okta

Überblick über die Produkt-Releases

Early Access und allgemeine Verfügbarkeit im 2. Quartal 2025 (April bis Juni 2025)

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 Effizienz-steigerungen 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 hier genannten Produkte, Funktionen, Zertifizierungen 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.

okta

Weitere Informationen zu den neuesten Innovationen und geplanten Features von Okta

Webseite: Überblick über die Produkt-Releases

Hier lernen Sie die wichtigsten Innovationen kennen, die wir in der Launch Week vorgestellt haben, und finden weiterführende Materialien.

Hier können Sie unser Vertriebsteam kontaktieren.

Webinar zur Okta-Produkt-Roadmap

Eine kurze Vorschau auf kommende Produkt-Releases.

Hier können Sie sich für das Webinar zur Okta-Produkt-Roadmap registrieren.

Videos zu Release-Highlights und Release-Hinweise

Sie erhalten einen kompakten und informativen Überblick über die neuesten Updates, Funktionen und Erweiterungen. Hier finden Sie die Highlights.

Hier finden Sie Release-Hinweise.

https://pages.okta.com/2025-06-WBN-LaunchWeekOkta-LP.html

okta

Willkommen bei der Release-Übersicht der Okta Platform

2. Quartal 2025

Angesichts einer wachsenden Identity-Angriffsfläche durch immer mehr Geräte, KI-Agenten und verteilte Umgebungen ist der Schutz jeder Identität wichtiger als je zuvor.

In diesem Quartal führen wir neue Funktionen ein, mit denen Sie diese Komplexität in den Griff bekommen. Die Innovationen in Okta Workforce Identity bieten diese Möglichkeiten:

- Stärkung der Gerätesicherheit in Ihrem gesamten Ökosystem
- Überwachung und Verwaltung des vollständigen Lebenszyklus nicht-menschlicher Identities

Diese Neuerungen unterstützen einen proaktiven Identity-zentrierten Sicherheitsansatz.

okta

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

Okta Workforce Identity stärkt Ihre Sicherheitslage mit automatisierten Zugriffsentscheidungen und einheitlichen Richtlinien, die den manuellen Aufwand für Ihr Team reduzieren und die IT-Abläufe vereinfachen.

Die Releases dieses Quartals führen stärkere Governance- und Sicherheitskontrollen für Ihre wichtigsten Assets ein: Geräte, Benutzer (einschließlich KI-Agenten) und privilegierte Ressourcen.

Spotlights

Okta Workforce Identity

- Sicherheit vor, während und nach der Authentifizierung
- Active Directory-Accounts
- Identity Threat Protection mit Okta AI-Verbesserungen
- Cross App Access (for AI Agents)
- Compliance-Roadmap-Neuerungen von Okta für den öffentlichen Sektor (USA)

Alle Funktionen

- Identity Security Posture Management (ISPM)
- Zugriffsmanagement
- Identity-Management
- Identity Governance
- Privileged Access
- Platform Services
- Premier Success Plans
- Okta Learning

Entwicklerressourcen

Die Okta Platform erweckt den Identity-Security-Fabric zum Leben

Secure Identity-Produkte

Governance
- Okta Identity Governance

Posture Management
- Identity Security Posture Management

Okta Privileged Management
- Okta Privileged Access

Zugriffsmanagement
- Universal Directory
- Single Sign-On
- Adaptive MFA
- API Access Management
- Okta Access Gateway
- Customer Identity

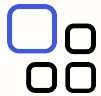
Okta Device Access
- Okta Device Access

Identity Threat Protection
- Identity Threat Protection mit Okta AI

Secure Identity-Orchestrierung

Secure Identity-Integrationen

Infrastruktur
IaaS  On-Premise-Server

Anwendungen
Cloud-Anwendungen  On-Premise-Anwendungen

APIs
Öffentlich  Privat

Identities
Directories  Nicht-menschliche/KI-Agenten

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

okta

Spotlight: Sicherheit vor, während und nach der Authentifizierung

Active Directory-Accounts

- Nutzung Ihres vorhandenen Okta-AD-Agenten für die Suche nach privilegierten Accounts
- Schutz der AD-Accounts mit Zugriffsrichtlinien und automatischer Rotation von Anmeldedaten

Verbesserung beim Identity Security Posture Management

- Visualisierung von Multi-Tenant-Zugriffsbeziehungen und MFA-Lücken übergreifend über Okta-Instanzen hinweg
- Identifizierung von MFA-Umgehungen und Richtlinienlücken in Ihrem Identity-Ökosystem

Identity Threat Protection mit Okta AI-Verbesserungen

- Verbesserte Sicherheit von Administrator-Accounts
- Vereinheitlichung der Echtzeit-Bedrohungserkennung und -abwehr in Ihrer Umgebung

okta

Early Access

Spotlight: Active Directory-Accounts

Verwaltung von Active Directory-Accounts

Was ist das?

Dank dieser Funktion können Sie sich mit Ihrem vorhandenen Okta-AD-Agenten mit Active Directory-Umgebungen verbinden, nach privilegierten AD-Accounts suchen und deren Passwörter verwalten, robuste Zugriffsrichtlinien erstellen und sämtliche Administrator- und Benutzeraktivitäten überprüfen.

Herausforderungen bei Kunden:

Privilegierte Active Directory-Accounts werden meist nicht verwaltet und sind sehr anfällig für Angriffe.

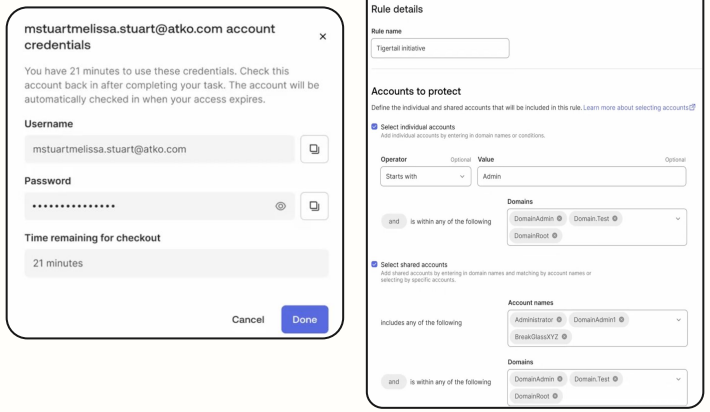
Vorteile

Active Directory-Accounts müssen vor nicht autorisierten Benutzern geschützt werden, um die Einhaltung der Compliance-Vorschriften zu gewährleisten und die Sicherheit zu stärken. Gängige Best Practices besagen, dass privilegierte Accounts per Vault sowie durch regelmäßige Passwort-Rotationen geschützt sein müssen und dass Sicherheitsverantwortliche einen Überblick darüber haben sollen, wer auf bestimmte Ressourcen zugreifen kann.

Installation

In Okta Privileged Access weltweit verfügbar. Sprechen Sie mit Ihrem CSM oder AE, um die Funktion für Ihre Umgebung zu aktivieren.

Erfahren Sie mehr im Blog.



Spotlight: Identity Threat Protection mit Okta AI-Verbesserungen

Erweiterter Überblick über Bedrohungen und Automatisierung von Echtzeit-Aktionen in Ihrer Umgebung

Was ist das?

Benutzerdefinierte Admin-Rollen für ITP: Durchsetzung von Least-Privilege-Zugriff, indem Sie für die Verwaltung von ITP-Konfigurationen Admin-Berechtigungen zuweisen

ITP-Erkennungen für Super-Admin-Rollen*: Überwachung und Erkennung von ungewöhnlichem Verhalten bei Super-Admins, um Account-Hacking aufzudecken

SSF-Integration mit Palo Alto Networks: Korrelation von Identity-Informationen mit Erkenntnissen von xDR-Plattformen wie Palo Alto Network, sodass die Erkennung verbessert, Silos beseitigt und koordinierte Maßnahmen in Ihrem gesamten Ökosystem möglich werden

SSF-Transmitter: Verwendung von Okta-Identity-Informationen für automatisierte Aktionen (z. B. Session-Widerruf, MFA-Abfragen) in externen Tools wie Apple Business Manager, um Incident Response-Workflows erheblich zu beschleunigen

*Jetzt für Adaptive MFA-Kunden verfügbar

Vorteile

Diese Verbesserungen erlauben stärkere Kontrolle über Admin-Berechtigungen, einen genaueren Überblick über Admin-Account-Risiken sowie Möglichkeiten zur schnelleren und proaktiveren Reaktion auf Bedrohungen in Ihrer Umgebung.

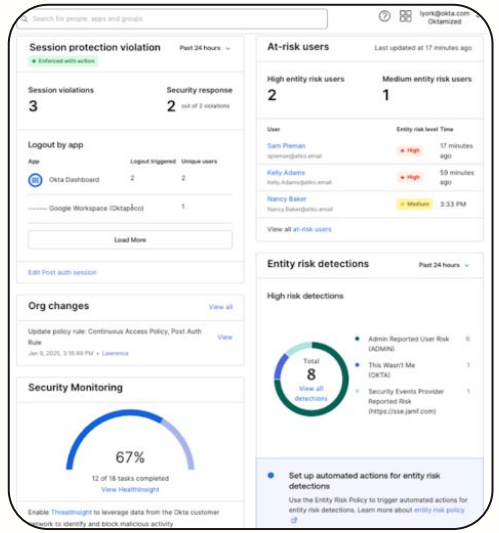
Herausforderungen bei Kunden:

Unternehmen haben häufig Schwierigkeiten, Least-Privilege-Sicherheit für Administratoren durchzusetzen. Das führt dazu, dass kritische Konfigurationen durch Rollen mit übermäßigen Berechtigungen gefährdet sind. Gleichzeitig erhöht ein begrenzter Überblick über Super-Admin-Aktivitäten das Risiko von Account-Hacking. Ohne integrierte Identity-Indikatoren und automatisierte Reaktionsmöglichkeiten bleibt die Bedrohungserkennung und -abwehr fragmentiert und langsam und verschlechtert die allgemeine Sicherheitslage.

Installation

- Benutzerdefinierte Admin-Rollen für ITP, SSF-Integration für Palo Alto Networks und SSF-Transmitter sind in der **ITP-SKU** enthalten.
- ITP-Erkennungen für Super-Admin-Rollen sind in der **Adaptive MFA-SKU** enthalten.

Mehr erfahren



Spotlight: Cross App Access (for AI Agents)

Absicherung der unsichtbaren Integrationsebene zwischen Anwendungen und KI-Agenten, damit ISVs können sofort mit der Entwicklung beginnen können; verfügbar als Okta-Funktion für ausgewählte Kunden ab dem 3. Quartal 2026

Was ist das?

Cross App Access for AI Agents ist ein Protokoll für vertrauenswürdige Verbindungen zwischen Anwendungen und KI-Agenten. Es überträgt Kontrolle und Consent an den IT-Administrator, der entscheiden kann, mit welchen Anwendungen Verbindungen zulässig sind, und einen Überblick darüber hat, worauf zugegriffen wird.

Herausforderungen bei Kunden:

KI-Agenten agieren unabhängig und ohne das Einholen von Berechtigungen, um Aufgaben durchzuführen, Entscheidungen zu treffen und sich mit anderen Systemen zu verbinden. KI-Agenten schaffen eine unsichtbare systemübergreifende Ebene mit privilegierten Zugriffen. Dies stellt ein neues und dringliches Sicherheitsrisiko dar, bei dem klassische Identity-Tools machtlos sind.

Vorteile für ISVs

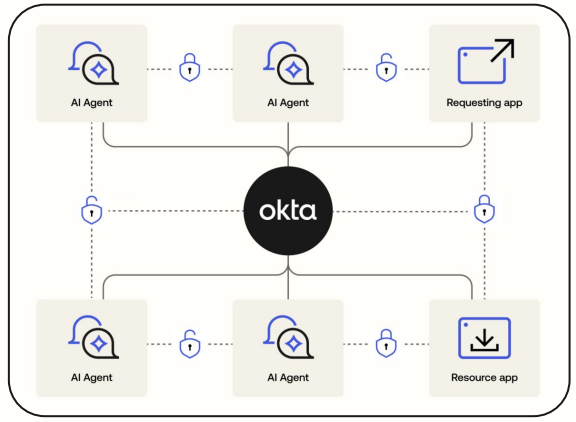
Für die Absicherung von KI-Agenten ist ein Ökosystem aus Entwicklern, Identity-Plattformen und Unternehmen notwendig, die Hand in Hand zusammenarbeiten. ISVs spielen dabei eine entscheidende Rolle.

KI-Agenten werden immer zahlreicher, bieten mehr Möglichkeiten und agieren systemübergreifend im Auftrag von Benutzern. Gleichzeitig wachsen jedoch auch die damit verbundenen Sicherheitslücken. Deshalb bietet Okta Cross App Access moderne Transparenzfunktionen, mit denen ISVs eine skalierbare und sichere Kontrolle darüber erhalten, wie autonome Agenten und Anwendungen kommunizieren. Auf diese Weise können B2B-SaaS-Ersteller die Anforderungen ihrer Unternehmenskunden erfüllen und Innovationen auf sichere Weise implementieren.

Mehr erfahren

ISVs können sofort mit der Entwicklung beginnen. Early Access für Kunden ab 3. Quartal 2026.

- Mehr erfahren
- **Teilnahme an unserem digitalen Event „Identity Summit: Securing Agentic AI“** (Mehr erfahren)



okta

Spotlight: Compliance-Roadmap-Neuerungen von Okta für den öffentlichen Sektor (USA)

Was ist das?

Die umfangreiche Okta-Plattform stellt neue autorisierte und Audit-fähige Identity-Lösungen für den öffentlichen Sektor in den USA bereit. Mit unseren integrierten Lösungen Identity-Governance, Workflows und Threat Protection mit Okta AI können Behörden ihre Abläufe modernisieren und profitieren gleichzeitig von größerer Unterstützung beim Identity-Management.

Herausforderungen bei Kunden:

- Erreichen messbarer Modernisierungs- und Effizienzziele bei Einhaltung strenger Compliance-Vorschriften
- Minimierung von Risiken auf oder unter akzeptable Grenzwerte
- Bewältigung von Ressourcenbeschränkungen und Fachkräftemangel

Vorteile

- Die Okta-Lösung stellt eine einheitliche Plattform dar, die Echtzeit-Cybersicherheit gewährleistet und die Produktivität der Belegschaft steigert.
- Organisationen im öffentlichen Sektor können mögliche Bedrohungen dank angepasster Identity-Flows, stets aktueller Informationen zu Zugriffsmustern und hervorragender Transparenz proaktiv identifizieren und beheben, Prozesse optimieren sowie messbare Kosteneinsparungen erreichen.

Installation

- Blog zur Ankündigung
- Support-Seite zur Produktbewertung
- Dieselben Produkt-SKU mit den folgenden Erweiterungen
  - Okta for Government Moderate
  - Okta for Government High
  - Okta for US Military

okta

Okta Workforce Identity-Releases

Okta Workforce Identity verbindet alle Ihre Identities – Benutzer, Geräte und KI-Agenten – in einem zentralen Security-Fabric.

Unsere neuesten Funktionen erweitern diesen Fabric und helfen Ihnen, Ihre privilegierten AD-Accounts abzusichern, Aktionen Ihrer Sicherheitstechnologien zur Reaktion auf Bedrohungen zu automatisieren und Least Privilege für Administratoren durchzusetzen.

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.

okta

Identity Security Posture Management (ISPM)

Allgemein verfügbar

Nicht-menschliche Identities – Transparenz und Risikoanalyse

Feature von Identity Security Posture Management (ISPM)

Security-Teams profitieren von der erforderlichen Transparenz zum Schutz vor Kompromittierungen nicht-menschlicher Identities: Erkennung und Meldung der riskantesten Service-Accounts, von menschlichen Benutzern, die Anmeldedaten nicht-menschlicher Identities verwenden, und von nicht rotierten Schlüsseln und Token.

Classic OIE

Konfigurationsfehler bei SFDC-KI-Agenten

Feature von Identity Security Posture Management (ISPM)

Erkennung riskanter Konfigurationsfehler bei SFDC-KI-Agenten einschließlich übermäßig privilegierter Zugriffsrechte und schwacher Authentifizierungsverfahren, die nicht autorisierte Datenzugriffe oder die Ausnutzung von KI-Agenten ermöglichen können.

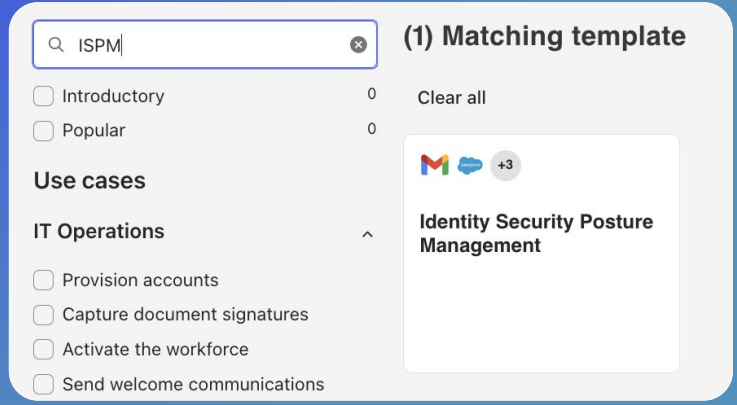
Classic OIE

Okta Workflows-Templates für automatische Behebung

Feature von Identity Security Posture Management (ISPM)

Bietet Kunden die Möglichkeit, mit wenigen Klicks automatische Behebungsaktionen auszulösen. ISPM bietet nun einen offiziellen Workflow, der Behebungsschritte wie Account-Sperrung, Passwortrücksetzungen und MFA-Durchsetzung oder -Registrierung auslöst.

Classic OIE



Okta Workflows-Templates für automatische Behebung

okta

Identity Security Posture Management (ISPM)

Early Access

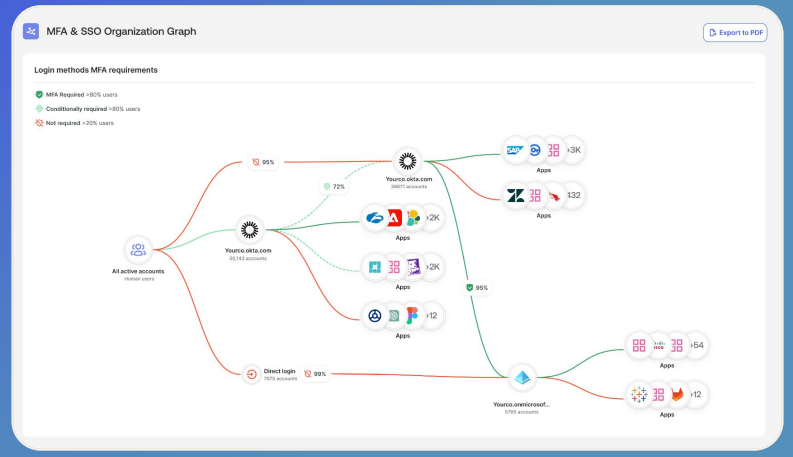
MFA- und SSO-Analysen – Dashboard und Diagramm

Feature von Identity Security Posture Management (ISPM)

Detaillierte Analyse von MFA, Faktoren und SSO in einem exportierbaren Dashboard, das Sie beim Identifizieren der wichtigsten Trends und Risiken unterstützt.

Classic

OIE



MFA- und SSO-Analysen – Dashboard und Diagramm

Zugriffsmanagement

Allgemein verfügbar

AMR-Claims-Zuordnung (Authentication Method Reference)

Verfügbar in Multi-Factor Authentication || Autorisiert für FedRAMP Moderate/High/DOD IL4

Da MFA für alle Administrator-Accounts erforderlich ist, können Org-to-Org-Administratoren mithilfe von AMR-Claims die User Experience verbessern und gleichzeitig zuverlässige Sicherheit gewährleisten. Mehr erfahren

OIE

Claims-Austausch zwischen Okta Orgs

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

Erweiterung des Identitätsverbunds durch sicheren und nahtlosen Zugriff auf Ressourcen über Okta Orgs hinweg. Mehr erfahren

Classic

OIE

Claims-Austausch zwischen Okta und externen Identity-Anbietern

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

Erweiterung des Identitätsverbunds durch sicheren und nahtlosen Zugriff auf Ressourcen über Okta und externe Identity-Anbieter hinweg, ohne die Sicherheit zu kompromittieren. Mehr erfahren: SAML | OIDC

Classic

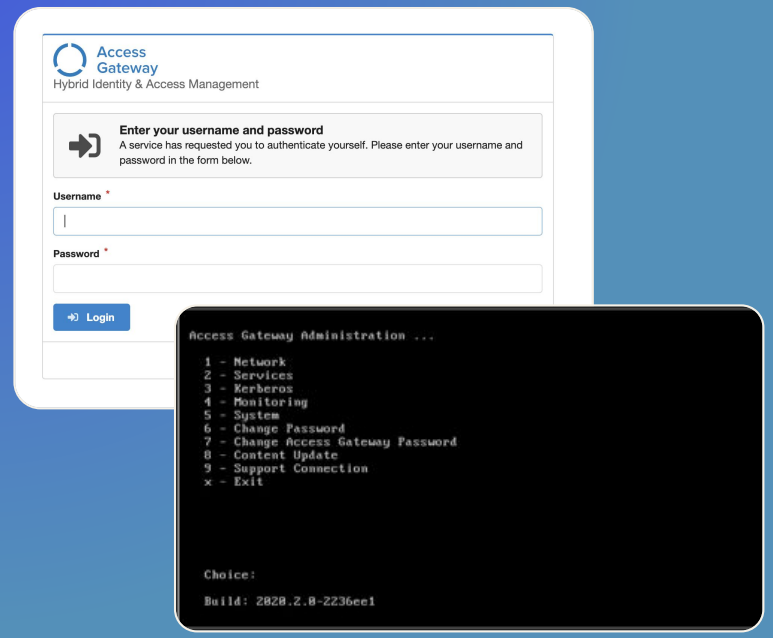
OIE

Änderungen im Zuge der OAG-Initiative „Secure by Design“

Verfügbar in Okta Access Gateway || Unterstützt für FedRAMP Moderate/High/DOD IL4

Standardmäßig ist der Zugriff auf die OAG-Administratorkonsole nur im lokalen Netzwerk möglich und erfordert eine Passwortänderung für die Administratorkonsole und die Befehlszeilenschnittstelle der Administratorverwaltung. Diese Änderungen dienen zur Umsetzung der Okta-Initiative „Secure by Design“.

OIE



Änderungen im Zuge der OAG-Initiative „Secure by Design“

okta

Zugriffsmanagement

Allgemein verfügbar

Desktop-Wiederherstellung mit MFA für macOS

Verfügbar in Okta Okta Device Access || Autorisiert für FedRAMP Moderate/High/DOD IL4

Sorgen Sie für kontinuierliche Produktivität, indem Sie Administratoren die Möglichkeit geben, Endbenutzer mit zeitlich begrenzten Wiederherstellungscodes für die Anmeldung an ihrem Gerät auszustatten, falls ein Smartphone oder Sicherheitsschlüssel abhanden gekommen ist. Mehr erfahren

OIE

Berechtigungen für SAML-Assertions und Token-Claims

Verfügbar in Okta Identity Governance (OIG) || Unterstützt für DOD IL4

Administratoren können jetzt benutzerdefinierte Claims in SAML-Assertion-Attributen und OpenID Connect-Token konfigurieren, Least Privilege durchsetzen und die Abhängigkeit von Gruppen verringern. Mehr erfahren

Classic

OIE

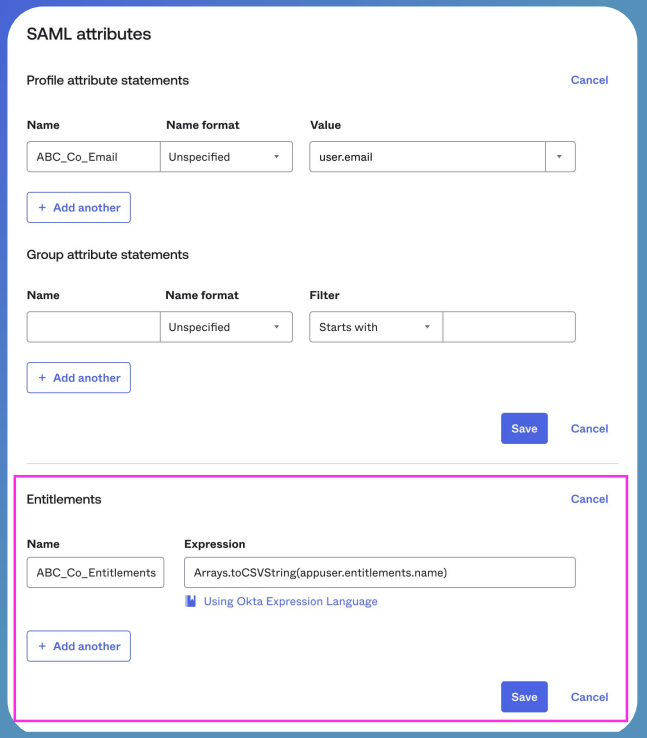
Detaillierte Admin-Berechtigungen für Identity-Anbieter

Verfügbar in Okta Identity Engine (OIE) || Autorisiert für FedRAMP Moderate/High/DOD IL4

Administratoren können jetzt über granulare Administratorberechtigungen spezifische Identity-Anbieter anderen Administratoren zuweisen. Das verbessert die Sicherheitslage, da nur autorisierte Benutzer Zugriff auf die Identity-Anbieter-Konfiguration erhalten.

Classic

OIE



Berechtigungen für SAML-Assertions und Token-Claims

Zugriffsmanagement

Allgemein verfügbar

Richtlinienaktualisierungen als geschützte Aktionen

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

Wenn Registrierungsrichtlinien für Anwendungen, globale Anmelderichtlinien, ITP-Richtlinien und Account-Management-Richtlinien in der Admin-Konsole aktualisiert werden, muss der Administrator eine Step-up-Authentifizierung durchlaufen. Das hindert Angreifer am Vornehmen von Änderungen, wenn sie Zugriff auf eine Administrator-Session haben.

Classic OIE

Registrierung auf dem gleichen Gerät in Okta Verify

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

Ermöglicht verbesserte Prozesse zur Endbenutzer-Registrierung für Okta Verify und FastPass auf Desktop- und Mobilgeräten.

Classic OIE

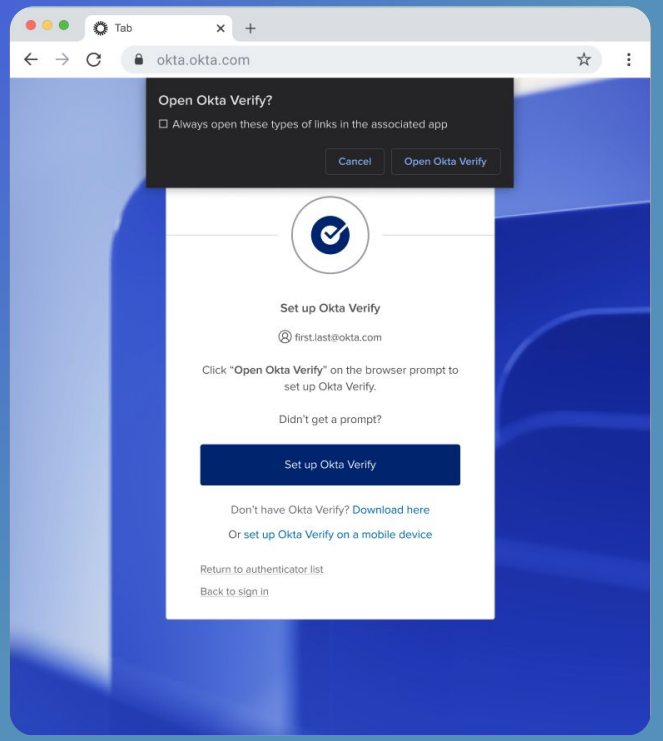
Okta Verify-Problembehebung für iOS

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

Erlaubt Benutzern, Probleme mit Push-Benachrichtigungen und FastPass innerhalb der Okta Verify-App zu beheben.

Mehr erfahren

Classic OIE



Registrierung auf dem gleichen Gerät in Okta Verify

Zugriffsmanagement

Early Access

Erweiterte Compliance-Prüfungen

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

Android Device Trust für Device Assurance

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

Durchsetzung umfangreicher zusätzlicher Geräteprüfungen unter Android im Rahmen der Device Assurance-Richtlinie.

Mehr erfahren

OIE

Erweiterung von appID Context für OIDC- und SAML-Anwendungen

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

Übergibt während der von Okta initiierten Föderation (SAML/OIDC) Informationen über Anwendungen (ID, Name) an externe Identity-Anbieter, um fundiertere Sicherheits- und Richtlinienentscheidungen beim Identity-Anbieter zu ermöglichen.

Classic

OIE

Schutz vor kompromittierten Anmeldedaten (Phase 2)

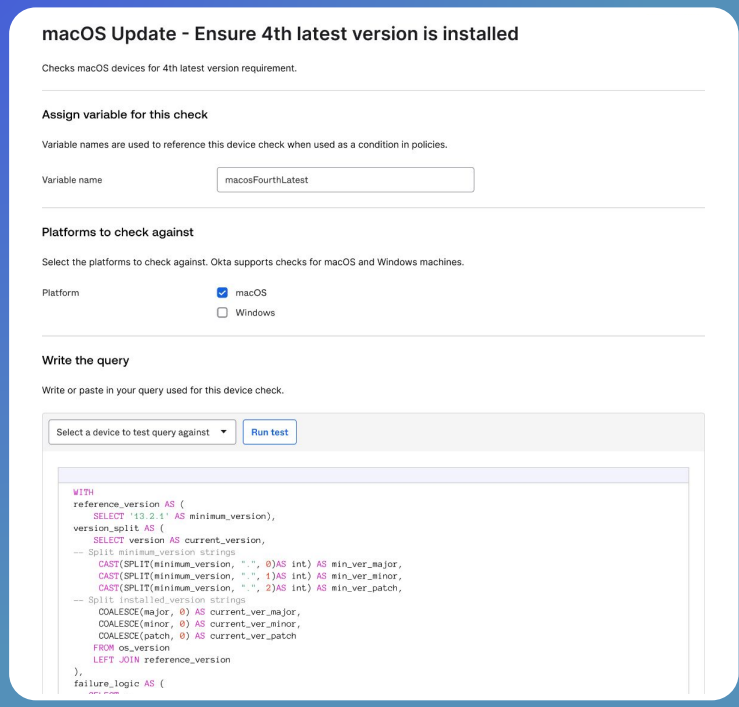
Verfügbar in allen SKUs

Anpassbare Reaktionsmaßnahmen für Ereignisse mit kompromittierten Anmeldedaten, wobei Administratoren die Prozesse bei kompromittierten Anmeldedaten mithilfe eines Test-Accounts überprüfen können.

Mehr erfahren

Classic

OIE



Erweiterte Compliance-Prüfungen

okta

Zugriffsmanagement

Early Access

Benutzerdefinierte FIDO2 AAGUID

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

Ermöglicht das Hinzufügen zulässiger AAGUID-basierter Authentifikatoren (z. B. Browser-Passwortmanager) zu FIDO2 (WebAuthn)-Gruppen.

Classic OIE

Residential Proxy als IP-Service-Kategorie

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

Enhanced Dynamic Zones unterstützt nun Residential Proxies und Blockchain VPNs als IP-Service-Kategorien, sodass Unternehmen den Zugriff vor der Richtlinienbewertung blockieren können.

Mehr erfahren

Classic OIE

ID-Verifizierung mit Namensabgleich

Verfügbar in SSO/MFA ‖ Autorisiert für FedRAMP Moderate/High/DOD IL4

Differenziert bei der verifizierbaren Claims-Zuordnung während der ID-Verifizierung zwischen dem offiziellen Namen und bevorzugten Namen.

Mehr erfahren

OIE

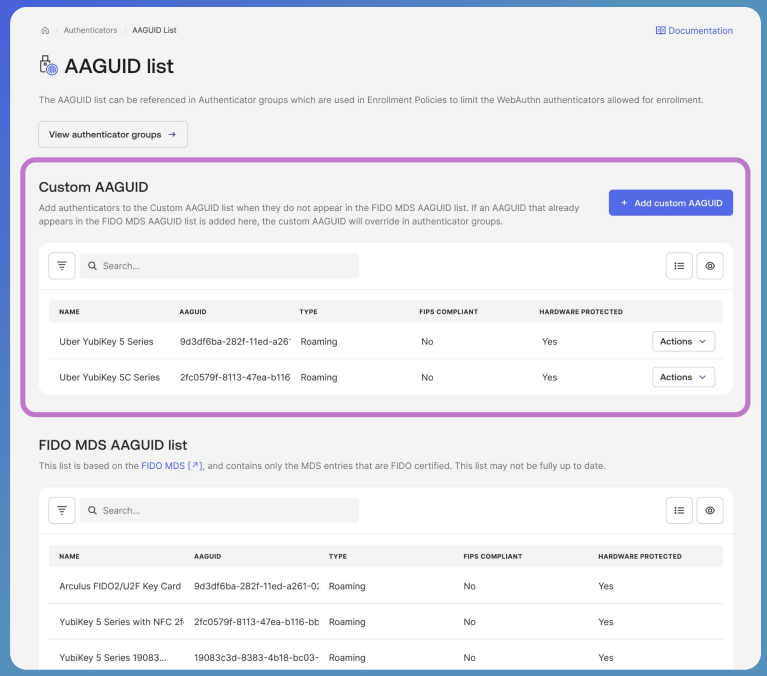
Unterstützung für Microsoft EAM (External Authentication Method)

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

Erlaubt Benutzern die Erfüllung von MFA- und anderen Sicherheitsanforderungen mit Okta, wenn der Zugriff auf Anwendungen erfolgt, die mit Entra ID agesichert sind.

Mehr erfahren

OIE



Benutzerdefinierte AAGUID

okta

Zugriffsmanagement

Early Access

Netzwerkbeschränkungen für Token Endpoint

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

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

OIE

Automatische OAG-Aktualisierung

Verfügbar in Okta Access Gateway || Unterstützt für FedRAMP Moderate/High/DOD IL4

Kunden können nun automatische Aktualisierungen aktivieren, damit ihre OAG-Bereitstellungen stets die neueste Version ausführen. Mehr erfahren

OIE

Überlappende Identity-Anbieter-Signaturzertifikate

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

Unterstützung mehrerer aktiver Signaturzertifikate pro Identity-Anbieter für nahtlose Zertifikatrotation, um Ausfallzeiten sowie Betriebsaufwand zu reduzieren und die Sicherheit zu verbessern. Mehr erfahren

Classic

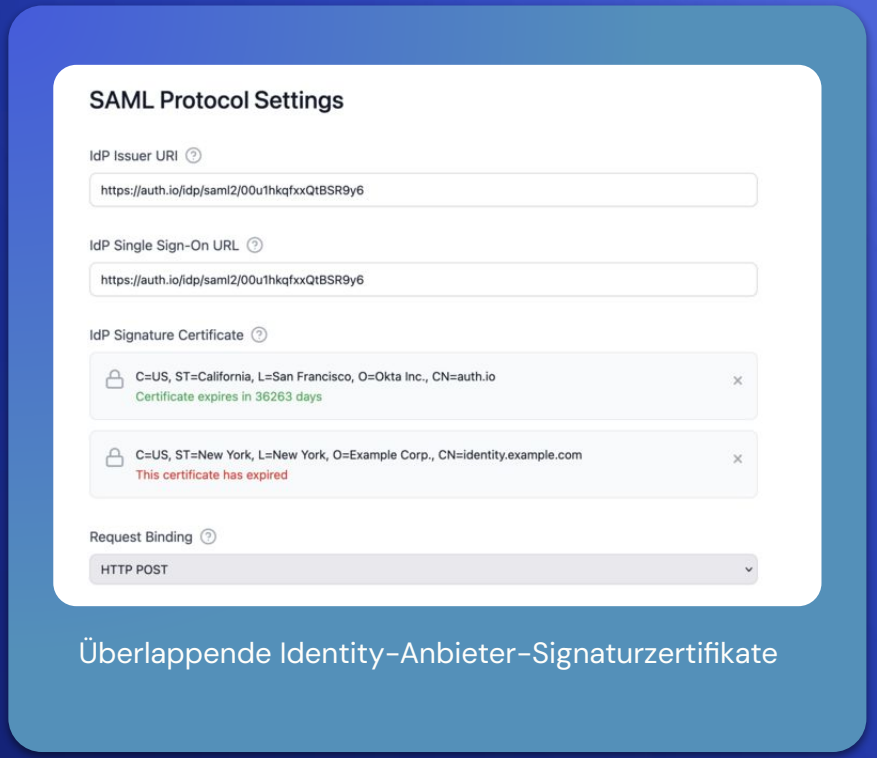
OIE

Unterstützung von Universal Logout für Okta Customer Identity-Anwendungen

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

Einfache Integration von Universal Logout in Ihre Okta Customer Identity-Anwendungen (ehemals CIS) – ohne jeden Entwicklungsaufwand. Mehr erfahren

OIE



Überlappende Identity-Anbieter-Signaturzertifikate

okta

Zugriffsmanagement

Early Access

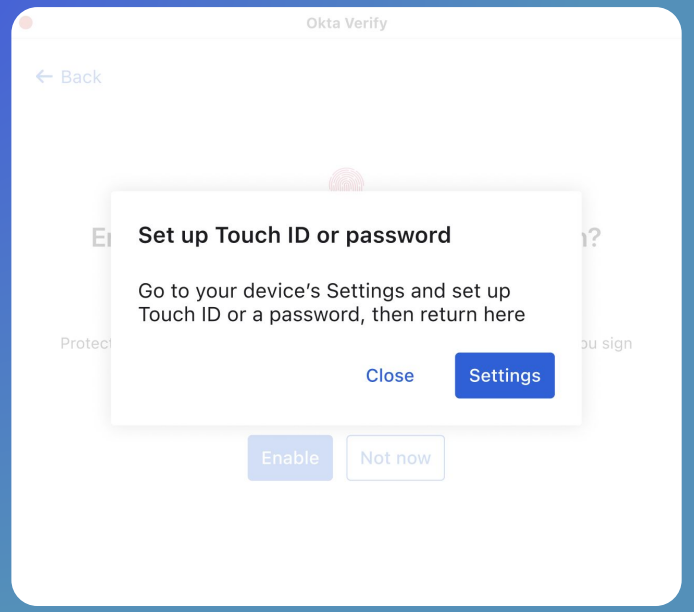
Behebungsempfehlungen für die Benutzerverifizierung

Verfügbar in MFA, AMFA || Autorisiert für FedRAMP Moderate/High/DOD IL4

Empfehlungen für Endbenutzer durch Aktivierung oder Verschärfung der Benutzerverifizierung, um die Anforderungen der Authentifizierungsrichtlinie zu erfüllen.

Classic

OIE



Behebungsempfehlungen für die Benutzerverifizierung

Identity-Management

Allgemein verfügbar

Durchgängige Verschlüsselung für LDAP-Agenten

Verfügbar in Okta Directory Integration || Unterstützt für FedRAMP Moderate/High/DOD IL4

Implementiert eine zusätzliche Sicherheitsebene mit Überwachung der Konfigurationsdatei von LDAP-Agenten sowie Nachrichtenverschlüsselung für jeden Datenaustausch zwischen Okta und dem LDAP-Agenten.

Classic OIE

OIN-Anwendungen für Berechtigungsmanagement – Splunk, Zoho Mail

Verfügbar in Okta Identity Governance (OIG) || Unterstützt für DOD IL4

Erkennung, Import, Speicherung und Verwaltung von Berechtigungen in Okta mithilfe von Paketen, Richtlinien und Regeln mit vorkonfigurierten Integrationen für vier OIN-Anwendungen: Splunk, Zoho Mail, CrowdStrike, Oracle IAM.

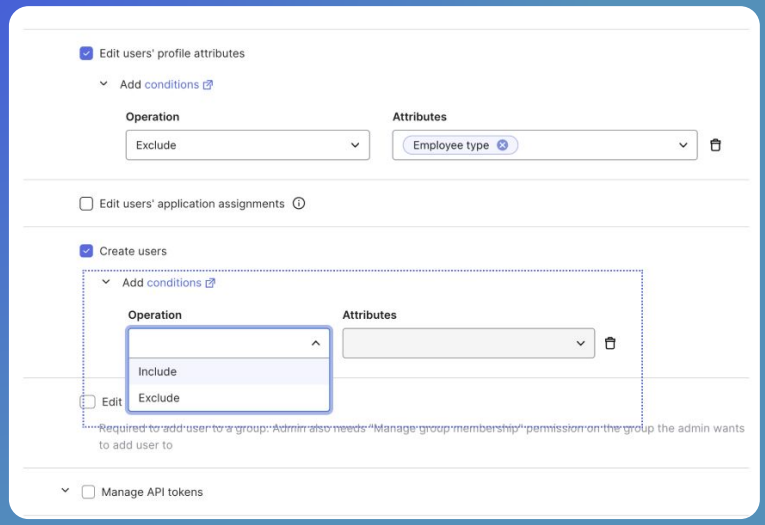
Classic OIE

Berechtigungsbedingungen für die Benutzererstellung

Feature von Custom Admin Roles, Secure Partner Access / Verfügbar in Secure Partner Access || Autorisiert für FedRAMP Moderate/High/DOD IL4

Verhindert, dass delegierte oder Partner-Administratoren vertrauliche Attributwerte (z. B. Rollen oder Abteilungen) zuweisen können, die unbeabsichtigt Zugriff auf kritische Systeme gewähren können. Ermöglicht die Durchsetzung attributbasierter Zugriffskontrollrichtlinien, indem sichergestellt wird, dass nur die richtigen Administratoren Identity-Attribute für die Autorisierung festlegen können. Verringert das Risiko von Konfigurationsfehlern während des Benutzer-Onboardings, insbesondere in Umgebungen mit ausgelagerter Verwaltung.

Classic OIE



Berechtigungsbedingungen für die Benutzererstellung

Identity-Management

Early Access

Inkrementelle Importe mit DirSync

Verfügbar in Okta Directory Integration || Autorisiert für FedRAMP Moderate/High/DOD IL4

Verbesserung der inkrementellen Importe aus Active Directory, was schnellere und effizientere Importe mit weniger Fallbacks zu vollständigen Importen ermöglicht.

Mehr erfahren

Classic OIE

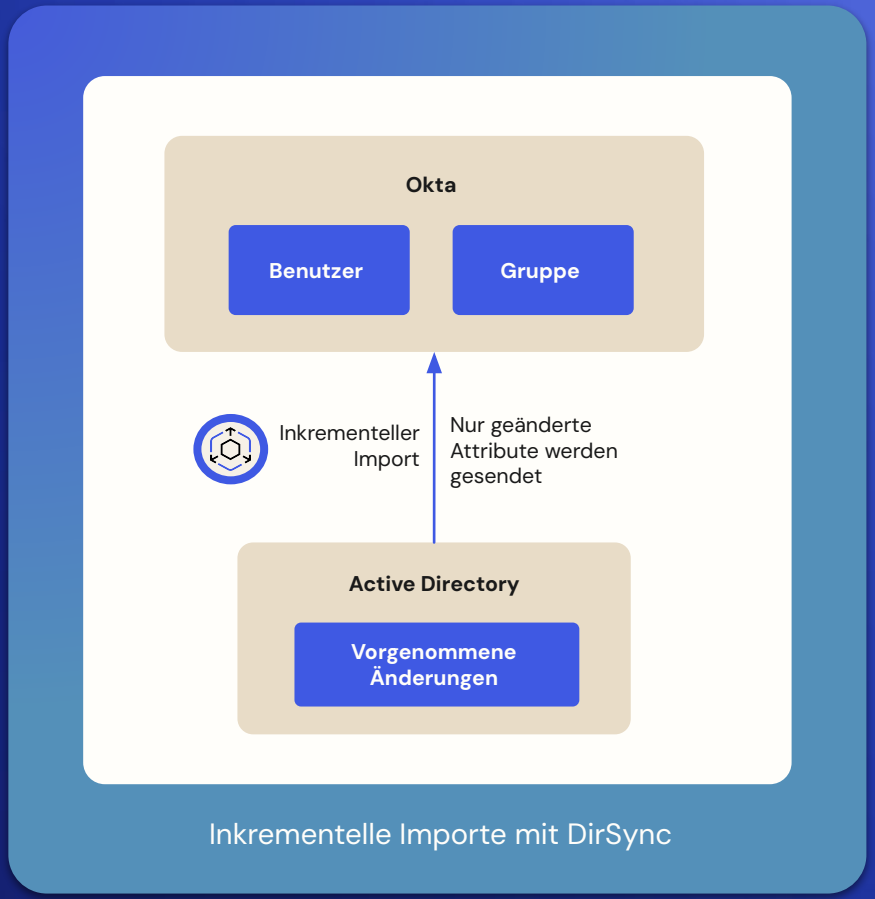
On-prem Connector für Oracle EBS

Verfügbar in Okta Identity Governance (OIG) || Unterstützt für DOD IL4

Vereinfacht die Identity Governance für lokale Anwendungen, indem Legacy-Systeme mit modernen Anwendungsumgebungen überbrückt werden, um verbesserte Sicherheit, nahtlose Automatisierung und Compliance zu ermöglichen.

Mehr erfahren

Classic OIE



Inkrementelle Importe mit DirSync

Identity Governance

Allgemein verfügbar

Verbesserungen bei der Barrierefreiheit und Neugestaltung von Zugriffsanforderungen

Verfügbar in Access Governance ‖ Unterstützt für DOD IL4

Einfachere Navigation dank einer einheitlichen Benutzeroberfläche für First-Party-Anwendungen von Okta. Unterstützt Compliance-Vorschriften für Barrierefreiheit mit neu gestalteten und inklusiven Layouts. Weniger Reibungspunkte durch Einhaltung bekannter Okta-Designmuster.

Mehr erfahren

Classic OIE

Neue LCM- / Okta Identity Governance (OIG)-Integrationen

Verfügbar in allen SKUs / LCM ist autorisiert für FedRAMP Moderate/High/DOD IL4; OIG wird unterstützt für DOD IL4

Integration mit mehr HR-Systemen und gängigen Anwendungen (Splunk), mit denen Benutzer, Gruppen und Berechtigungen verwaltet werden.

Mehr erfahren

Classic OIE

Ressourcensammlungen

Verfügbar in Okta Identity Governance (OIG) – Access Governance ‖ Unterstützt für DOD IL4

Die Bündelung mehrerer Anwendungen und Gruppen ermöglicht die Optimierung des Berechtigungsmanagements, sodass Benutzer die richtigen Zugriffsrechte schnell und effizient erhalten, während die Komplexität der Anfragen und Genehmigungsprozesse minimiert wird.

Mehr erfahren

Classic OIE

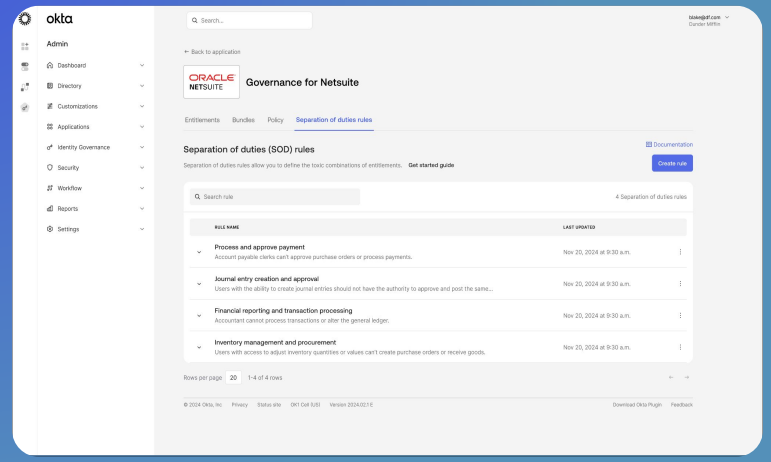
Aufgabentrennung

Verfügbar in Okta Identity Governance (OIG) – Access Governance ‖ Unterstützt für DOD IL4

Erstellung von Regeln, die gefährliche Kombinationen aus Berechtigungen definieren, und Durchführung von Zertifizierungskampagnen, mit denen gefährliche Kombinationen bei Benutzern entfernt werden.

Mehr erfahren

Classic OIE



Aufgabentrennung

okta

Privileged Access

Early Access

Active Directory-Accounts

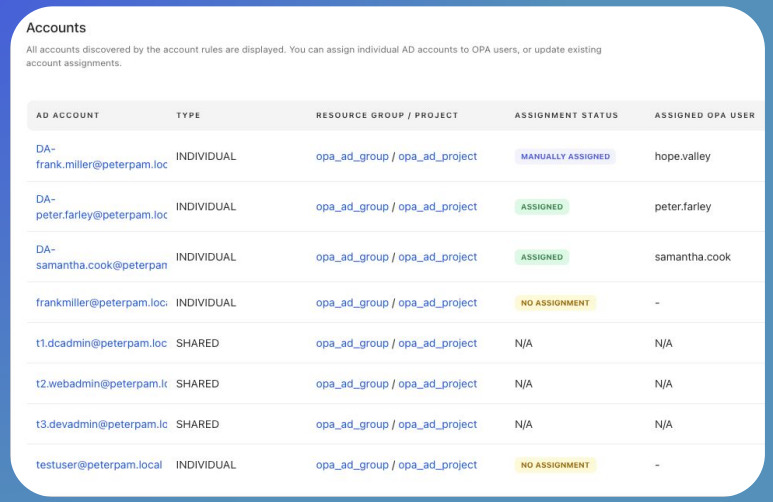
Verfügbar in Okta Privileged Access

Verwaltung der Passwörter für privilegierte Active Directory-Accounts, ohne die operativen Abläufe zu verkomplizieren. Nutzung Ihres bestehenden Okta Active Directory-Agenten zum Identifizieren von AD-Accounts, Erstellen von Zugriffsrichtlinien, Automatisieren von Anmeldedaten-Rotationen und zum Auditieren aller Administrator- und Benutzeraktivitäten.

Mehr erfahren

Classic

OIE



Active Directory-Accounts

Platform Services

Allgemein verfügbar

Barrierefreiheit-ACRs

Classic OIE

Bewertung: VPATS stehen für alle Okta-Umgebungen zur Verfügung, einschließlich FedRAMP Moderate/High/DOD IL4

Überblick über den aktuellen Stand der Barrierefreiheit bei Produkten für Kunden. Nützlich auch zum Einhalten von gesetzlichen und Compliance-Anforderungen insbesondere für FED- und SLED-Kunden.

Mehr erfahren

Dynamische Ressourcen-Sets

Classic OIE

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

Erlaubt Kunden das Beschränken des Zugriffs auf sensible Ressourcen auf einen kleinen Teil der Administratoren.

Mehr erfahren

Neue Workflows-Konnektoren

Classic OIE

Verfügbar in Workflows || Autorisiert für FedRAMP High, Unterstützt für FedRAMP Moderate/DOD IL4

Integration mit mehr Okta-APIs und gängigen Anwendungen (Coupa, Splunk), um Benutzer und Gruppen zu verwalten.

Mehr erfahren

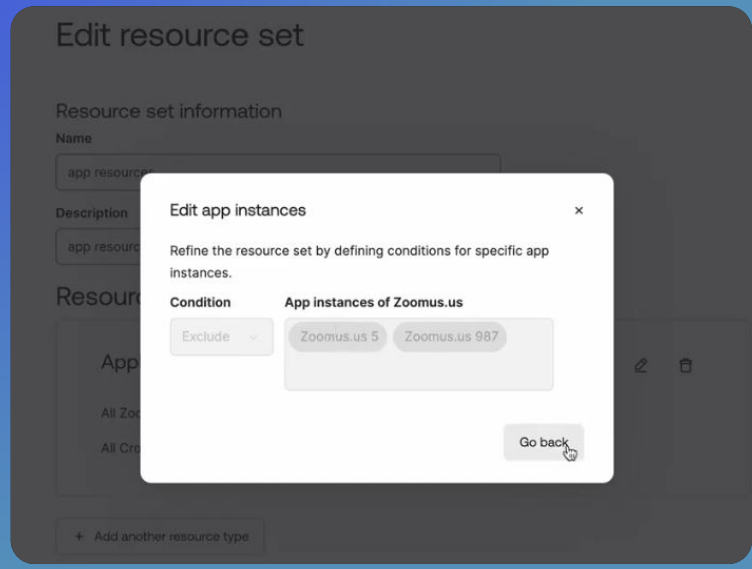
Okta ITP-Konnektor für Workflows

Classic OIE

Verfügbar in Workflows || Autorisiert für FedRAMP High, Unterstützt für FedRAMP Moderate/DOD IL4

Nutzung des Okta ITP-Konnektors zum Debugging oder Auditieren von ITP-Ereignissen und Erstellen oder Ändern von Benutzerrisikostufen.

Mehr erfahren



Dynamische Ressourcen-Sets

okta

Platform Services

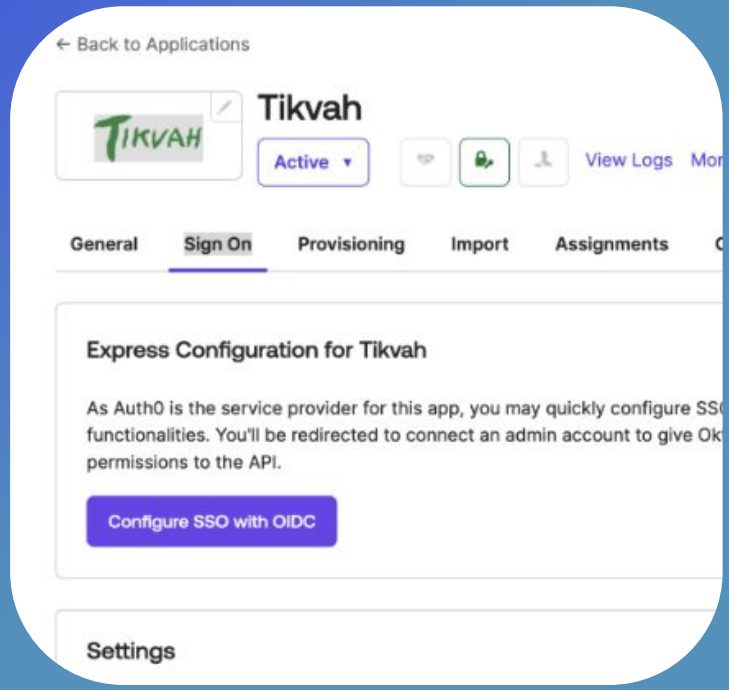
Allgemein verfügbar

Feature des Oktane ISV-Pakets: Express-Konfiguration

Verfügbar in allen SKUs

Mit der Express-Konfiguration können Kunden schnell eine Instanz Auth0-kompatibler OIDC-Anwendungen hinzufügen, die im OIN-Katalog ihrer Okta Org veröffentlicht wurde. Dieser Prozess nutzt den automatischen Datenaustausch zwischen Okta und Auth0.

OIE



Express-Konfiguration

Platform Services

Early Access

Governance für Workflows

Verfügbar in Workflows || Okta Identity Governance (OIG) unterstützt in DOD IL4; Workflows autorisiert für FedRAMP High, unterstützt für FedRAMP Moderate/DOD IL4

Nutzung der Access Requests- und Access Certifications-Rollen und -Ressourcen für Workflows in OIC zur Optimierung von Rollenzuweisungen und Gewährung von zeitgebundenen Zugriffen mit benutzerdefinierten Zugriffsanforderungen.

OIE

ISV-Paket: Activate-Programm

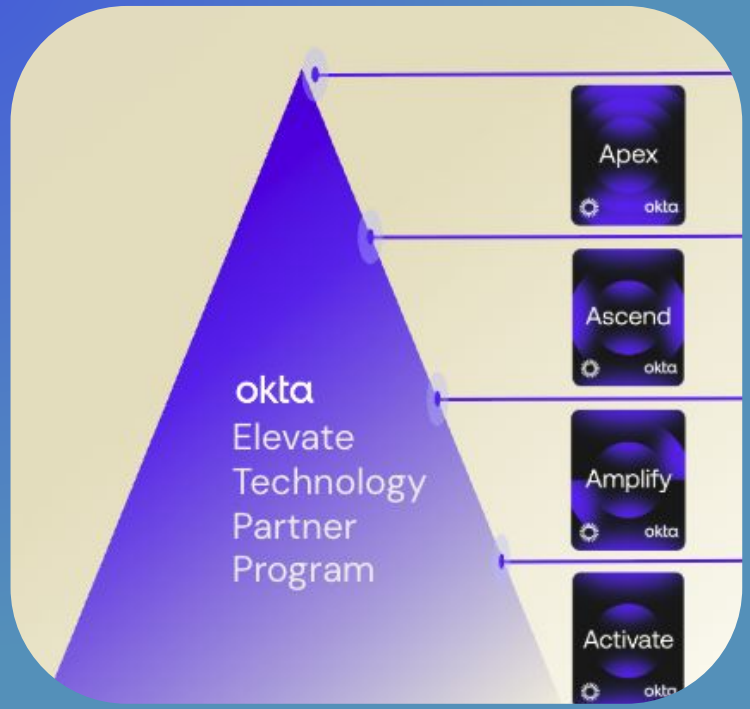
Verfügbar in Okta Platform (Okta Integration Network)

Programm zur einfachen Erstellung, Veröffentlichung und Pflege von SSO- und LCM-Integrationen, mit dem ISVs von Transparenz, Unterstützung bei der Implementierung sowie Self-Service-Marketing-Unterstützung mit Okta profitieren. Mehr erfahren

ISV-Paket: secureintegrations.dev

Verfügbar in allen SKUs

Microsite zum Thema Standards, auf der Entwickler über die genauen Erstellungsprozesse informiert werden, einschließlich aktueller Informationen über bereits ratifizierte IPSIE-Stufen.



Activate-Programm

Premier Success Plans

Allgemein verfügbar

Checkliste für Identity-Reifegrad

Verfügbar in Silver Premier Success Plan

Eine schrittweise Self-Service-Checkliste zur Verbesserung des Identity-Reifegrads basierend auf ausgewählten Geschäftszielen und dem aktuellen Implementierungsstatus, umfasst außerdem zusätzliche Event- und Schulungsressourcen.

Mehr erfahren

OIE

Plan zur Steigerung des Identity-Reifegrads

Verfügbar in Gold Premier Success Plan

Personalisierte Empfehlungen zur Verbesserung des Identity-Reifegrads basierend auf ausgewählten Geschäftszielen und dem aktuellen Implementierungsstatus, umfasst außerdem On-Demand-Aktivierungsmetriken, Zusammenarbeit mit Ihrem CSM, empfohlene Okta-Lernpfade und weitere Schulungsressourcen.

Mehr erfahren

OIE

Expert Learning Pass

Verfügbar in Premier Success Plans der Stufen Silver und Gold

Bietet Zugriff auf einen exklusiven On-Demand-Katalog, Experten-geführte Live-Schulungs-Sessions und Zertifizierungs-Voucher. Silver-Kunden erhalten einen Expert Learning Pass, während Gold-Kunden sechs Expert Learning Passes erhalten.

Mehr erfahren

Classic

OIE

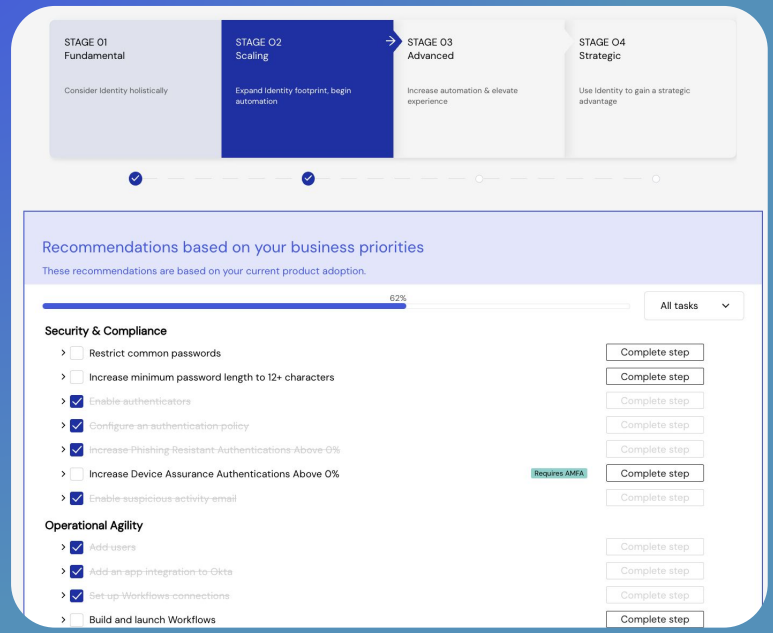
Dedizierter Technical Account Manager

Verfügbar als Add-on für den Gold Premier Success Plan

Ein Technical Advisor mit umfangreichem Wissen über Ihre Produkte und Ihre Architektur, der maßgeschneiderte und langfristige Implementierungs- und Optimierungsstrategien entwickelt.

Classic

OIE



Checkliste für Identity-Reifegrad

Okta Learning

Allgemein verfügbar

Security Series I – NEUE OSIC-Kurse

Classic OIE

Verfügbar im öffentlichen Katalog

Eine falsch konfigurierte Identity ist ein Einfallstor für böswillige Akteure oder nachlässige Insider. Daher ist es wichtig, dass Sie von Anfang an die richtige Identity-Konfiguration nutzen. Dieser Plan zeigt Ihnen die wichtigsten Bereiche, auf die Sie sich konzentrieren sollten, sowie Best Practices im Rahmen des Okta Secure Identity Commitment (OSIC).

Mehr erfahren

Neues Okta Skill Badge – Optimierung von Gerätesicherheit und Verwaltung

OIE

Verfügbar im öffentlichen Katalog

Erfahren Sie, wie Okta sich mit verschiedenen Device Management-Lösungen integriert, um Desktop- und Mobilgeräte abzusichern und zu verwalten. Lernen Sie maßgeschneiderte Sicherheitskonfigurationen und umfassende Bewertungsprozesse kennen, mit denen Sie die Gerätesicherheit verbessern und Management-Aufgaben optimieren können, um einen sicheren und produktiveren Arbeitsplatz zu erreichen.

Mehr erfahren

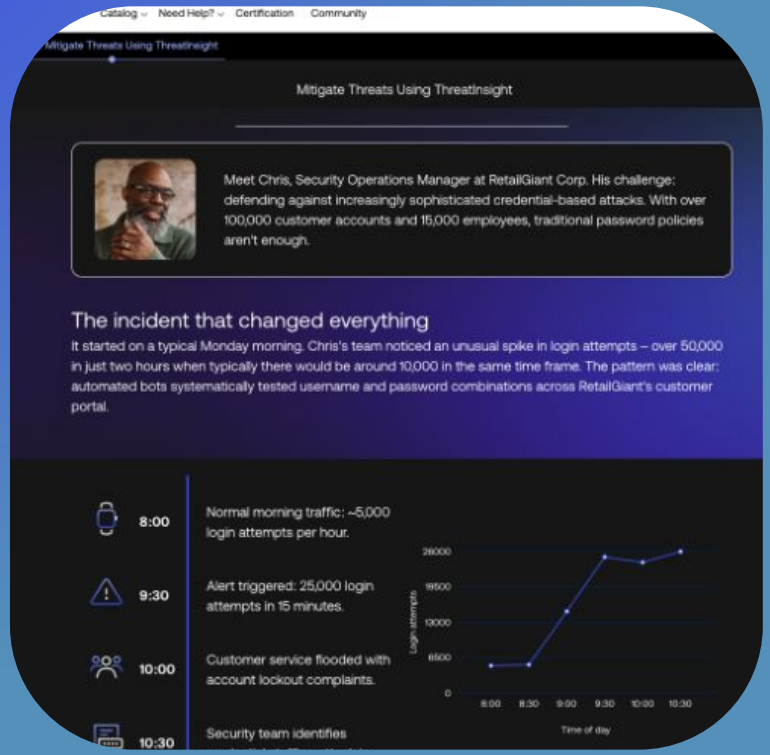
Neues Okta Skill-Badge! Verwaltung von BYOD per Identity-Aware Integration

OIE

Verfügbar im öffentlichen Katalog

Transformieren Sie die Mobilgeräte-Sicherheit Ihres Unternehmens durch die Implementierung von Plattform-spezifischer BYOD-Strategien, die den Identity-orientierten Okta-Ansatz zum Schutz von Unternehmensdaten und Benutzer-Privatsphäre nutzen. Außerdem erhalten Sie nach Abschluss des Lernpfads ein Okta Skill Badge!

Mehr erfahren



NEU: Behebung von Bedrohungen mit ThreatInsight – Security Series I

okta

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

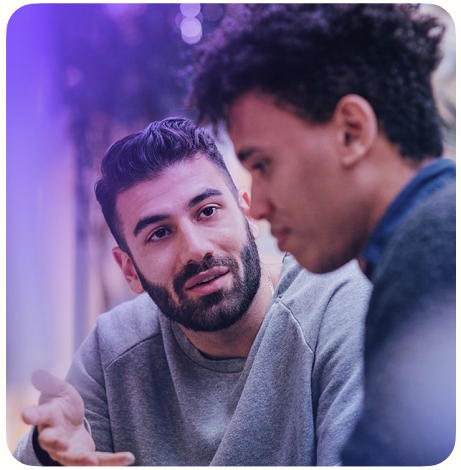
Okta Customer Identity gewährleistet, dass die Sicherheit Ihrer nahtlosen digitalen Experiences an erster Stelle steht. Dadurch erzielen Unternehmen schnelleres Wachstum, bleiben der dynamischen Bedrohungslandschaft einen Schritt voraus und können ihre Kunden und Geschäftsdaten absichern.

Informieren Sie sich über unsere neuesten Releases.

okta

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

okta

Allgemein verfügbar

Spotlight: Okta Customer Identity

Erweiterung des Identity-Security-Fabric für Kunden und Partner

Was ist das?

Okta Customer Identity (OCI) erweitert die vertrauenswürdigen Identity-Sicherheits- und Management-Funktionen, die Sie für Ihre Belegschaft nutzen, auf Ihre externen Benutzer sowie auf Kunden, Partner und Bürger. Diese umfassende Plattform wurde entwickelt, um externe Identities im großen Umfang zu verwalten und abzusichern, nahtlosen und sicheren Zugriff auf Ihre digitalen Anwendungen bereitzustellen und die User Experience zu verbessern.

Herausforderungen bei Kunden:

Viele Unternehmen arbeiten mit fragmentierten Identity-Lösungen für Ihre Belegschaft und externen Benutzer, was zu komplexen Arbeitsprozessen, Sicherheitslücken und inkonsistenten User Experiences führt. Die Verwaltung separater Identity-Systeme für Mitarbeiter, Kunden und Partner führt zu Silos, vergrößert die Angriffsfläche und behindert digitale Transformationsinitiativen.

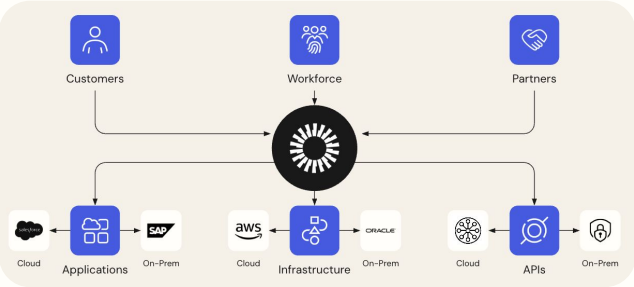
Vorteile

- **Einheitliche Identity-Plattform:** OCI ermöglicht die Konsolidierung des Identity-Managements für die Belegschaft und Kunden auf einer einzigen, einheitlichen Okta Platform. Das minimiert die Komplexität, optimiert die Prozesse und bietet einen vollständigen Überblick über alle Ihre Identities, was die Sicherheit und Compliance verbessert.
- **Verringerte Risiken und verbesserte Sicherheit:** Erweitern Sie Ihren vertrauenswürdigen Okta-Identity-Security-Fabric auf Kunden und Partner – mithilfe zuverlässiger Authentifizierung und Bedrohungserkennung, die Risiken für Ihr digitales Ökosystem minimiert.
- **Verbesserte User Experience und Vertrauen:** Stellt eine einheitliche, sichere und reibungslose Experience für alle Ihre Benutzer bereit – unabhängig davon, ob es sich um Angestellte, Kunden oder Partner handelt. Das schafft Vertrauen, stärkt die Loyalität und fördert die Kundenbindung für Ihre digitalen Services.

Installation

Kontaktieren Sie Ihren Okta-Vertreter oder unser Vertriebsteam, um über konkrete Anforderungen zu sprechen und zu erfahren, wie Ihr Unternehmen von Okta Customer Identity profitieren kann.

Mehr erfahren



okta

Early Access

Spotlight: Schutz vor kompromittierten Anmeldedaten

Proaktiver Schutz vor Credential Stuffing- und Account-Hacking-Angriffen

Was ist das?

Überprüft automatisch Benutzerpasswörter anhand eines kontinuierlich aktualisierten, externen Datensatzes mit nachweislich kompromittierten Anmeldedaten. Mit dieser proaktiven Maßnahme wird festgestellt, ob das Passwort eines Benutzers in einem Data Breach kompromittiert wurde, selbst wenn sich der Vorfall woanders ereignet hat.

Herausforderungen bei Kunden:

In einer Zeit mit häufigen Data Breaches sind Credential Stuffing- und Account-Hacking-Angriffe eine ständige Bedrohung. Unternehmen haben Schwierigkeiten zu erkennen, ob kompromittierte Anmeldedaten ihrer Benutzer im Internet abrufbar sind, sodass sie durch Angreifer gefährdet sind, die mit gestohlenen Anmeldedaten unbefugten Zugriff auf ihre Systeme erlangen können.

Vorteile

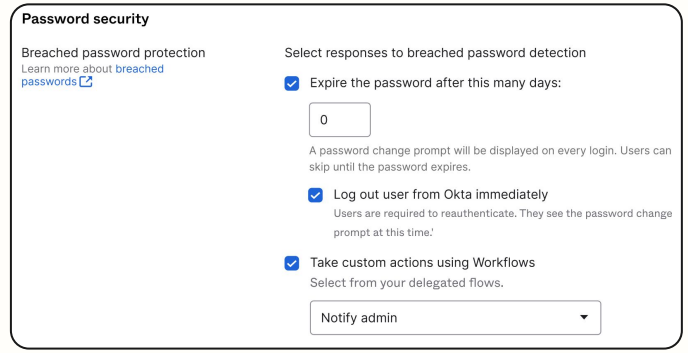
- **Proaktiver Bedrohungsschutz:** Erkennt und behebt automatisch das Risiko von Credential Stuffing- und Account-Hacking-Angriffen durch Identifizieren kompromittierter Passwörter, noch bevor sie ausgenutzt werden können. Da schützt Ihre Benutzer und Daten zuverlässig vor Bedrohungen.
- **Anpassbare Sicherheitsrichtlinien:** Stellt Administratoren detaillierte Kontrollen zur Verfügung, mit denen sie bestimmte Aktionen konfigurieren können, sobald kompromittierte Anmeldedaten erkannt wurden. Dies ermöglich maßgeschneiderte Sicherheitsmaßnahmen wie eine Passwortrücksetzung oder die Erzwingung zusätzlicher Authentifizierung.
- **Verbesserte Sicherheitslage:** Verbessert Ihre allgemeine Sicherheitslage dank einer wichtigen Schutzebene gegen einen der häufigsten Angriffspunkte. Dies verhindert unbefugte Zugriffe und verringert die Gefahr potenzieller Data Breaches.

Installation

Diese Funktion steht im Early Access zur Verfügung.

Kontaktieren Sie Ihren Okta-Vertreter oder unser Vertriebsteam, um über konkrete Anforderungen zu sprechen und zu erfahren, wie Ihr Unternehmen von Okta Customer Identity profitieren kann.

Mehr erfahren



okta

Okta Customer Identity

Allgemein verfügbar

Claims-Austausch zwischen Okta und externen Identity-Anbietern

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

Verbessert die User Experience und gewährleistet starke Sicherheit, indem vertrauenswürdige Claims von externen Identity-Anbietern beim Okta-Service Provider validiert werden.

Classic OIE

Claims-Austausch zwischen Okta Orgs

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

Erweiterung des Identitätsverbunds durch sicheren und nahtlosen Zugriff auf Ressourcen über Okta Orgs hinweg.

Classic OIE

Neue Workflows-Konnektoren

Verfügbar in Workflows || Autorisiert für FedRAMP High, Unterstützt für FedRAMP Moderate/DOD IL4

Integration mit mehr Okta-APIs und gängigen Anwendungen (Coupa, Splunk), um Benutzer und Gruppen zu verwalten.

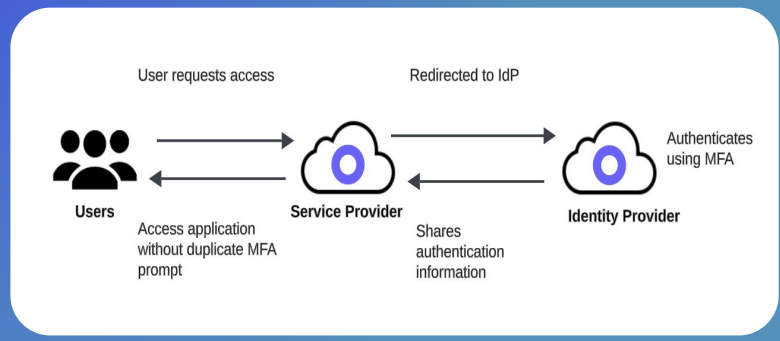
Classic OIE

Berechtigungsbedingungen für die Benutzererstellung

Feature von Custom Admin Roles, Secure Partner Access / Verfügbar in allen SKUs || Autorisiert für FedRAMP Moderate/High/DOD IL4

Verhindert, dass delegierte oder Partner-Administratoren vertrauliche Attributwerte zuweisen können. Setzt attributbasierte Zugriffskontrollen durch und reduziert das Risiko von Konfigurationsfehlern beim Benutzer-Onboarding.

Classic OIE



Claims-Austausch zwischen Okta Orgs

Okta Customer Identity

Allgemein verfügbar

Nicht-menschliche Identities – Transparenz und Risikoanalyse

Feature von Identity Security Posture Management (ISPM)

Security-Teams profitieren von der erforderlichen Transparenz zum Schutz vor Kompromittierungen nicht-menschlicher Identities: Erkennung und Meldung der riskantesten Service-Accounts, von menschlichen Benutzern, die Anmeldedaten nicht-menschlicher Identities verwenden, und von nicht rotierten Schlüsseln und Token.

Classic

OIE

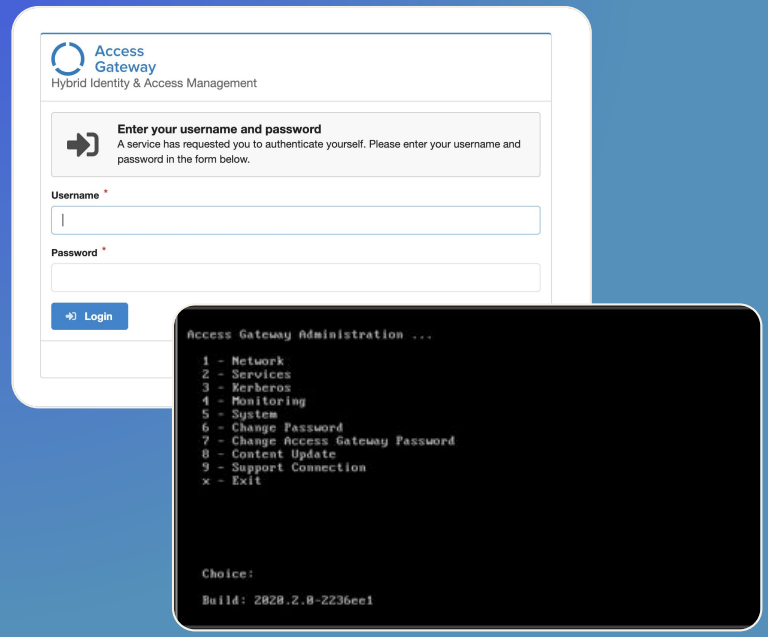
Änderungen im Zuge der OAG-Initiative „Secure by Design“

Verfügbar in Okta Access Gateway / Unterstützt für FedRAMP Moderate/High/DOD IL4

Standardmäßig ist der Zugriff auf die OAG-Administratorkonsole nur im lokalen Netzwerk möglich und erfordert eine Passwortänderung für die Administratorkonsole und die Befehlszeilenschnittstelle der Administratorverwaltung. Diese Änderungen dienen zur Umsetzung der Okta-Initiative „Secure by Design“.

Classic

OIE



Änderungen im Zuge der OAG-Initiative „Secure by Design“

Okta Customer Identity

Early Access

Weitergabe von Single-Logout-Anforderungen an externen Identity-Anbieter

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

Bereitstellung von stärkerer Sicherheit für Kunden mit Okta Customer Identity (ehemals CIS), die Anwendungsfälle mit gemeinsam genutzten Geräten abdecken müssen.

OIE

Netzwerkbeschränkungen für Token Endpoint

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

Ermöglicht kundenspezifische zulässige Zonen (per Allow-Liste), um das Risiko von Token-Missbrauch zu reduzieren, Kunden-Sessions abzusichern und Backend-Systeme vor DoS-Angriffen und Ausschöpfung der Anzahlbegrenzung zu schützen.

OIE

Residential Proxy als IP-Service-Kategorie

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

Enhanced Dynamic Zones unterstützt nun Residential Proxies und Blockchain VPNs als IP-Service-Kategorien, sodass Unternehmen den Zugriff vor der Richtlinienbewertung blockieren können.

Classic

OIE

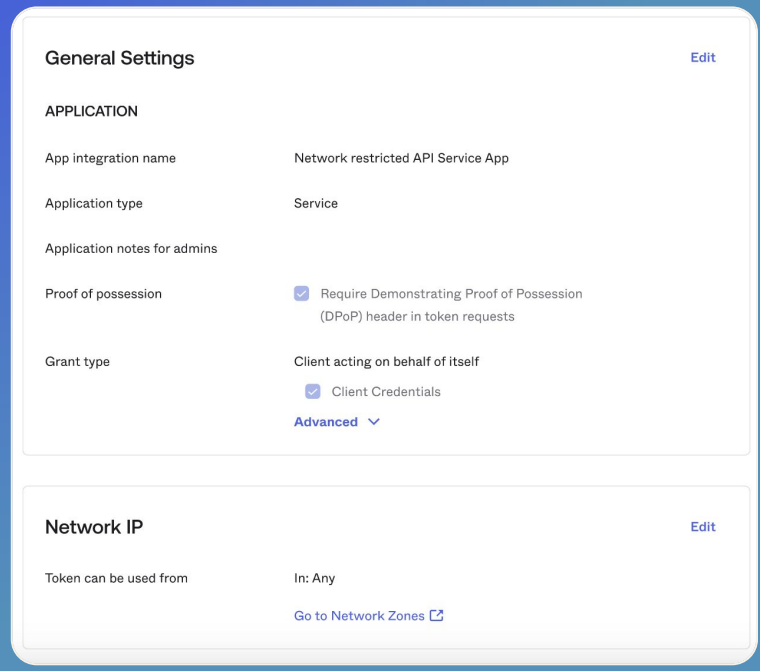
Inkrementelle Importe mit DirSync

Verfügbar in Okta Directory Integration || Autorisiert für FedRAMP Moderate/High/DOD IL4

Verbesserung der inkrementellen Importe aus Active Directory, was schnellere und effizientere Importe mit weniger Fallbacks zu vollständigen Importen ermöglicht. Dies ist zur Bereitstellung nahtloser Customer Experiences unverzichtbar.

Classic

OIE



Netzwerkbeschränkungen für Token Endpoint

Okta Customer Identity

Early Access

ID-Verifizierung mit Namensabgleich

Verfügbar in SSO/MFA || Autorisiert für FedRAMP Moderate/High/DOD IL4

Verbessert die Genauigkeit und User Experience, indem genau zwischen offiziellem Namen und bevorzugtem Namen differenziert wird. Dies verbessert das Vertrauen und die Sicherheit bei Onboarding, Authentifizierung, Account-Wiederherstellung und Support-Workflows.

OIE

Erweiterung von appID Context für OIDC- und SAML-Anwendungen

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

Übergibt während der von Okta initiierten Föderation (SAML/OIDC) Informationen über Anwendungen (ID, Name) an externe Identity-Anbieter, um fundiertere Sicherheits- und Richtlinienentscheidungen beim Identity-Anbieter zu ermöglichen.

OIE

Überlappende Identity-Anbieter-Signaturzertifikate

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

Unterstützung mehrerer aktiver Zertifikate pro Identity-Anbieter für nahtlose Zertifikatrotation, um Ausfallzeiten sowie Betriebsaufwand zu reduzieren und die Sicherheit zu verbessern.

Classic

OIE

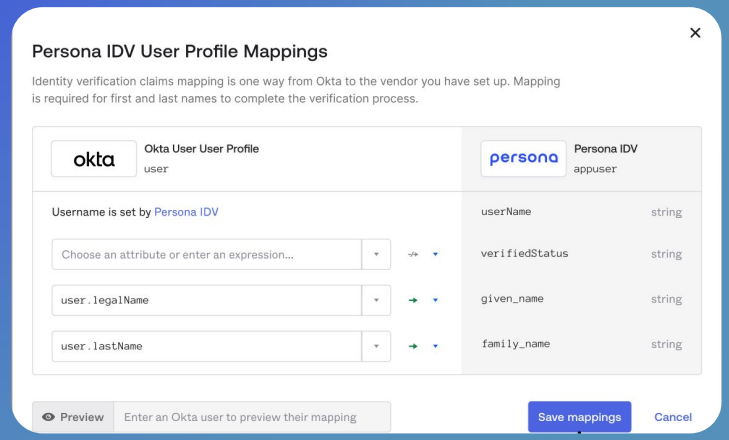
Schutz vor kompromittierten Anmeldedaten (Phase 2)

Verfügbar in allen SKUs

Ermöglicht maßgeschneiderte User Experiences und Verifizierungs-Workflows mithilfe von Test-Accounts. Dies verbessert die Sicherheit und das Vertrauen in Abläufe.

Classic

OIE



ID-Verifizierung mit Namensabgleich

Okta Customer Identity

Early Access

Unterstützung von Universal Logout für Okta Customer Identity-Anwendungen

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

Einfache Integration von Universal Logout in Ihre Okta Customer Identity-Anwendungen (ehemals CIS) – ohne jeden Entwicklungsaufwand.

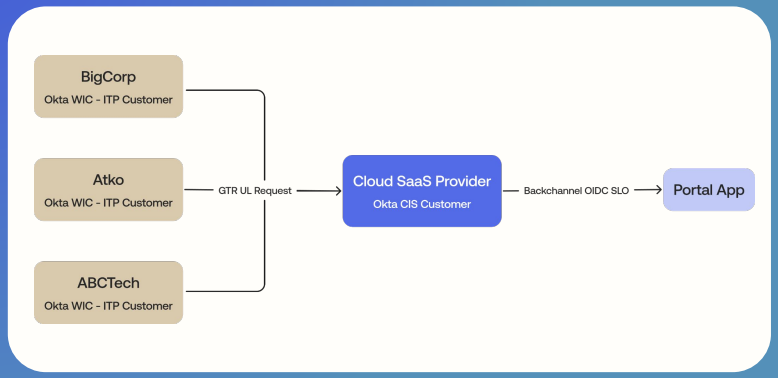
OIE

Governance für Workflows

Verfügbar in Workflows || Okta Identity Governance (OIG) unterstützt in DOD IL4; Workflows autorisiert für FedRAMP High, unterstützt für FedRAMP Moderate/DOD IL4

Nutzung der Nutzung der Access Requests- und Access Certifications-Rollen und -Ressourcen für Workflows in OIC zur Optimierung des Kundensupports und Gewährung von zeitgebundenen Zugriffen mit benutzerdefinierten Zugriffsanforderungen.

OIE



Unterstützung von Universal Logout für OCI-Anwendungen


okta