experience

Funktion von Produkt / Verfügbar in SKU

Dieser Lernpfad bietet eine umfassende Lösung und zeigt Ihnen, wie Sie die standardmäßige Login-Experience von Okta in eine vollständig benutzerdefinierte, gebrandete Benutzeroberfläche verwandeln.

Mehr erfahren

Classic OIE

Expert Learning Pass

Funktion von Produkt / Verfügbar in SKU

Okta Identity Governance: Lernpfade und Skill-Badges:

- Zugriffsanforderungen
- Berechtigungsmanagement
- Zugriffszertifizierungen

Live Learning Labs – kürzlich wurden neue FastPass-Labs bis einschließlich März in den Kalender aufgenommen.

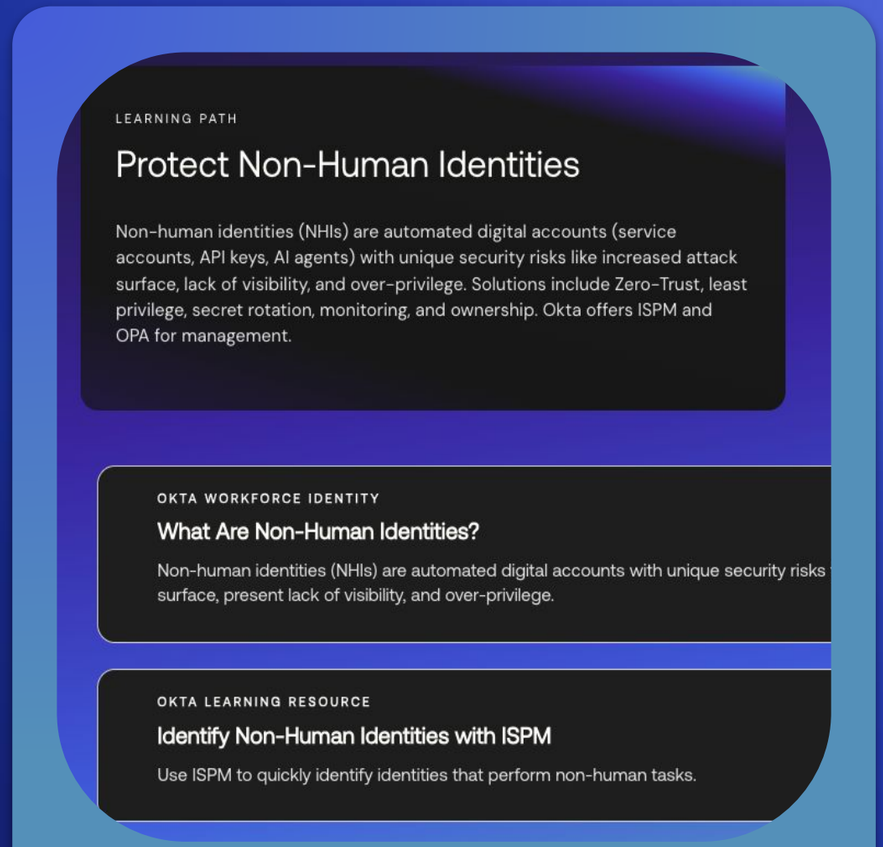
Classic OIE

Zertifizierung

Funktion von Produkt / Verfügbar in SKU

Neue praktische Prüfungen für Okta Certified Professional- und Administrator-Zertifizierungen.

Classic OIE



Lernpfad: Schutz nicht-menschlicher Identitäten

Entwicklerressourcen

Okta Workforce Identity

Mit Okta können Sie User Experiences entwickeln, integrieren und bereitstellen, die großen Benutzerkomfort bieten. Sie profitieren von den neuesten Release-Updates, kuratierten Leitfäden und Community-Feedback zu Ihren Versionen.

Ressourcen

Okta Architecture Center: Klicken Sie hier.

Workshops zu Vorteilen für Unternehmen: Klicken Sie hier.

Developer-Blog: Klicken Sie hier.

Sprachen und SDKs: Klicken Sie hier.

Leitfäden zu ersten Schritten: Klicken Sie hier.

Release-Hinweise: Klicken Sie hier.

Okta-Entwickler-Community-Forum: Klicken Sie hier.

Okta-Community-Toolkit – Anwendungspräsentation: Klicken Sie hier.

OktaDev-YouTube-Kanal: Klicken Sie hier.

okta

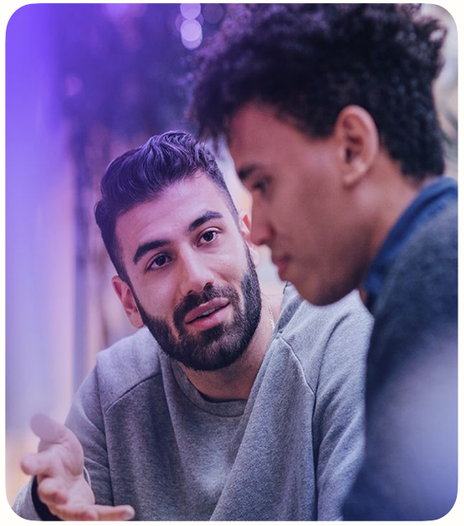
Okta Customer Identity–Releases

Okta Customer Identity gewährleistet, dass die Sicherheit Ihrer nahtlosen digitalen Experiences an erster Stelle steht. Dadurch erzielen Unternehmen schnelleres Wachstum, bleiben der dynamischen Bedrohungslandschaft einen Schritt voraus und können ihre Kunden und Geschäftsdaten absichern.

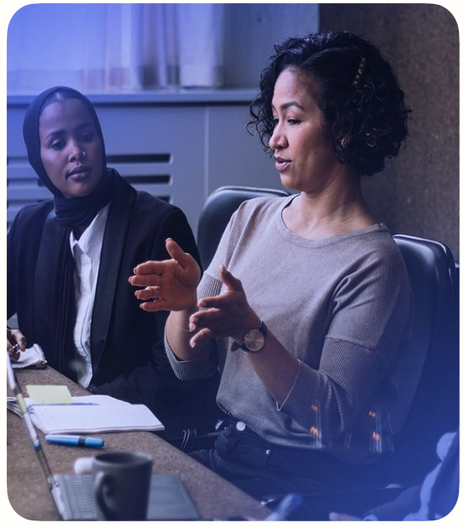
Informieren Sie sich über unsere neuesten Releases.

Okta Customer Identity für Ihre Identity-Anforderungen von heute und morgen

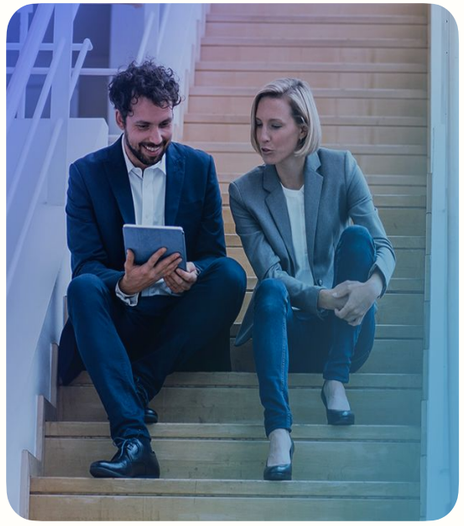
Okta Customer Identity wird von Tausenden Kunden genutzt



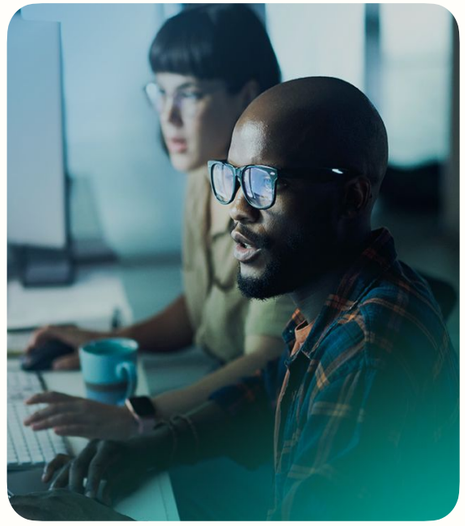
Entwickelt für branchenübergreifende IT- und Security-Teams



Konzipiert für nahtlose User Experiences



Erweiterte Sicherheitsfunktionen für den notwendigen Überblick, um Angriffe zu erkennen und abzuwehren



Early Access

Spotlight: Verbesserungen beim Customer Identity-Schutz

Kontinuierliche Identity-Sicherheit während des gesamten Prozesses: vor, während und nach der Anmeldung.

Was ist das?

Okta Identity Threat Protection (ITP) für OCI ist eine kontinuierliche, Identity-zentrierte Kontrollebene. Sie wurde für Unternehmen entwickelt, die in großer Zahl externe Identitäten verwalten, und erweitert das Sicherheitskonzept von der einmaligen Überprüfung zum Zeitpunkt der Anmeldung hin zu einem kontinuierlichen Überwachungsmodell, das das Risiko während des gesamten aktiven Session-Lebenszyklus bewertet.

Herausforderungen bei Kunden:

Für CIAM-Verantwortliche kann jede Millisekunde an Reibungsverlusten zu abgebrochenen Anmeldungen und Umsatzeinbußen führen. Gleichzeitig sehen sich Security-Teams mit einer Zunahme raffinierter Betrugsfälle konfrontiert. Die klassischen „Front-Door"-Sicherheitsmaßnahmen versagen bei Angreifern, die automatisierte Bots einsetzen, um Benutzerwachstumsanalysen mit gefälschten Accounts aufzublähen, oder bei Angreifern, die legitime Sessions kapern, um nach der Authentifizierung eines Benutzers Treuepunkte und sensible Daten abzugreifen. Es war noch nie so schwierig wie heute, eine nahtlose, abschlussstarke User Experience mit der Notwendigkeit in Einklang zu bringen, die Markenreputation zu schützen und großmaßstäblichen Betrug zu verhindern.

Vorteile

- **Vor der Anmeldung (Proactive Bot & Fraud Defense):**
  Blockiert automatisierte Skripte und die Registrierung von „gefälschten Accounts", bevor diese Ihre Datenbank erreichen. Damit wird sichergestellt, dass sich Ihre Wachstumsanalyse auf echte menschliche Kunden bezieht.

- **Während der Anmeldung (Precision Access Verification):**
  Identifiziert und blockiert kompromittierte Anmeldedaten sofort in Echtzeit, um Account-Hacking-Versuche zu neutralisieren, ohne dass es für legitime Benutzer zu Reibungsverlusten kommt.

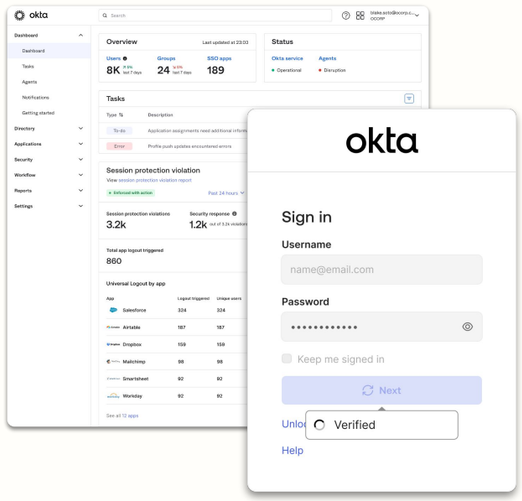
- **Nach der Anmeldung (Continuous Post-Auth Protection):**
  Überwacht die aktive Session auf nicht plausible Ortsveränderungen oder Token-Diebstahl und löst die richtigen Schritte aus, um gekaperte Sessions in allen unterstützten Anwendungen sofort zu beenden.

Installation

Im **Early Access** verfügbar ab **12. Februar 2026**.

OCI ITP-SKU: Erfordert Enterprise- und AMFA-SKUs, deren Menge der üblichen Anzahl monatlich aktiver Enterprise-Benutzer entspricht. Nur für die OIE-Plattform (Okta Identity Engine) verfügbar.

Mehr erfahren



Okta Customer Identity

Allgemein verfügbar

Erweiterte Verzeichnisverwaltung (ehemals Secure Partner Access)

Classic OIE

Funktion von OCI / Verfügbar mit OIG for OCI-SKU || Autorisiert für FedRAMP High/DOD IL4, unterstützt für FedRAMP Moderate

Bieten Sie Ihren Partnern sicheren und nahtlosen Zugriff auf interne Ressourcen bei minimalem IT-Aufwand.

Mehr erfahren

Unterstützung von Universal Logout für OCI-Anwendungen (ehemals CIS)

OIE

Funktion von OCI || Verfügbar für alle SKUs || Autorisiert für FedRAMP Moderate/High/DOD IL4

Null Entwicklungsaufwand für Anwendungsentwickler bei der Integration von Universal Logout in ihre Okta Customer Identity-Anwendungen (ehemals CIS).

Mehr erfahren

Einheitliche Claims-Generierung für per Okta föderierte Anwendungen

OIE

Funktion von OWI/OCI || Verfügbar in allen SKUs || Autorisiert für FedRAMP Moderate/High/DOD IL4

Optimierung der SAML- und OIDC-Integration über eine einzige Schnittstelle. Verwendung von Okta Expressions, um Gruppen-, Profil- und Geräte-Claims in präzise, relevante Payloads zu filtern.

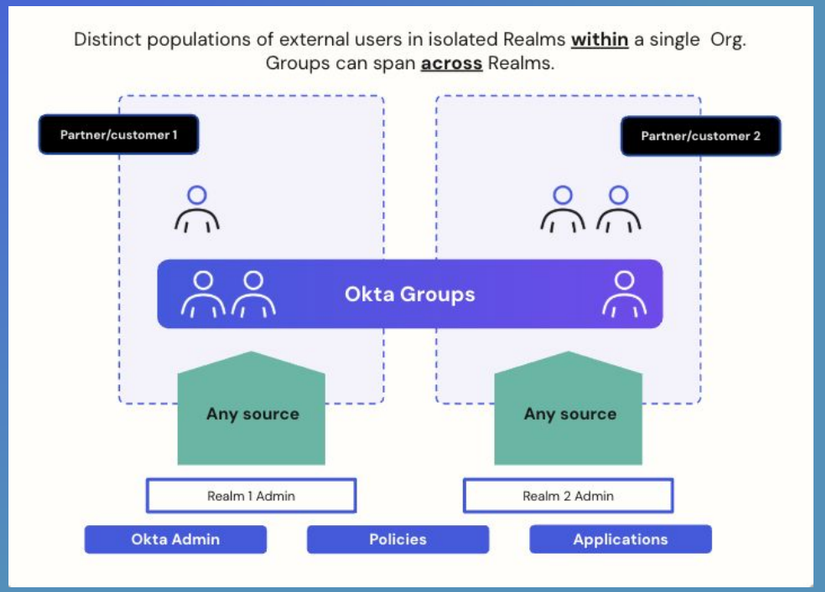
Mehr erfahren

Profilbearbeitungen für deaktivierte Benutzer

Classic OIE

Funktion von OWI/OCI || Verfügbar in Universal Directory-SKU || Autorisiert für FedRAMP High/Moderat/DOD IL4

Aktualisierung von inaktiven Profilen, um Datensätze für langfristige Analysen und reibungslose Kundenretouren aktuell zu halten.



Erweiterte Verzeichnisverwaltung

Mehr erfahren

Okta Customer Identity

Allgemein verfügbar

Export von OIG-Berichten im PDF-Format

Classic OIE

Funktion von OWI/OCI || Verfügbar in OIG || Autorisiert für FedRAMP High/DOD IL4, Unterstützt für FedRAMP Moderate

Einfachere gemeinsame Nutzung von Identity-Einblicken, die über Rohdaten hinausgeht, indem Ergebnisse der Zugangszertifizierung in ein aufbereitetes PDF-Format exportiert werden.

ITP, OIG und Workflows in IL4

Classic OIE

Funktion von OWI/OCI || Verfügbar in OIG || OIG und Workflows sind für IL4 und FRH autorisiert und werden für FRM unterstützt, ITP ist für FRM und FRH autorisiert und wird für IL4 unterstützt

Kunden des US-Verteidigungsministeriums können ITP, OIG und Workflows in IL4-regulierten Zellen (OM1- und zugehörige produktspezifische Zellen) verwenden.

Bidirektionale LDAP-APIs

Classic OIE

Verfügbar in Okta Directory-Integrationen || Autorisiert für FedRAMP Moderate/High

Einfaches Hinzufügen oder Entfernen von Benutzern in lokalen Gruppen auf der Basis von Triggern, die in Okta mit APIs für LDAP festgelegt werden.

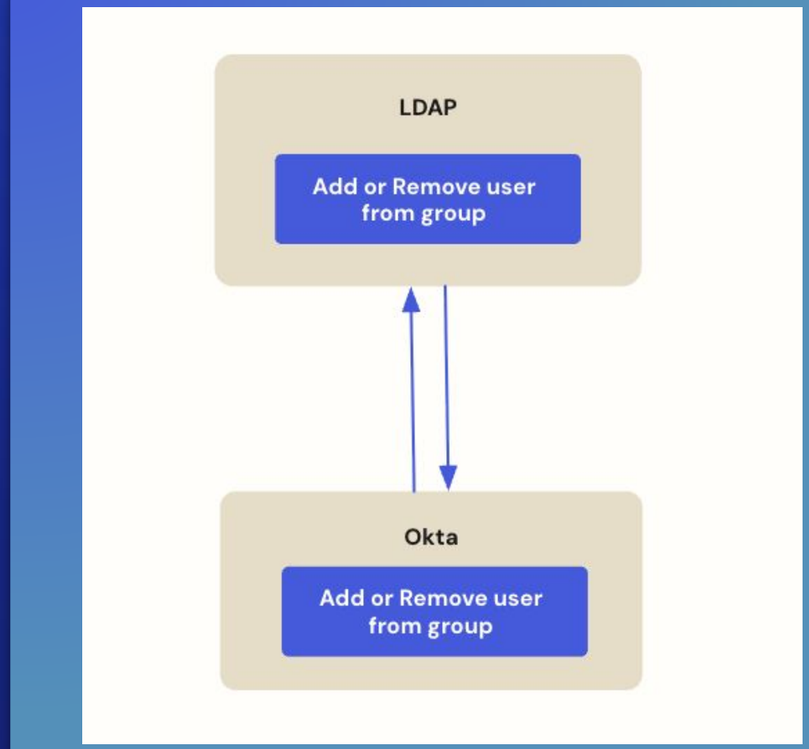
Mehr erfahren

Upgrade von LDAPi auf OIDC

OIE

Verfügbar in UD || Autorisiert für FedRAMP High/Moderate/DOD IL4

Verlagert den LDAPi-Ansatz für Superadministratoren und Manager aus dem Directory Integration- zu einem Anwendungsinstanz-Modell.



Bidirektionale LDAP-APIs

Okta Customer Identity

Allgemein verfügbar

OIDC-Token-Verschlüsselung

Funktion von OWI/OCI || Verfügbar in allen SKUs || Autorisiert für FedRAMP Moderate/High/DOD IL4

Schützt die Übertragung streng vertraulicher personenbezogener Daten an vertrauenswürdige Verbundressourcen und verhindert gleichzeitig das Abfangen durch unbefugte Dritte und böswillige Angreifer.

Mehr erfahren

Classic OIE

Zellerweiterungen – Kanada und Indien

Funktion von OWI/OCI || Verfügbar in allen Tarifen

Dadurch können Kunden ihre Daten lokal in diesen Regionen so hosten, dass sie die Datenresidenzanforderungen erfüllen, die Leistung optimieren und die Einhaltung lokaler Vorschriften verbessern.

Mehr erfahren

Classic OIE

Okta Aerial für Multi-Org-Management

Funktion von Okta Platform || Verfügbar in Sandbox- und Multi-Org Platform-SKU

Zentrales Dashboard auf Account-Ebene, das Transparenz und Managementfunktionen für mehrere Okta Orgs innerhalb eines einzelnen Kunden-Accounts bietet.

Mehr erfahren

Classic OIE

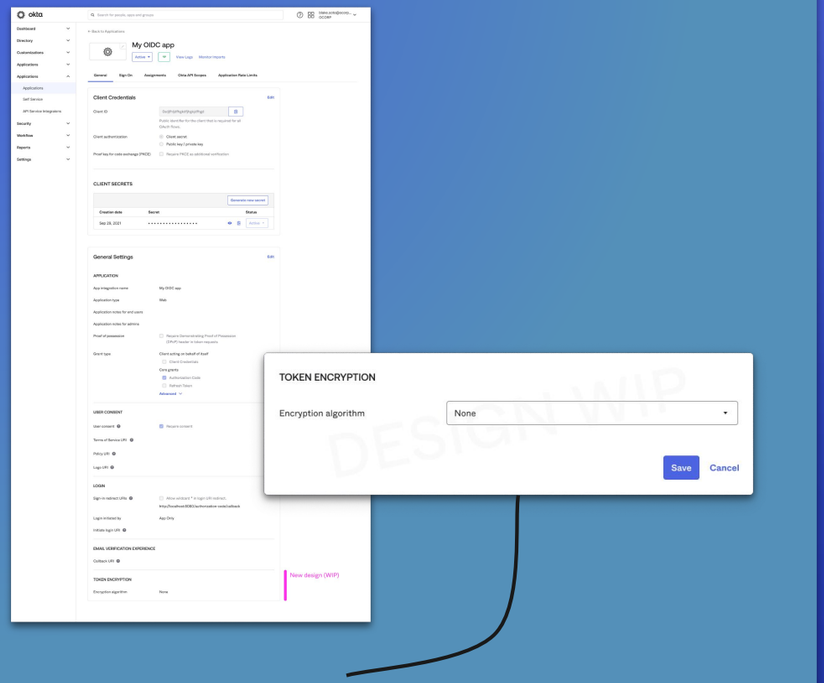
Unterstützung von Okta Account Management-Richtlinien für Passwort-Ablauf

Funktion von OWI/OCI || Verfügbar in allen SKUs || Autorisiert für FedRAMP Moderate/High/DOD IL4

Ermöglicht die bessere Kontrolle über die Sicherheitsanforderungen, wenn das Passwort des Endbenutzers abläuft oder kompromittiert wird.

Mehr erfahren

OIE



OIDC-Token-Verschlüsselung

Okta Customer Identity

Allgemein verfügbar

OEL für Passwortkomplexität (ehemals Höhere Sicherheit für Anmeldedaten)

OIE

Funktion von OWI/OCI || Verfügbar für alle SKUs || Autorisiert für FedRAMP Moderate/High/DOD IL4

Verstärkung des Passwortschutzes und verwandter Schutzmaßnahmen durch eine zusätzliche Sicherheitsebene und Support der Kunden auf ihrem Weg zu passwortlosen Lösungen.

Mehr erfahren

Gerätebedingungen in OAMP

OIE

Funktion von OWI/OCI || Verfügbar in allen SKUs || Unterstützt für FedRAMP Moderate/High/DOD IL4

Verwendung von gerätebasierten Bedingungen, um sicherzustellen, dass Self-Service-Wiederherstellungen und Sicherheitsupdates nur von vertrauenswürdigen Geräten eines Benutzers aus zugänglich sind. Baut eine leistungsstarke Sicherheitsebene ein, die vor raffinierten Phishing- und Social-Engineering-Angriffen schützt.

Mehr erfahren

Erweiterte dynamische Netzwerkzonen: Residential Proxies

Classic

OIE

Funktion von OWI/OCI || Verfügbar in AMFA-SKU || Unterstützt für FedRAMP Moderate/High/DOD IL4

Schutz Ihres Kundenportals vor raffinierten Bedrohungen, indem Datenverkehr von Residential Proxies, VPNs und Anonymisierungsdiensten blockiert wird. Bietet granulare Kontrollen zum Stoppen von Botnets und Angreifern, die legitime Kundenstandorte imitieren, um die Sicherheitsmaßnahmen zu umgehen.

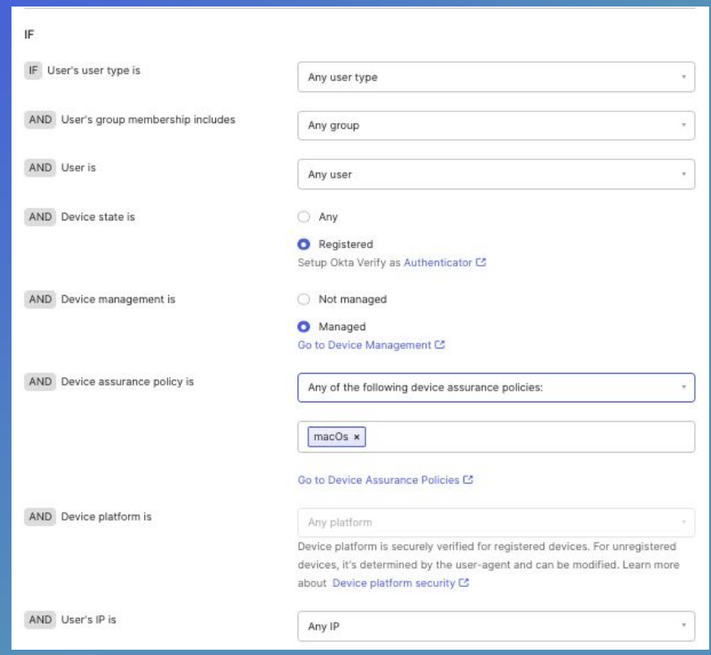
Netzwerkbeschränkungen für Token Endpoint

OIE

Funktion von OWI/OCI || Verfügbar für alle SKUs || Autorisiert für FedRAMP Moderate/High/DOD IL4

Definition einer Netzwerkzone für jeden Client (per Allow-Liste), um Token-Anfragen auf bestimmte IP-Adressen oder -Bereiche zu beschränken und damit die Sicherheit der Token Endpoints zu erhöhen.

Mehr erfahren



Gerätebedingungen in OAMP

Okta Customer Identity

Allgemein verfügbar

Unterstützung für hochsichere Zertifikate von Zertifizierungsstellen

Funktion von OWI/OCI || Verfügbar für alle SKUs || Autorisiert für FedRAMP Moderate/High/DOD IL4

Erweitert Support für Zertifikate, die in Custom Domains-Abläufen verwendet werden, auf ein Höchstmaß an Sicherheit (SHA-384 und SHA-512).

Mehr erfahren

OIE

Native Passkey-Unterstützung

Funktion von OWI/OCI || Verfügbar in MFA/AMFA-SKU || Unterstützt für FedRAMP Moderate

Ermöglicht sichere und benutzerfreundliche Experiences dank nahtloser Passkey-Authentifizierung direkt in nativen Mobilgeräte-Apps, sodass kein Webbrowser notwendig ist.

Mehr erfahren

OIE

OAuth für E-Mail-Anbieter

Funktion von OWI/OCI || Verfügbar in allen SKUs

Absicherung Ihres Kundenkommunikationskanals, indem die Standardauthentifizierung durch OAuth für eigene SMTP-Integrationen ersetzt wird.

Mehr erfahren

OIE

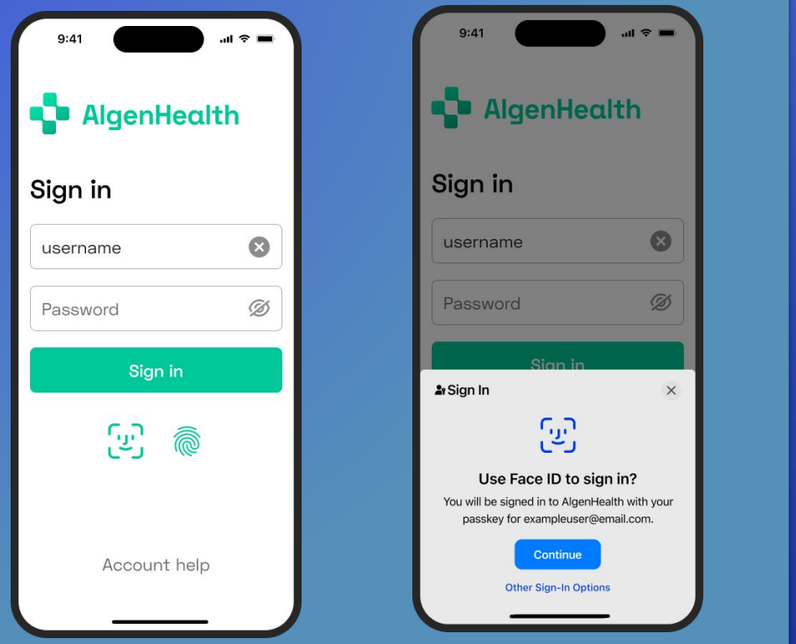
Benutzerdefinierte Administratorberechtigungen für Zugriffsrichtlinien

Funktion von OWI/OCI || Verfügbar in SKU || Autorisiert für FedRAMP Moderate/High/DOD IL4

Ermöglicht Konsistenz und granulare Kontrolle über Authentifizierungs-, Session- und Account Management-Richtlinien.

Mehr erfahren

OIE



Native Passkey-Unterstützung

Okta Customer Identity

Allgemein verfügbar

Zusätzliche biografische Attribute für die ID-Verifizierung

Funktion von OWI/OCI || Verfügbar für alle SKUs || Autorisiert für FedRAMP Moderate/High/DOD IL4

Ermöglicht das Hinzufügen weiterer biografischer Attribute während der Zuordnung verifizierbarer Claims im Rahmen der Identitätsprüfung, z. B. Geburtsdatum, E-Mail-Adresse, Telefonnummer.

Mehr erfahren

OIE

Support des SHA256-Digests in SAML-AuthN-Anfragen

Funktion von OWI/OCI || Verfügbar für alle SKUs || Autorisiert für FedRAMP Moderate/High/DOD IL4

Aktualisiert die SAML-Implementierung von Okta, um den sicheren SHA-256-Digest-Algorithmus anstelle des veralteten SHA-1- zu verwenden.

Mehr erfahren

OIE

Neue Workflows-Konnektoren

Funktion von Workflows || Verfügbar in allen Workflows-SKUs

Integration mit mehr Okta-APIs und gängigen Anwendungen (Checkpoint, LucidChart, Okta OIG, Snowflake, Tenable, Trend Micro) zur Verwaltung von Benutzern und Gruppen.

Mehr erfahren

Classic

OIE

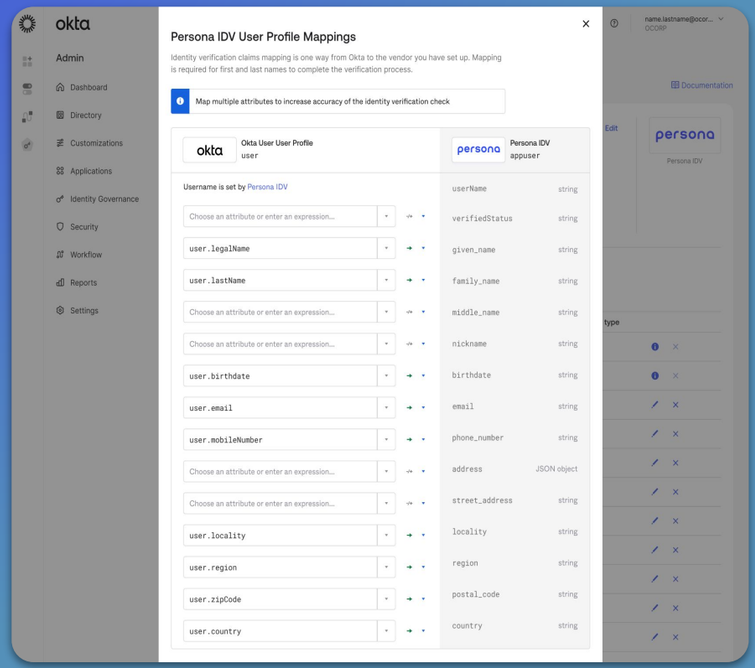
Neue Integrationen für Provisionierung/Berechtigungen

Funktion von Workflows || Verfügbar in Okta Platform || Autorisiert für FedRAMP Moderate/High/DOD IL4

Integriert sich mit weiteren HR-Systemen und gängigen Anwendungen zur Verwaltung von Benutzern, Gruppen und Berechtigungen, darunter CrowdStrike, LucidChart, Netskope, Oracle IAM, SAP Analytics, SAP Concur, Trend Micro und Mimecast.

Classic

OIE



Zusätzliche biografische Attribute für die ID-Verifizierung

Okta Customer Identity

Allgemein verfügbar

Benutzerdefinierte AAGUID

Funktion von OWI/OCI || Verfügbar in MFA/AMFA-SKU || Unterstützt für FedRAMP Moderate/High/DOD IL4

Beschränkt die Authentifikator-Registrierung durch Endbenutzer ausschließlich auf zulässige Authentifikatoren und Passwortmanager.

Mehr erfahren

OIE

Erneute Authentifizierung bei Identity-Anbietern

Funktion von OWI/OCI || Verfügbar in allen SKUs

Optimierung der plattformübergreifenden Customer Journey, indem aktuelle Anmeldungen beim Quell-Identity-Anbieter durchgesetzt werden. Eliminiert „Session Lag“ und stellt damit sicher, dass hochriskante Aktionen durch eine Echtzeit-Authentifizierungsprüfung und nicht durch eine veraltete Hintergrund-Session geschützt werden.

OIE

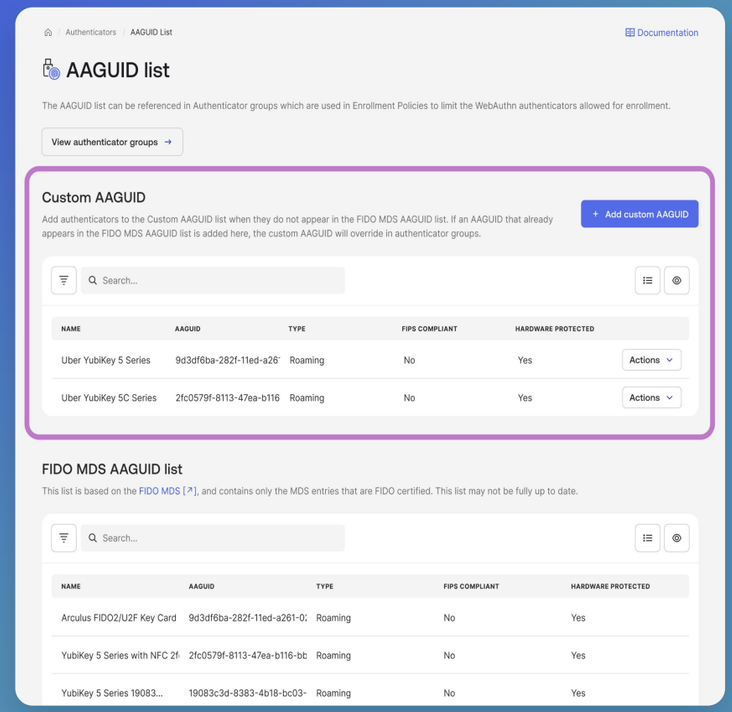
Globale Suche – Enthält

Funktion von OWI/OCI || Verfügbar in allen SKUs

Hilft Administratoren, gesuchte Elemente über die globale Suchleiste schneller zu finden. Administratoren können nach Benutzern mit einem bestimmten Domain-Namen oder einer teilweisen Übereinstimmung eines Gruppennamens suchen, um die Notwendigkeit zu reduzieren, in der erweiterte Suche produktübergreifend zu navigieren.

Classic

OIE



Benutzerdefinierte AAGUID

Okta Customer Identity

Early Access

Launch der ITP OCI-SKU

Funktion von OCI || Verfügbar in ITP OCI-SKU || Autorisiert für FedRAMP Moderate/High, unterstützt für DOD IL4

Kontinuierlicher Schutz vor Identity-Bedrohungen durch Bewertung des Benutzer-, Geräte- und Kontextrisikos vor, während und nach der Authentifizierung.

Mehr erfahren

OIE

Verbesserter Schutz vor kompromittierten Anmeldedaten

Funktion von OCI || Verfügbar in ITP OCI-SKU

Optimierung Ihrer Reaktion auf kompromittierte Anmeldedaten, ohne aktive Kunden zu beeinträchtigen.

Classic

OIE

Native-to-Web-SSO

Funktion von OCI || Verfügbar in allen SKUs || Unterstützt für FedRAMP Moderate/High/DOD IL4

Eliminiert wiederholte Anmeldungen und verbessert die Zufriedenheit und Bindung von Benutzern sowie Interaktionen. Vereinfacht die Entwicklung und reduziert die Authentifizierungskomplexität sowohl für B2C- als auch für B2B-Anwendungsfälle.

Mehr erfahren

OIE

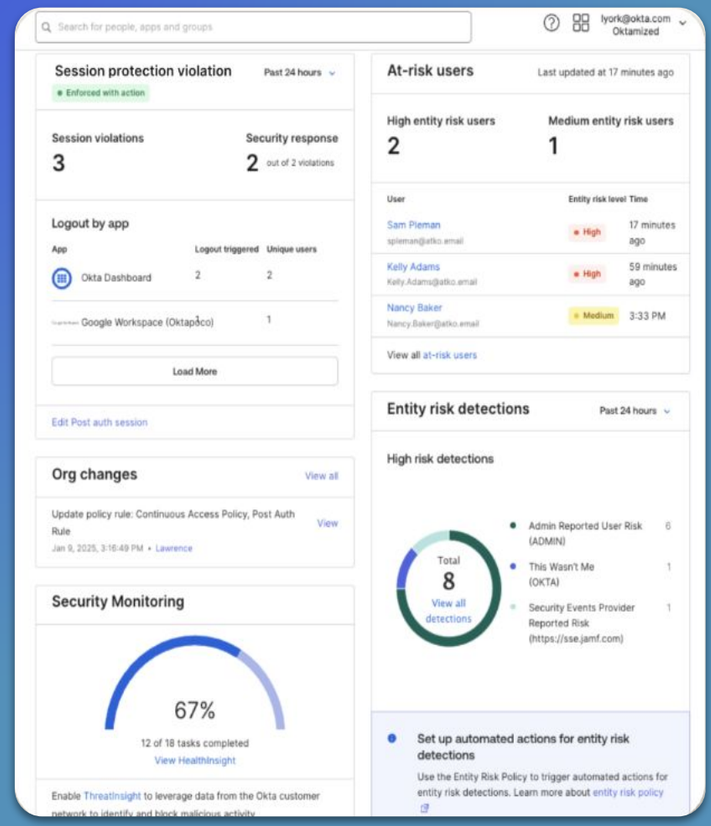
Self-Service-Failover – Erweiterte Disaster Recovery

Funktion von Okta || Verfügbar in Enhanced Disaster Recovery-SKU

Ermöglicht es Kunden, auf eine Backup-Region oder die primäre Region für ihre eigenen Okta Orgs zurückzugreifen – alles über ein Self-Service-Portal oder per API. Ermöglicht auch das Testen von Fallback- und Restore-Funktionen im Rahmen Ihrer eigenen Geschäftsprozesse.

Classic

OIE



ITP für OCI

Okta Customer Identity

Early Access

SKU für Workflows Dedicated Infrastructure Add-on

Classic

OIE

Funktion von Workflows || Verfügbar in Plattform: Workforce Identity Workflows Dedicated Infrastructure Add-On; Plattform: Customer Identity Workflows Dedicated Infrastructure Add-On

Unterstützt leistungsstärkere Anwendungsfälle mit höherer Zuverlässigkeit, insbesondere im Bereich des Niedriglatenzmodus und der Nutzung von Inline-Hooks, sowie ein höheres Volumen an Anfragen durch gelockerte Systemgrenzen.

OAG-Offline-Zugriff

Classic

OIE

Funktion von OWI/OCI || Verfügbar in Okta Access Gateway || Unterstützt für FedRAMP Moderate/High/DOD IL4

Wenn Okta Access Gateway (OAG) die Verbindung zu Okta verliert, können Benutzer weiterhin auf lokale Anwendungen zugreifen.

Einblicke zu Richtlinien

OIE

Funktion von OWI/OCI || Verfügbar in MFA/AMFA-SKU || Autorisiert für FedRAMP Moderate/High/DOD IL4

Ermöglicht Administratoren sichere Richtlinienänderungen dank verbesserter Transparenz, gestaffelter Aktualisierungen und einfacher Rollbacks.

Mehr erfahren

RBAC-Ordnerrollen

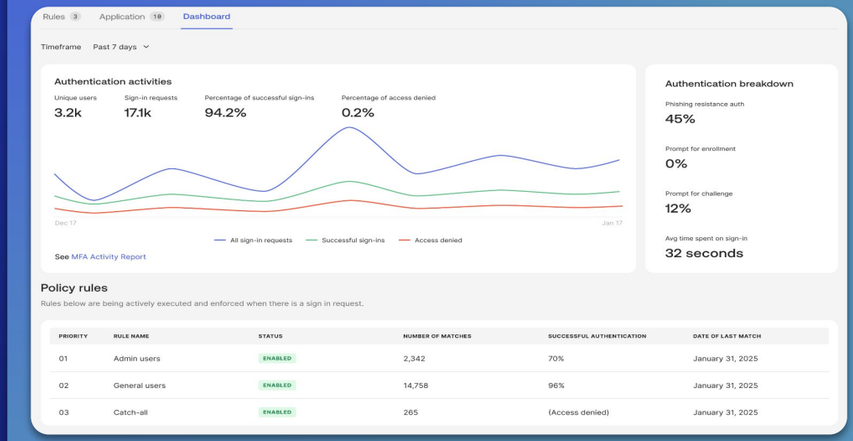
Classic

OIE

Funktion von Workflows || Autorisiert für FedRAMP High/DOD IL4, unterstützt für FedRAMP Moderate

Gewährt Benutzern Zugriff auf einzelne Ordner, in denen sie nur bestimmte Abläufe, Tabellen und Verbindungen verwenden und verwalten können. Ermöglicht es Kunden, die Nutzung von Workflows auch Benutzern zu erlauben, die nicht zum IT-Team gehören.

Mehr erfahren



Einblicke zu Richtlinien

Okta Customer Identity

Early Access

Erkenntnisse zu Authentifikator-Rollouts

Funktion von OWI/OCI || Verfügbar in MFA/AMFA-SKU || Unterstützt für FedRAMP Moderate/High/DOD IL4

Mit dieser Erweiterung des Berichts zu Authentifizierungsaktivitäten sieht der Administrator genau, wie Faktoren genutzt werden – nach Anmeldemethode, Verwaltungsstatus und Registrierungsstatus aufgeschlüsselt.

Mehr erfahren

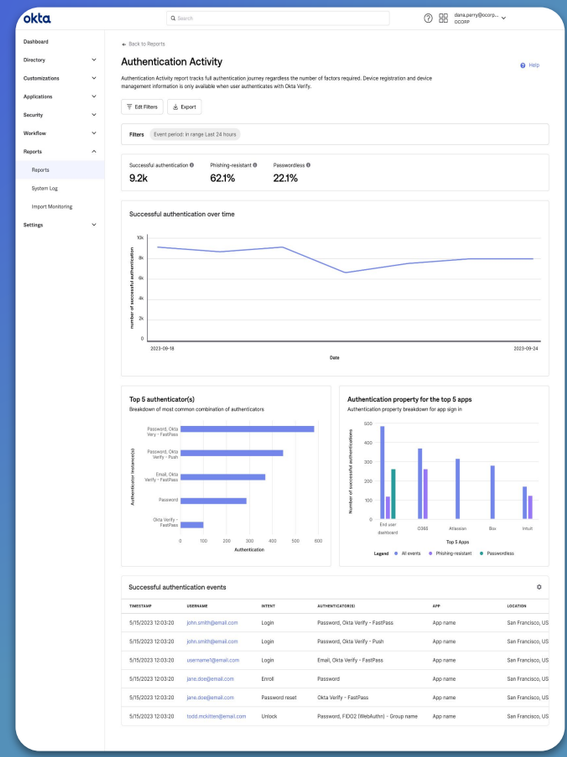
OIE

WebAuthn-Rebranding + Anmeldung mit Passkey

Funktion von OWI/OCI || Verfügbar in allen SKUs || Unterstützt für FedRAMP Moderate/High/DOD IL4

Eine vereinfachte, standardisierte Authentifizierungs-Experience, die den Kunden mehr Kontrolle über den Passkey-Prozess ermöglicht.

OIE



Erkenntnisse zu Authentifikator-Rollouts

okta