Présentation des nouveautés

en Early Access ou General Availability au T2 (avril-juin 2025)

Safe Harbor

Cette présentation contient des déclarations prospectives au sens des dispositions dites de « Safe Harbor » du Private Securities Litigation Reform Act de 1995, y compris, mais sans s'y limiter, des déclarations concernant nos perspectives financières, notre stratégie d'entreprise, nos plans de développement, les tendances du marché, la taille du marché, les opportunités de marché et notre positionnement sur le marché. Ces déclarations prospectives sont le reflet des attentes, estimations, prévisions et projections actuelles. Dans certains cas, les déclarations prospectives peuvent être identifiées par l'utilisation de termes tels que « prévoir », « anticiper », « devrait », « penser », « espérer », « viser », « projeter », « objectifs », « estimer », « potentiel », « prédire », « peut », « sera », « pourrait », « avoir l'intention », « doit », des variations de ces termes ou d'autres expressions similaires. Les déclarations prospectives sont sujettes à un certain nombre de risques et d'incertitudes, dont beaucoup impliquent des facteurs ou des circonstances hors de notre contrôle. Par exemple, le contexte économique mondial a par le passé et pourrait à l'avenir réduire la demande de nos produits ; nous et nos prestataires de services tiers avons par le passé et pourrions à l'avenir subir des incidents de cybersécurité ; nous pourrions ne pas être en mesure de gérer ou de maintenir le niveau de croissance que notre entreprise a connu au cours de périodes antérieures ; nos ressources financières pourraient ne pas être suffisantes pour maintenir ou améliorer notre compétitivité ; nous pourrions ne pas être en mesure d'attirer de nouveaux clients, ou de fidéliser ou de vendre des produits supplémentaires à nos clients actuels ; la croissance de la clientèle a ralenti au cours des dernières périodes et pourrait continuer de décélérer à l'avenir ; nous pourrions subir des interruptions ou des problèmes de performances liés à nos technologies, notamment une interruption de service ; nous et nos prestataires de services tiers n'avons pas respecté, ou avons donné l'impression de ne pas avoir respecté, diverses dispositions de confidentialité et de sécurité auxquelles nous sommes soumis, et des incidents similaires pourraient survenir à l'avenir ; nous pourrions ne pas atteindre les synergies et les efficacités opérationnelles escomptées suite à des acquisitions ou à des regroupements d'entreprises, et nous pourrions ne pas réussir à intégrer les entreprises que nous rachetons ; et nous pourrions ne pas être en capacité de rembourser nos billets convertibles de premier rang dans les délais attendus. De plus amples informations sur les facteurs potentiels qui pourraient affecter nos résultats financiers sont incluses dans notre dernier rapport trimestriel sur le formulaire 10-Q et les autres documents que nous avons déposés auprès de la Securities and Exchange Commission. Les déclarations prospectives comprises dans cette présentation ne représentent que notre point de vue à la date de cette présentation. Nous déclinons toute obligation de mettre à jour ces déclarations prospectives et n'avons pas l'intention de le faire.

Tous les produits, fonctions et fonctionnalités, certifications ou attestations référencés dans cette présentation qui ne sont pas encore disponibles en version GA, qui n'ont pas encore été distribués ou ne sont pas encore gérés, pourraient être distribués à une date ultérieure à la date annoncée, ou annulés. Les roadmaps produits ne représentent en rien un engagement, une obligation ou une promesse d'offre de produit, de fonctionnalité, de certification ou d'attestation, et les clients ne doivent pas se baser sur ces plans pour prendre leur décision d'achat.

Pour en savoir plus sur nos dernières innovations et nos projets en cours

Page web de présentation des nouveautés

Découvrez les innovations annoncées lors de la Launch Week et de nombreuses ressources pour en savoir plus ici.

Contactez l'équipe commerciale ici.

Webinars sur la roadmap produits Okta

Découvrez les nouveautés produits en avant-première.

Inscrivez-vous au webinar sur la roadmap produits Okta ici.

Résumé vidéo des points clés + Notes de distribution

Regardez une présentation courte et instructive sur les dernières mises à jour, fonctionnalités et améliorations.
Résumé des points clés.

Consultez les notes de distribution ici.

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

okta

Bienvenue dans la présentation des nouveautés Okta Platform

T2 2025

Avec l'élargissement de la surface d'attaque, causé par la multiplication des terminaux, des agents d'IA et des environnements distribués, protéger chaque identité est un enjeu plus critique que jamais.

Ce trimestre, nous lançons de nouvelles fonctionnalités pour vous aider à relever ce défi. Grâce aux dernières améliorations apportées à Okta Workforce Identity, vous pouvez :

- Renforcer la sécurité des terminaux au sein de votre écosystème
- Découvrir et gérer le cycle de vie complet des identités non humaines

Ces mises à jour soutiennent une approche de la sécurité proactive et axée sur l'identité, car l'identité est la clé de la sécurité.

Explorer la présentation

La présentation des nouveautés produits possède deux sections principales :

Okta Workforce Identity

- Présentation d'Okta Workforce Identity
- En vedette
- Présentation des nouveautés produits
- Ressources pour les développeurs

Okta Customer Identity

- Présentation d'Okta Customer Identity
- En vedette
- Présentation des nouveautés produits

Okta Workforce Identity

Okta Workforce Identity renforce votre posture de sécurité en automatisant la prise de décision d'accès et en appliquant des politiques cohérentes. Cette approche permet de réduire les tâches manuelles pour votre équipe et simplifie les opérations IT.

Ce trimestre, nous capitalisons sur ces acquis et nous proposons des contrôles de sécurité et de gouvernance plus robustes destinés à vos ressources les plus critiques : terminaux, utilisateurs (agents d'IA compris) et ressources à privilèges.

En vedette

Okta Workforce Identity

- Sécurité avant, pendant et après l'authentification
- Comptes Active Directory
- Identity Threat Protection avec Okta AI
- Cross App Access (for AI Agents)
- Roadmap de conformité pour le secteur public aux USA

Toutes les fonctionnalités

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

Ressources pour les développeurs

Okta Platform donne vie à l'écosystème de sécurité des identités

Produits de sécurité des identités

Governance
- Okta Identity Governance

Posture Management
- Identity Security Posture Management

Okta Privileged Management
- Okta Privileged Access

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

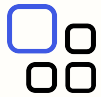
Device Access
- Okta Device Access

Identity Threat Protection
- Identity Threat Protection avec Okta AI

Orchestration de sécurité des identités

Intégrations de sécurité des identités

Infrastructure
IaaS  Serveurs on-premise

Applications
Apps cloud  Apps on-premise

API
Publiques  Privées

Identités
Annuaires  Non humaines / Agents d'IA

99,99 % de disponibilité. Des dizaines de milliards de connexions mensuelles. Aucune interruption planifiée.

okta

En vedette : Sécurité avant, pendant et après l'authentification

Comptes Active Directory

- Tirez parti de votre agent Okta AD existant pour identifier les comptes à privilèges.
- Protégez les comptes AD avec des politiques d'accès et la rotation automatique des identifiants

Identity Security Posture Management

- Visualisez les relations d'accès multitenants et les failles MFA au niveau des instances Okta.
- Identifiez les contournements du MFA et les faiblesses des politiques au sein de votre écosystème d'identités.

Identity Threat Protection avec Okta AI

- Renforcez la sécurité des comptes administrateurs.
- Unifiez la détection et la réponse aux menaces au sein de votre environnement et en temps réel.

okta

Early Access

En vedette : Comptes Active Directory

Gérez les comptes Active Directory

Présentation

Cette fonctionnalité vous permet de vous connecter aux environnements Active Directory à l'aide de votre agent Okta AD existant, d'identifier les comptes AD à privilèges et d'en gérer les mots de passe, de créer des politiques d'accès robustes et d'auditer toutes les activités des administrateurs et des utilisateurs.

Défis pour les clients :

Les comptes à privilèges dans Active Directory sont généralement non gérés et particulièrement convoités par les acteurs malveillants.

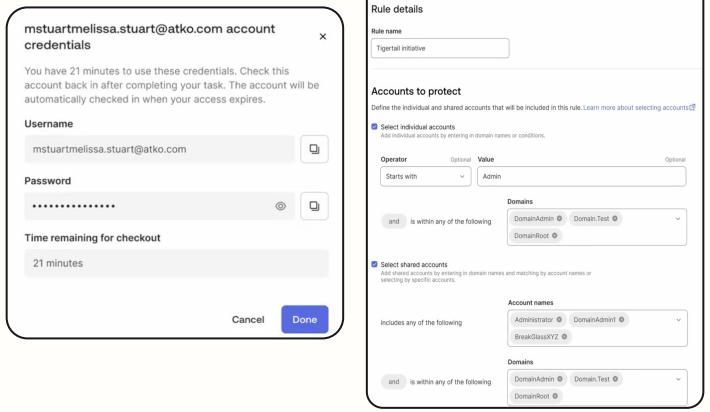
Pourquoi c'est important

Que ce soit à des fins de conformité ou de renforcement de la posture de sécurité, les comptes Active Directory doivent être protégés contre les utilisateurs non autorisés. Les bonnes pratiques exigent que les comptes à privilèges soient mis en coffre, que leurs mots de passe fassent l'objet d'une rotation régulière et que les responsables de la sécurité sachent qui a accès à quelles ressources.

Comment en bénéficier

Cette fonctionnalité est en disponibilité globale (GA) dans Okta Privileged Access. Contactez votre CSM ou votre responsable de compte pour la faire activer pour votre environnement.

Voir l'article de blog



En vedette : Identity Threat Protection avec Okta AI

Étendez la visibilité sur les menaces et automatisez les actions sur l'ensemble de votre pile technologique en temps réel

Présentation

Rôles administrateurs personnalisés pour ITP – Appliquez le principe du moindre privilège en octroyant des autorisations administrateurs pour la gestion des configurations ITP.

Détections ITP pour les rôles de super administrateur* – Surveillez et détectez les comportements anormaux qui ciblent des super administrateurs afin d'identifier les tentatives d'usurpation de compte (ATO).

Intégration SSF avec Palo Alto Networks – Corrélez les signaux d'identité avec les informations provenant de plateformes XDR comme Palo Alto Networks pour améliorer la détection, réduire les silos et favoriser des actions coordonnées au sein de votre écosystème.

Transmetteur SSF – Utilisez les signaux d'identité d'Okta pour déclencher des actions automatisées (révocation de session, demandes MFA, etc.) dans des outils tiers tels qu'Apple Business Manager, en vue d'accélérer les workflows de réponse aux incidents.

* Désormais disponibles pour les clients Adaptive MFA

Pourquoi c'est important

Ces nouveautés offrent un contrôle accru sur les autorisations administrateurs, une visibilité étendue sur les risques liés à ces comptes à privilèges élevés, ainsi que la possibilité de répondre aux menaces plus rapidement et de façon plus proactive au sein de votre environnement.

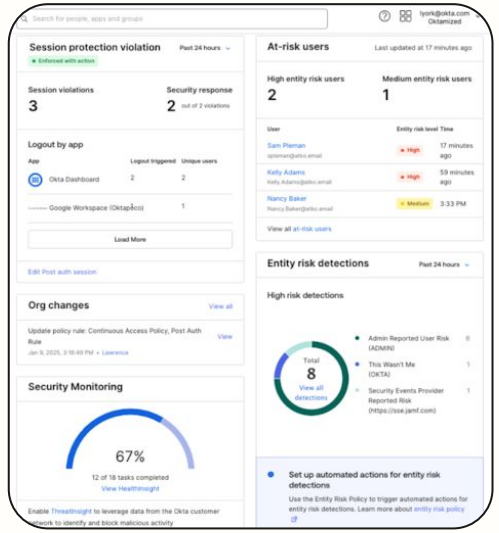
Défis pour les clients :

Les entreprises peinent souvent à appliquer le principe du moindre privilège aux administrateurs, ce qui entraîne l'exposition de configurations critiques en raison de rôles aux autorisations excessives. En parallèle, une visibilité limitée sur les activités des super administrateurs augmente le risque d'usurpations de comptes non détectées. Sans signaux d'identité intégrés ni fonctionnalités de réponse automatisées, la détection et la réponse aux menaces restent fragmentées et lentes, ce qui affaiblit la posture de sécurité globale.

Comment en bénéficier

- Les rôles administrateurs personnalisés pour ITP, l'intégration SSF pour Palo Alto Networks et le transmetteur SSF sont disponibles avec le **SKU ITP**.
- Les détections ITP pour les rôles de super administrateur sont désormais disponibles avec le **SKU Adaptive MFA.**

En savoir plus



En vedette : Cross App Access (for AI Agents)

Sécurisez la couche invisible d'intégration entre apps et agents d'IA. Les ISV peuvent se lancer immédiatement – disponible comme fonctionnalité Okta pour certains clients au T3 2026

Présentation

Cross App Access for AI Agents est un protocole qui assure des connexions de confiance entre les applications et les agents d'IA. Il transfère le contrôle et le consentement à l'administrateur IT afin que celui-ci puisse décider quelles applications se connectent et déterminer les ressources exactes auxquelles elles accèdent.

Défis pour les clients :

Les agents d'IA agissent de manière indépendante pour accomplir des tâches, prendre des décisions et se connecter à d'autres systèmes, sans demander d'autorisation. Ils créent ainsi une couche cachée d'accès à privilèges au sein des systèmes. Cela engendre un risque de sécurité inédit et urgent que les outils d'identité traditionnels n'ont pas été conçus pour gérer.

Pourquoi l'adopter en tant qu'ISV

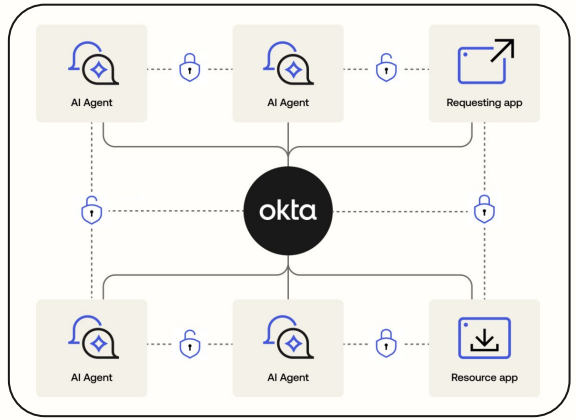
La sécurisation de l'IA agentique nécessite un écosystème de développeurs, de plateformes d'identité et d'entreprises qui travaillent ensemble. Les éditeurs de logiciels indépendants (ISV) jouent un rôle déterminant.

Alors que les agents d'IA se multiplient et gagnent en sophistication (et agissent au nom des utilisateurs), les failles de sécurité qu'ils engendrent augmentent elles aussi. Le protocole Cross App Access d'Okta offre un système de supervision moderne pour faire face à cette nouvelle réalité, fournissant aux éditeurs de logiciels indépendants un moyen sécurisé de contrôler la façon dont les agents autonomes et les applications communiquent. Il aide les développeurs d'applications SaaS B2B à répondre aux exigences des entreprises tout en stimulant l'innovation.

Pour en savoir plus

Les ISV peuvent se lancer dès aujourd'hui. Disponible en Early Access pour les clients au T3 2026.

- En savoir plus
- **Participez à notre événement en ligne « Identity Summit: Securing Agentic AI »** (En savoir plus).



okta

En vedette : Roadmap de conformité pour le secteur public aux USA

Présentation

La plateforme complète d'Okta propose désormais de nouvelles solutions d'identité autorisées et prêtes pour les audits à destination du secteur public aux États-Unis. Nos solutions intégrées Identity Governance, Workflows et Identity Threat Protection avec Okta AI permettent aux organismes publics de moderniser leurs opérations tout en assurant une meilleure prise en charge en matière de gestion des identités.

Défis pour les clients :

- Atteindre des objectifs de modernisation et d'efficacité mesurables tout en respectant des exigences de conformité strictes
- Maintenir les risques à des niveaux acceptables spécifiques ou à des niveaux inférieurs
- Gérer les contraintes en termes de ressources et la pénurie de compétences

Pourquoi c'est important

- La solution d'Okta offre une plateforme unifiée qui améliore le niveau de préparation de cybersécurité des organismes publics et assure l'alignement de la productivité des collaborateurs sur les missions.
- Grâce à des flux d'identité personnalisés, à des renseignements continus sur les tendances d'accès et à une visibilité inégalée, les organisations du secteur public peuvent identifier et neutraliser les menaces de façon proactive, simplifier les opérations et réaliser des économies mesurables.

Comment en bénéficier

- Annonce
- Page de support pour l'évaluation des produits
- Mêmes SKU produits avec ces extensions
  - Okta for Government Moderate
  - Okta for Government High
  - Okta for US Military

okta

Nouveautés d'Okta Workforce Identity

Okta Workforce Identity réunit toutes vos identités – des utilisateurs aux terminaux en passant par les agents d'IA – au sein d'un même écosystème de sécurité.

Nos dernières fonctionnalités étendent cet écosystème en vous aidant à renforcer les comptes AD à privilèges, à automatiser la réponse aux menaces sur l'ensemble de votre pile de sécurité et à appliquer le principe du moindre privilège aux administrateurs.

Identifiez facilement les technologies intégrant chaque nouvelle fonctionnalité* :

Classic | Okta Identity Engine (OIE)

***Prise en charge FedRAMP Moderate/High/DOD IL4 :** ce produit fonctionne comme prévu et est totalement pris en charge dans le portefeuille de solutions Secteur public d'Okta.
***Autorisation FedRAMP Moderate/High/DOD IL4 :** cette fonctionnalité ou ce produit est disponible, totalement pris en charge et a reçu l'autorisation FedRAMP et/ou DISA.

okta

Identity Security Posture Management (ISPM)

General Availability

Identités non humaines – Visibilité et analyse des risques

Fonctionnalité d'Identity Security Posture Management (ISPM)

Les équipes sécurité bénéficient de la visibilité nécessaire pour se protéger contre les brèches imputables à des identités non humaines. Identifiez et signalez les comptes de service les plus à risque, les utilisateurs humains disposant d'identifiants associés à des identités non humaines, ainsi que les clés et les tokens non renouvelés.

Classic

OIE

Erreurs de configuration des agents d'IA SFDC

Fonctionnalité d'Identity Security Posture Management (ISPM)

Détectez les erreurs de configuration à risque pour les agents d'IA SFDC, notamment les accès à privilèges excessifs et les méthodes d'authentification faibles qui pourraient permettre un accès non autorisé aux données ou l'exploitation d'agents d'IA.

Classic

OIE

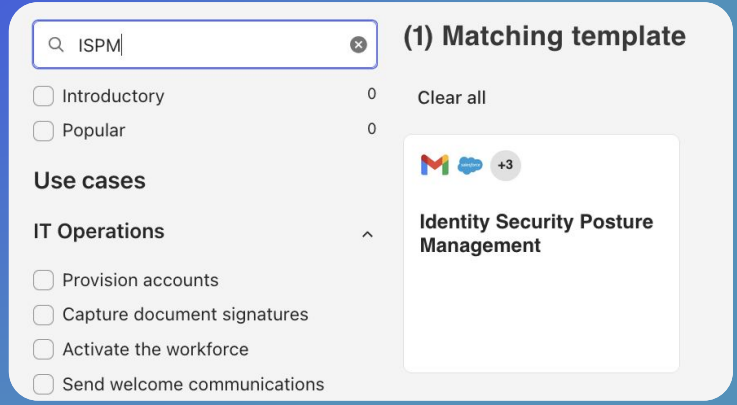
Modèles Okta Workflows de remédiation automatique

Fonctionnalité d'Identity Security Posture Management (ISPM)

Permettez aux clients de déclencher des actions de remédiation automatique en seulement quelques clics. ISPM est désormais doté d'un workflow officiel qui initie des étapes de remédiation telles que la suspension de compte, la réinitialisation de mot de passe, et l'application du MFA ou l'adhésion à ce dernier.

Classic

OIE



Modèles Okta Workflows de remédiation automatique

okta

Identity Security Posture Management (ISPM)

Early Access

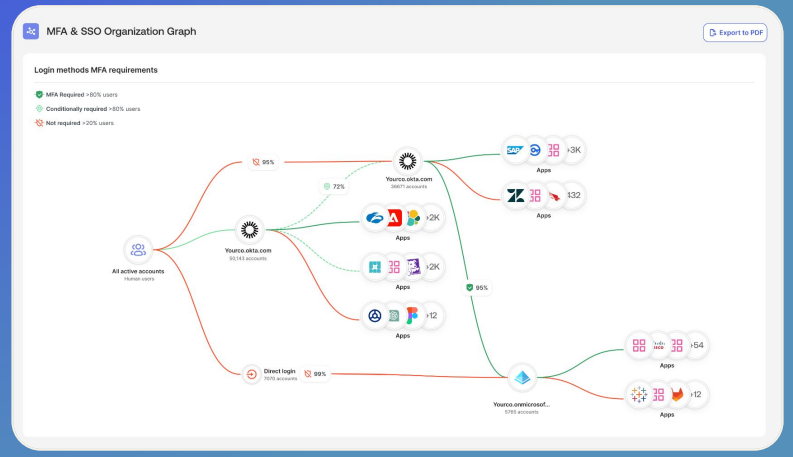
Analyse du MFA et du SSO – Tableau de bord et graphique

Fonctionnalité d'Identity Security Posture Management (ISPM)

Tirez parti d'analyses granulaires du MFA, des facteurs d'authentification et du SSO au sein d'un tableau de bord exportable vous permettant d'identifier plus facilement les principales tendances et les principaux risques.

Classic

OIE



Analyse du MFA et du SSO – Tableau de bord et graphique

Access Management

General Availability

Mappage des demandes AMR (Authentication Method Reference)

Disponible dans Multi-Factor Authentication || Autorisation FedRAMP Moderate/High/DOD IL4

Comme le MFA est obligatoire pour tous les comptes admin, les administrateurs gérant plusieurs organisations peuvent utiliser les demandes AMR pour améliorer l'expérience utilisateur tout en maintenant une sécurité robuste. En savoir plus

OIE

Partage des revendications entre les organisations Okta

Disponible dans tous les SKU || Autorisation FedRAMP Moderate/High/DOD IL4

Améliorez la fédération des identités en mettant en place un accès fluide et sécurisé aux ressources entre les organisations Okta. En savoir plus

Classic

OIE

Partage des revendications entre Okta et les IdP externes

Disponible dans tous les SKU || Autorisation FedRAMP Moderate/High/DOD IL4

Améliorez la fédération des identités en mettant en place un accès fluide et sécurisé aux ressources entre Okta et les IdP tiers sans compromettre la sécurité.

En savoir plus : SAML | OIDC

Classic

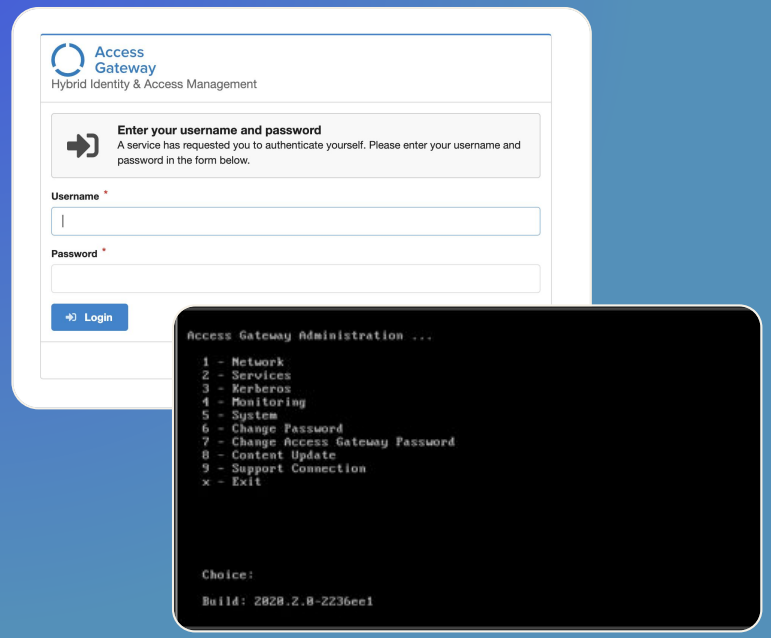
OIE

Modifications apportées à la sécurité dès la conception d'OAG

Disponible dans Okta Access Gateway || Prise en charge FedRAMP Moderate/High/DOD IL4

La console d'administration OAG sera uniquement accessible sur le réseau local par défaut et forcera la modification du mot de passe administrateur pour la console d'administration et l'interface de ligne de commande destinée à la gestion des administrateurs. Ces changements visent à honorer l'engagement de sécurité dès la conception pris par Okta.

OIE



Modifications apportées à la sécurité dès la conception d'OAG

okta

Access Management

General Availability

Récupération MFA sur les postes de travail macOS

Disponible dans Okta Device Access || Autorisation FedRAMP Moderate/High/DOD IL4

Préservez la productivité en permettant aux administrateurs de proposer aux utilisateurs finaux des codes de récupération à durée limitée pour se connecter à leurs terminaux en cas de perte d'un téléphone, d'une clé de sécurité, etc.

En savoir plus

OIE

Droits dans les revendications de jeton et les assertions

Disponible dans Okta Identity Governance (OIG) || Prise en charge DOD IL4

Les administrateurs peuvent désormais configurer des revendications personnalisées dans les attributs des assertions SAML et les tokens OpenID Connect, afin d'appliquer le principe du moindre privilège et de limiter la dépendance vis-à-vis des groupes.

En savoir plus

Classic

OIE

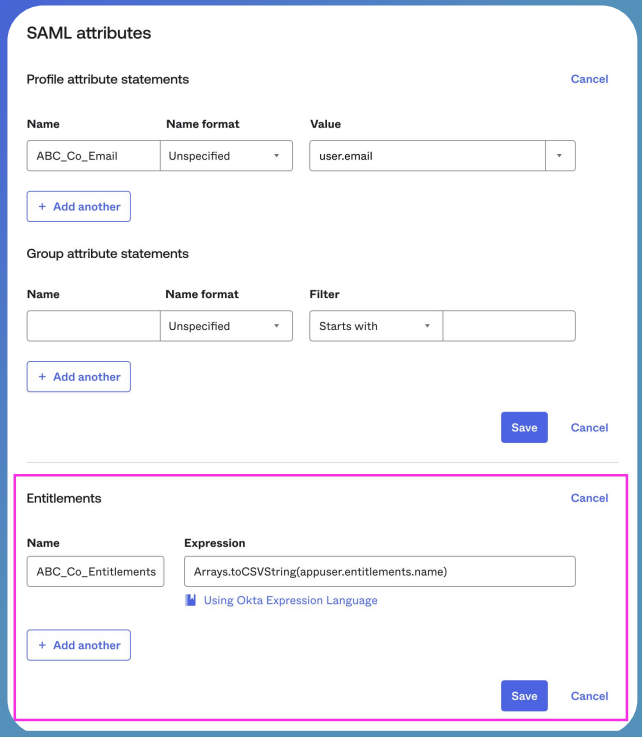
Autorisations administrateur granulaires pour accéder aux fournisseurs d'identité

Disponible dans Okta Identity Engine (OIE) || Autorisation FedRAMP Moderate/High/DOD IL4

Les administrateurs peuvent désormais attribuer des IdP spécifiques à d'autres administrateurs par le biais d'autorisations administrateurs granulaires. Améliorez la posture de sécurité en n'accordant un accès à la configuration des IdP qu'aux utilisateurs autorisés.

Classic

OIE



Droits dans les revendications de jeton et les assertions

Access Management

General Availability

Mises à jour des politiques sous la forme d'actions protégées

Disponible dans tous les SKU || Autorisation FedRAMP Moderate/High/DOD IL4

Lorsque les politiques ITP, de connexion aux applications, de connexion globale et de gestion des comptes sont mises à jour dans la console d'administration, l'administrateur est tenu d'effectuer une authentification renforcée. Cela contribue à empêcher un acteur malveillant d'apporter des modifications s'il accède à une session administrateur.

Classic OIE

Inscription sur le même terminal pour Okta Verify

Disponible dans tous les SKU || Autorisation FedRAMP Moderate/High/DOD IL4

Améliorez les procédures d'inscription des utilisateurs finaux à Okta Verify et à FastPass sur les ordinateurs de bureau et les terminaux mobiles.

Classic OIE

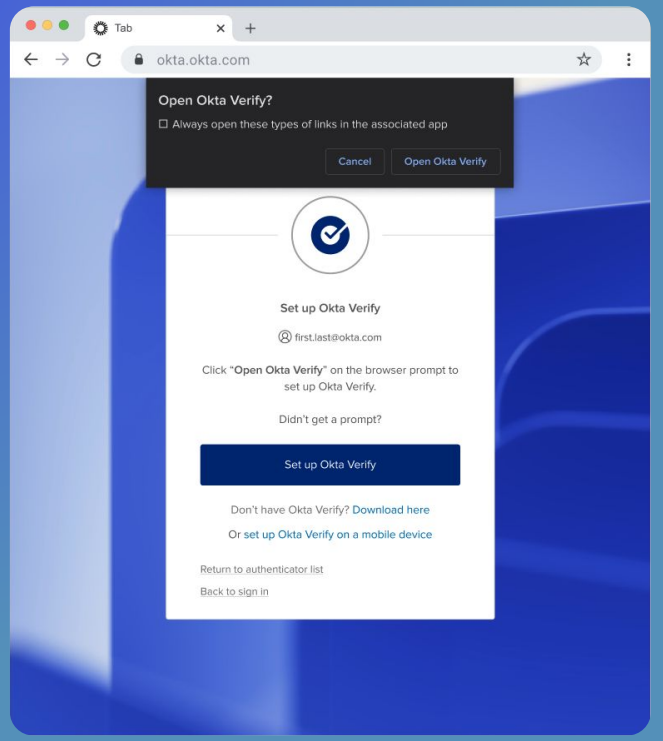
Utilitaire de résolution des problèmes Okta Verify pour iOS

Disponible dans tous les SKU || Autorisation FedRAMP Moderate/High/DOD IL4

Permettez aux utilisateurs de résoudre les problèmes liés aux notifications push et à FastPass au sein de l'application Okta Verify.

En savoir plus

Classic OIE



Inscription sur le même terminal pour Okta Verify

Access Management

Early Access

Advanced Posture Checks

Disponible dans AMFA ‖ Autorisation FedRAMP Moderate/High/DOD IL4

Obtenez et évaluez le contexte d'un terminal, pour n'importe quel paramètre de sécurité ou attribut Windows ou macOS, afin que vous puissiez renforcer la sécurité Zero Trust lors de l'authentification.

En savoir plus

OIE

Évaluation de la fiabilité des terminaux Android pour les politiques Device Assurance

Disponible dans AMFA/ASSO ‖ Autorisation FedRAMP Moderate/High/DOD IL4

Appliquez un large éventail de vérifications supplémentaires des terminaux sous Android dans le cadre d'une politique Device Assurance.

En savoir plus

OIE

Enrichissement du contexte appID pour les applications OIDC et SAML

Disponible dans tous les SKU ‖ Autorisation FedRAMP Moderate/High/DOD IL4

Transmet les détails de l'application (identifiant, nom) aux IdP externes pendant la fédération initiée par Okta (SAML/OIDC), pour une meilleure connaissance situationnelle à la prise de décisions concernant la sécurité et les politiques.

Classic

OIE

Protection contre les identifiants compromis (phase 2)

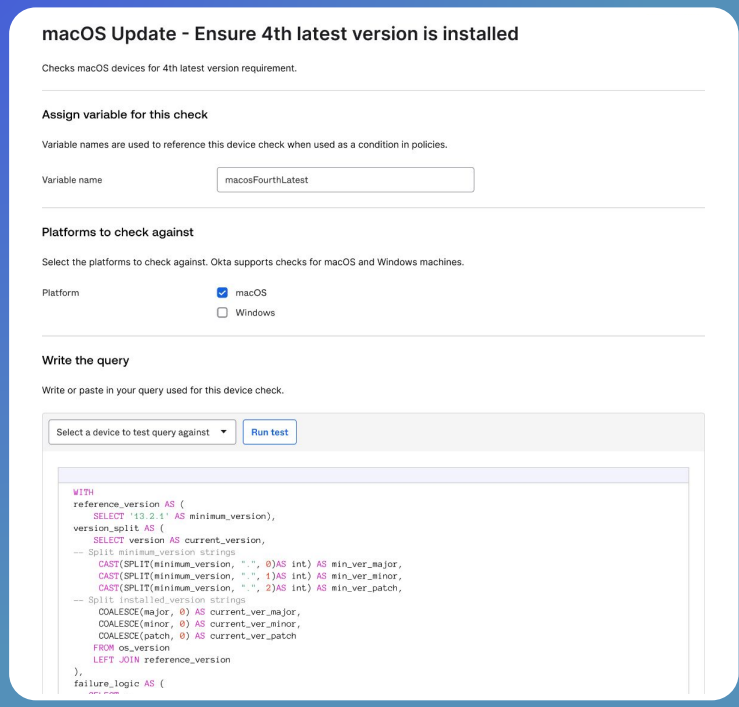
Disponible dans tous les SKU

Réponses personnalisables aux événements associés à des identifiants compromis, avec possibilité pour les administrateurs de valider le flux de réponse aux identifiants compromis à l'aide d'un compte de test.

En savoir plus

Classic

OIE



Advanced Posture Checks

okta

Access Management

Early Access

AAGUID FIDO2 personnalisé

Classic | OIE

Disponible dans MFA/AMFA ‖ Autorisation FedRAMP Moderate/High/DOD IL4

Permettez l'ajout d'authentificateurs approuvés basés sur un AAGUID, tels que les gestionnaires de mots de passe du navigateur, en vue de les utiliser dans des groupes FIDO2 (WebAuthn).

Définition de proxys résidentiels comme catégories de services IP

Classic | OIE

Disponible dans AMFA ‖ Autorisation FedRAMP Moderate/High/DOD IL4

Les zones dynamiques améliorées prennent désormais en charge les proxys résidentiels et les VPN blockchain en tant que catégories de services IP, ce qui permet de bloquer l'accès avant l'évaluation des politiques. En savoir plus

Mise en correspondance des noms pendant la vérification de l'identité

OIE

Disponible dans SSO/MFA ‖ Autorisation FedRAMP Moderate/High/DOD IL4

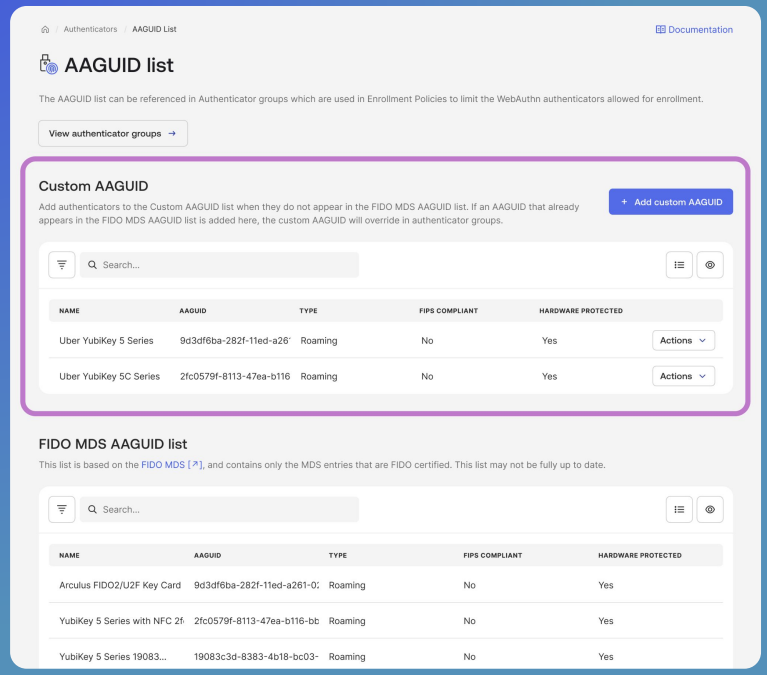
Faites la différence entre le nom légal et le nom choisi en procédant à une mise en correspondance vérifiable des revendications pendant la vérification de l'identité. En savoir plus

Prise en charge de la méthode EAM (External Authentication Method) de Microsoft

OIE

Disponible dans MFA/AMFA ‖ Autorisation FedRAMP Moderate/High/DOD IL4

Permet aux utilisateurs de répondre aux demandes MFA et à d'autres exigences d'assurance en utilisant Okta pour accéder aux applications sécurisées par Entra ID. En savoir plus



AAGUID personnalisé

Access Management

Early Access

Restrictions réseau pour les tokens

Disponible dans tous les SKU || Autorisation FedRAMP Moderate/High/DOD IL4

Renforcez la sécurité en ajoutant à votre liste d'autorisation les zones réseau par client, en restreignant les demandes de tokens aux IdP de confiance et en vous protégeant contre les attaques par réexécution, le vol de tokens, les attaques DoS et l'utilisation abusive de la limitation du débit. En savoir plus

OIE

Mise à jour automatique d'OAG

Disponible dans Access Gateway || Prise en charge FedRAMP Moderate/High/DOD IL4

Les clients peuvent désormais activer les mises à jour automatiques pour s'assurer que leurs déploiements OAG exécutent la dernière version. En savoir plus

OIE

Redondance des certificats de signature des IdP

Disponible dans tous les SKU || Autorisation FedRAMP Moderate/High/DOD IL4

Prenez en charge plusieurs certificats de signature actifs par IdP afin de favoriser une rotation fluide des certificats, en vue de réduire les indisponibilités et les coûts opérationnels tout en renforçant la sécurité. En savoir plus

Classic

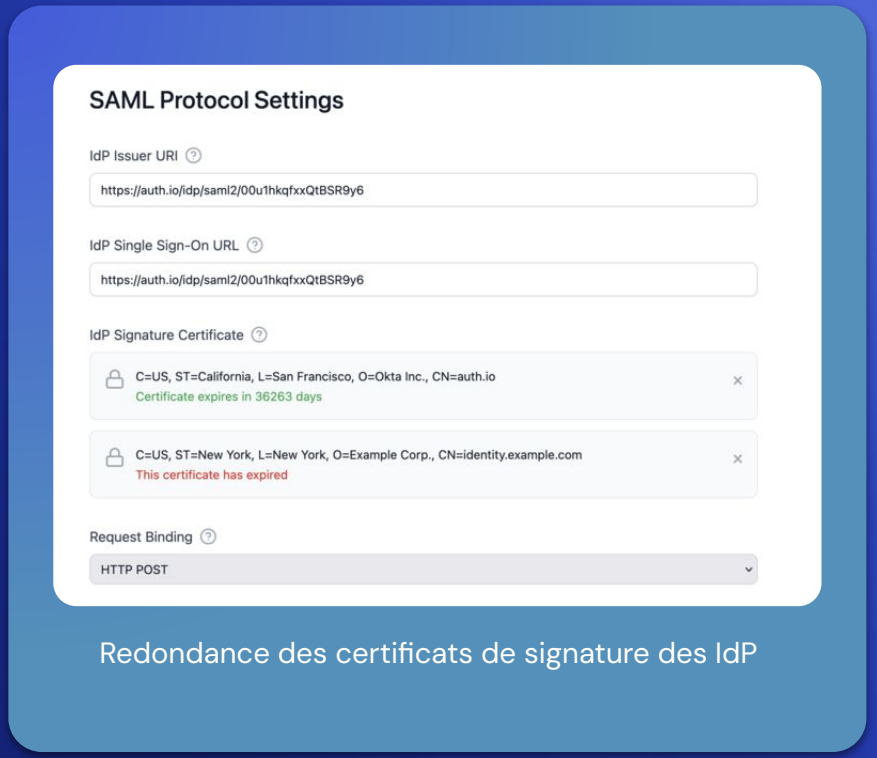
OIE

Prise en charge d'Universal Logout pour les applications Okta Customer Identity

Disponible dans tous les SKU || Autorisation FedRAMP Moderate/High/DOD IL4

Intégrez facilement Universal Logout à vos applications Okta Customer Identity (anciennement CIS), sans aucun travail de développement requis. En savoir plus

OIE



Redondance des certificats de signature des IdP

okta

Access Management

Early Access

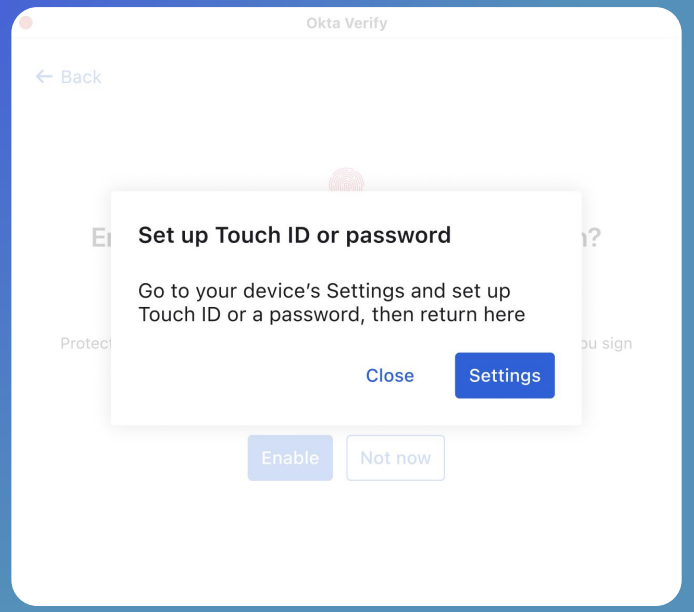
Remédiation de la vérification de l'utilisateur

Disponible dans MFA/AMFA ‖ Autorisation FedRAMP Moderate/High/DOD IL4

Aidez les utilisateurs finaux à activer ou à renforcer la fonction de vérification de l'utilisateur afin de répondre aux exigences des politiques d'authentification.

Classic

OIE



Remédiation de la vérification de l'utilisateur

Identity Management

General Availability

Chiffrement de bout en bout pour l'agent LDAP

Disponible dans les intégrations d'annuaires || Prise en charge FedRAMP Moderate/High/DOD IL4

Renforcez le niveau de sécurité grâce à la surveillance du fichier de configuration de l'agent LDAP et à un chiffrement au niveau du message pour chaque charge utile transférée entre Okta et l'agent LDAP.

Classic OIE

Applications OIN pour la gestion des droits – Splunk, Zoho Mail

Disponible dans Okta Identity Governance (OIG) || Prise en charge DOD IL4

Découvrez, importez, stockez et gérez les droits dans Okta via des offres packagées, des politiques et des règles grâce aux intégrations prêtes à l'emploi pour 4 applications OIN : Splunk, Zoho Mail, CrowdStrike et Oracle IAM.

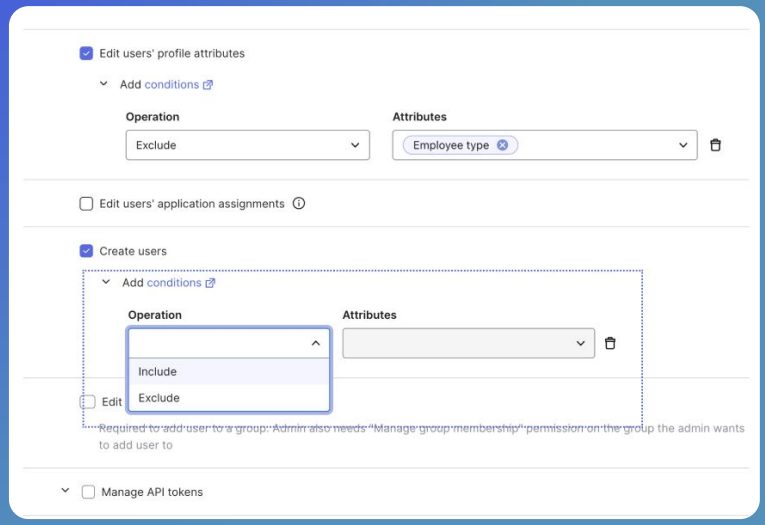
Classic OIE

Conditions d'autorisation pour la création d'un utilisateur

Fonctionnalité de Custom Admin Roles et Secure Partner Access / Disponible dans Secure Partner Access || Autorisation FedRAMP Moderate/High/DOD IL4

Empêche les administrateurs délégués ou des partenaires d'attribuer des valeurs d'attributs sensibles (comme des rôles ou des départements) qui pourraient octroyer involontairement un accès aux systèmes critiques. Permet d'appliquer des politiques de contrôle d'accès basé sur les attributs (ABAC) en s'assurant que seuls les administrateurs adéquats peuvent définir des attributs d'identité liés à l'autorisation. Réduit le risque d'erreur de configuration pendant l'onboarding des utilisateurs, en particulier dans les environnements dont l'administration est déléguée.

Classic OIE



Conditions d'autorisation pour la création d'un utilisateur

okta

Identity Management

Early Access

Importations progressives avec DirSync

Disponible dans les intégrations d'annuaires || Autorisation FedRAMP Moderate/High/DOD IL4

Améliorez les importations progressives à partir d'Active Directory pour optimiser la vitesse et l'efficacité des importations, et pour réduire les recours à des importations complètes.

En savoir plus

Classic OIE

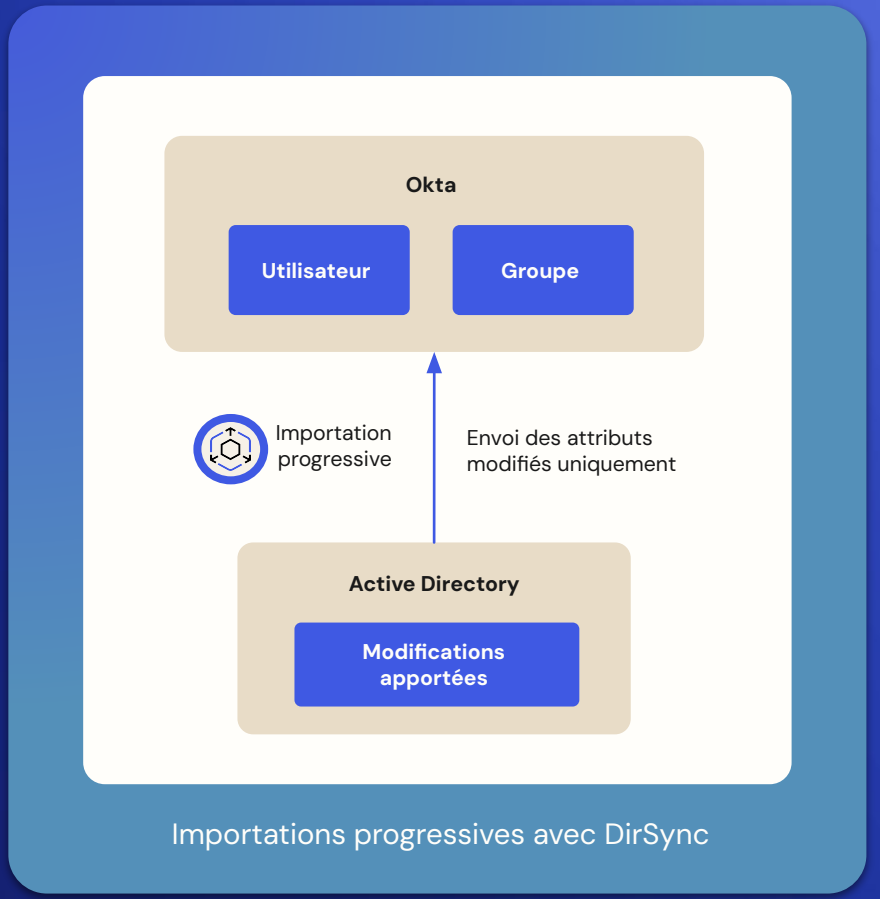
On-prem Connector for Oracle EBS

Disponible dans Okta Identity Governance (OIG) || Prise en charge DOD IL4

Simplifie la gouvernance des identités pour les applications on-premise qui font le lien entre des systèmes hérités et des piles d'applications modernes pour offrir sécurité renforcée, automatisation fluide et conformité.

En savoir plus

Classic OIE



Importations progressives avec DirSync

Identity Governance

General Availability

Améliorations de l'accessibilité et refonte pour Access Requests

Classic OIE

Disponible dans Access Governance || Prise en charge DOD IL4

Facilite la navigation grâce à une interface utilisateur cohérente dans toutes les applications first-party d'Okta. Assure la conformité en matière d'accessibilité grâce à des présentations repensées et inclusives. Réduit la friction pour les utilisateurs en s'alignant sur les modèles de conception habituels d'Okta. En savoir plus

Nouvelles intégrations LCM/Okta Identity Governance (OIG)

Classic OIE

Disponible dans tous les SKU. Autorisation FedRAMP Moderate/High/DOD IL4 pour LCM, prise en charge DOD IL4 pour OIG

Intégrez-vous à davantage de systèmes RH et d'applications populaires (Splunk) pour gérer les utilisateurs, les groupes et les droits. En savoir plus

Collections de ressources

Classic OIE

Disponible dans Okta Identity Governance (OIG) – Access Governance || Prise en charge DOD IL4

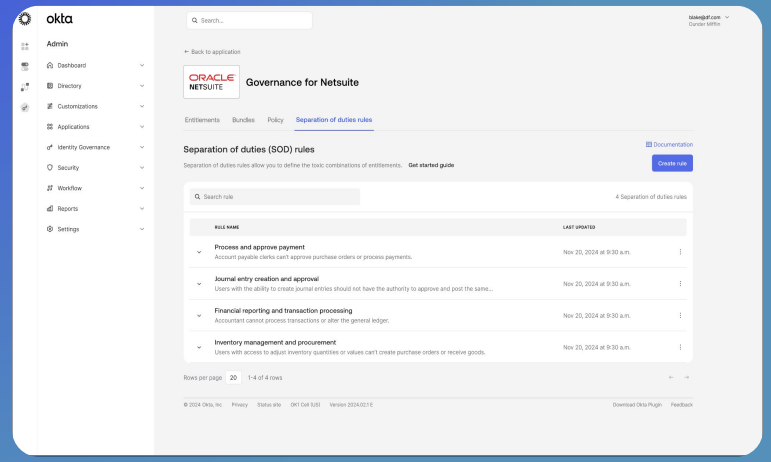
Simplifiez la gestion des droits en regroupant plusieurs applications et groupes afin que les utilisateurs puissent recevoir rapidement l'accès approprié, tout en réduisant la complexité des demandes et des approbateurs. En savoir plus

Séparation des tâches

Classic OIE

Disponible dans Okta Identity Governance (OIG) – Access Governance || Prise en charge DOD IL4

Créez des règles pour définir les combinaisons toxiques de droits et lancez des campagnes de certification afin de corriger les combinaisons toxiques au niveau des utilisateurs. En savoir plus



Séparation des tâches

okta

Privileged Access

Early Access

Comptes Active Directory

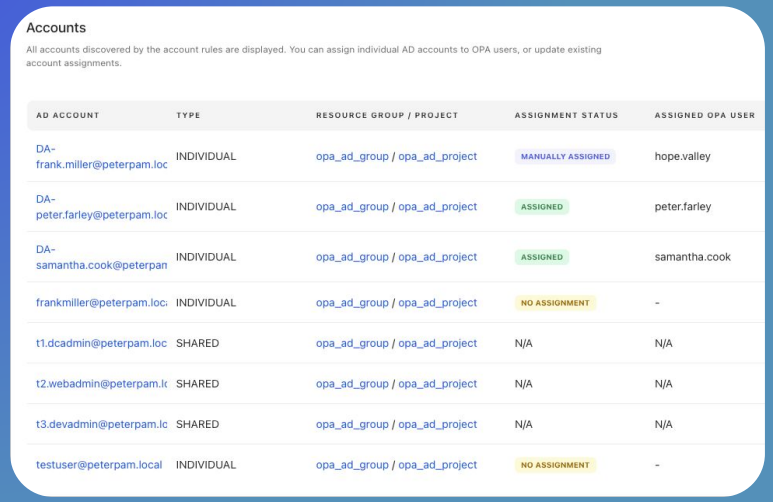
Disponible dans Okta Privileged Access

Gérez les mots de passe des comptes Active Directory à privilèges sans accroître la complexité opérationnelle. Utilisez votre agent Okta Active Directory existant pour identifier les comptes AD, créer des politiques d'accès, automatiser la rotation des identifiants et auditer toutes les activités des administrateurs et des utilisateurs.

En savoir plus

Classic

OIE



Comptes Active Directory

Platform Services

General Availability

Rapports de conformité en matière d'accessibilité (ACR)

Classic OIE

Évaluation : les modèles VPAT couvrent tous les environnements Okta, y compris FedRAMP Moderate/High/DOD IL4.

Offrent une visibilité sur l'état actuel de l'accessibilité du produit pour les clients ; également utiles pour satisfaire les exigences légales et de conformité, en particulier pour les organismes de secteur public au niveau national et régional.

En savoir plus

Ensembles de ressources dynamiques

Classic OIE

Disponible dans tous les SKU || Autorisation FedRAMP Moderate/High/DOD IL4

Permettez aux clients de réserver l'accès aux ressources sensibles à un petit sous-ensemble d'administrateurs.

En savoir plus

Nouveaux connecteurs Workflows

Classic OIE

Disponible dans Workflows || Autorisation FedRAMP High, prise en charge FedRAMP Moderate, DOD IL4

Intégrez-vous à davantage d'API Okta et d'applications populaires (Coupa, Splunk) pour gérer les utilisateurs et les groupes.

En savoir plus

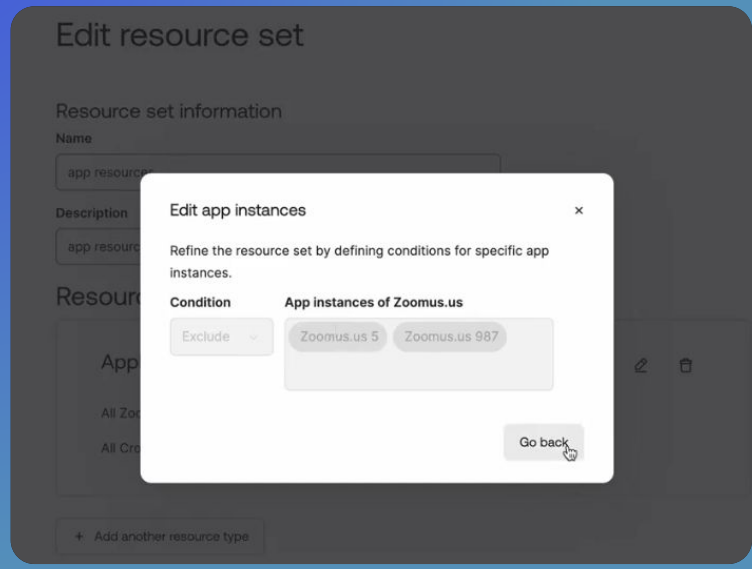
Connecteur Okta ITP pour Workflows

Classic OIE

Disponible dans Workflows || Autorisation FedRAMP High, prise en charge FedRAMP Moderate, DOD IL4

Utilisez le connecteur Okta ITP pour déboguer ou auditer les événements ITP ainsi que pour créer ou modifier les niveaux de risque des utilisateurs.

En savoir plus



Ensembles de ressources dynamiques

okta

Platform Services

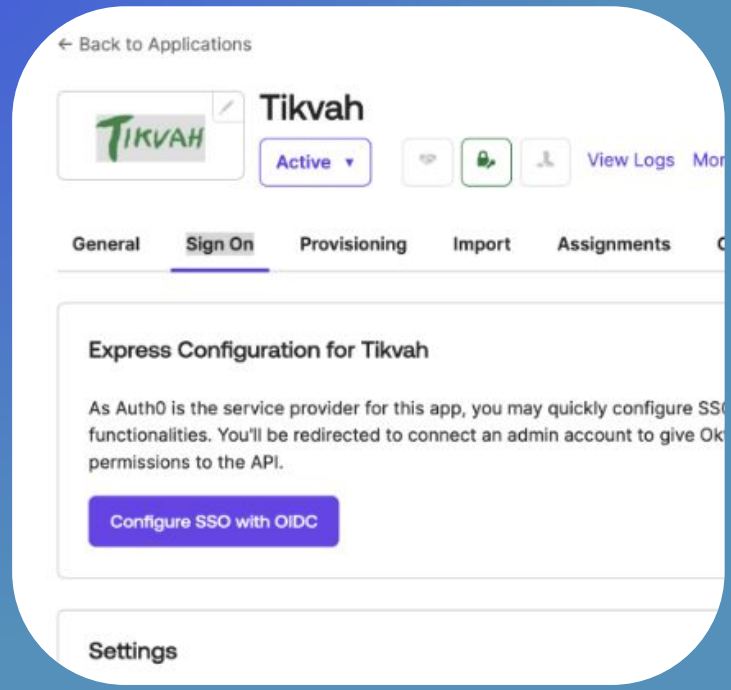
General Availability

Offre packagée Oktane pour ISV : Express Configuration

Disponible dans tous les SKU

Express Configuration permet aux clients professionnels d'ajouter rapidement à leur organisation Okta une instance des applications OIDC opérées par Auth0 publiées dans le catalogue OIN. Ce processus s'appuie sur le partage automatisé de données entre Okta et Auth0.

OIE



Express Configuration

Platform Services

Early Access

Gouvernance pour Workflows

Disponible dans Workflows ‖ Prise en charge DOD IL4 pour Okta Identity Governance (OIG).
Autorisation FedRAMP High et prise en charge FedRAMP Moderate/DOD IL4 pour Workflows

Tirez parti de la puissance des rôles et des ressources Access Requests et Access Certifications pour Workflows dans OIG afin de simplifier l'attribution de rôles et d'octroyer un accès à durée limitée au moyen de demandes d'accès personnalisées.

OIE

Offre packagée pour ISV : programme Activate

Disponible dans Okta Platform (Okta Integration Network)

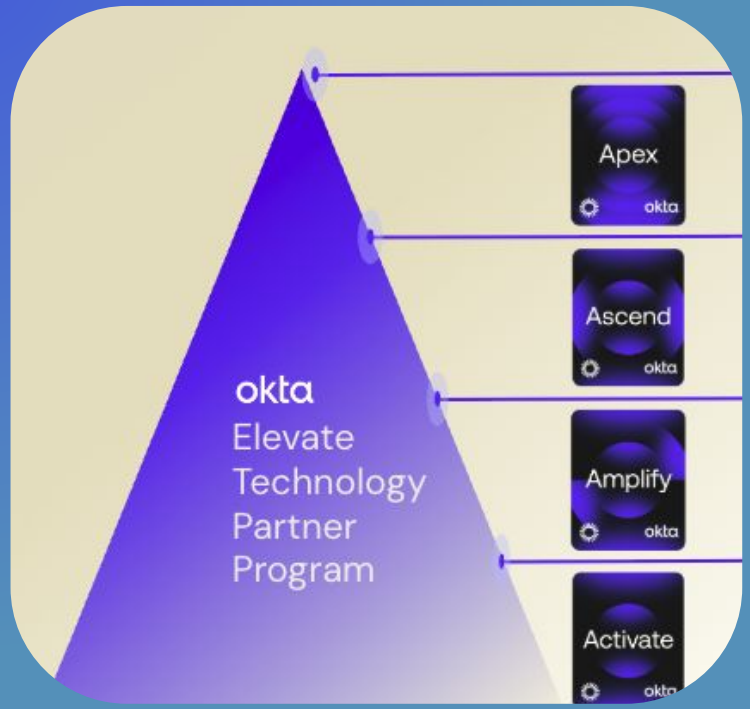
Programme permettant aux ISV de bénéficier d'une visibilité, de formations et d'avantages marketing en libre-service avec Okta en créant, publiant et gérant simplement des intégrations SSO et LCM.

En savoir plus

Offre packagée pour ISV : secureintegrations.dev

Disponible dans tous les SKU

Micro-site axé sur les standards qui indique aux développeurs la procédure à suivre, avec des informations à jour permettant d'inclure les niveaux IPSIE qui ont déjà été ratifiés.



Programme Activate

Offres Premier Success

General Availability

Checklist de maturité de l'identité

Disponible dans Premier Success Plan Silver

Checklist détaillée en libre-service expliquant comment améliorer la maturité de l'identité en fonction de certains objectifs métier et des données récentes sur l'adoption, plus autres ressources de formation et relatives aux événements. En savoir plus

OIE

Plan de maturité de l'identité

Disponible dans Premier Success Plan Gold

Recommandations personnalisées visant à renforcer la maturité de l'identité en fonction de certains objectifs métier et des données récentes sur l'adoption, plus métriques d'activation à la demande, collaboration avec votre Customer Success Manager, suggestions de parcours de formation Okta et autres ressources de formation. En savoir plus

OIE

Expert Learning Pass

Disponible dans Premier Success Plan Silver / Gold

Débloquez l'accès à un catalogue de cours à la demande exclusif, à des sessions de formation animées par des experts et à des bons de certification. Les clients Silver et Gold reçoivent respectivement un et six Expert Learning Pass. En savoir plus

Classic

OIE

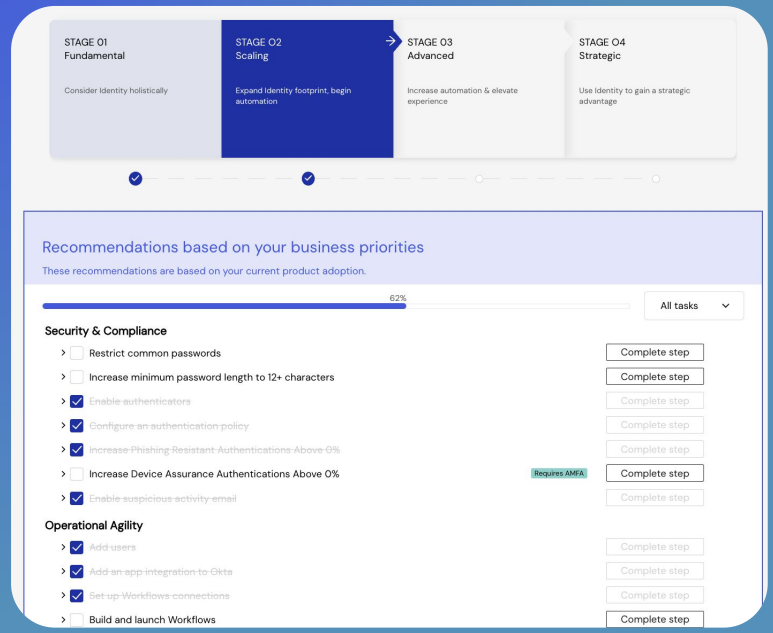
Responsable de compte technique dédié

Disponible en tant qu'extension de Premier Success Plan Gold

Conseiller technique possédant une excellente connaissance de vos produits et de votre architecture, capable de vous proposer des stratégies d'adoption et d'optimisation sur mesure et à long terme.

Classic

OIE



Checklist de maturité de l'identité

Okta Learning

General Availability

Security Series I – NOUVEAU Cours OSIC

Classic | OIE

Disponible dans le catalogue public

Les identités mal configurées offrent aux acteurs malveillants ou aux utilisateurs internes négligents un point d'entrée dans l'infrastructure. Vous devez impérativement vous assurer de disposer d'une configuration optimale de l'identité dès le départ. Ce plan vous indique les axes de travail prioritaires et les bonnes pratiques à suivre dans le cadre de l'engagement Okta Secure Identity Commitment (OSIC). En savoir plus

Nouveau badge Okta – Optimisation de la sécurité et de la gestion des terminaux

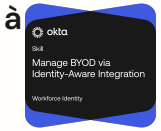
OIE

Disponible dans le catalogue public

Découvrez comment Okta s'intègre à diverses solutions de gestion des terminaux pour sécuriser et gérer les ordinateurs de bureau et les terminaux mobiles. Explorez des configurations de sécurité personnalisées et des processus d'attestation approfondis qui renforcent la sécurité des terminaux et simplifient les tâches de gestion afin d'augmenter la sécurité et la productivité sur le lieu de travail. En savoir plus

Nouveau badge Okta – Gestion du BYOD par une intégration sensible à l'identité

OIE



Disponible dans le catalogue public

Transformez le paysage de la sécurité mobile de votre organisation en implémentant des stratégies BYOD spécifiques à la plateforme qui s'appuient sur l'approche axée sur l'identité d'Okta pour protéger les données d'entreprise et la vie privée des utilisateurs. Au terme du parcours, vous obtiendrez un badge de compétence Okta. En savoir plus

NOUVEAU – Neutralisation des menaces avec ThreatInsight – Security Series I

Ressources pour les développeurs

Okta Workforce Identity

Avec Okta, vous pouvez créer, intégrer et offrir des expériences que vos utilisateurs apprécieront. Découvrez les dernières mises à jour de fonctionnalités, des guides pour développeurs et le feedback de la communauté sur vos builds.

Ressources

Okta Architecture Center : cliquez ici

Ateliers sur la préparation des entreprises : cliquez ici

Blog Développeurs : cliquez ici

Langages et kits SDK : cliquez ici

Guides de démarrage : cliquez ici

Notes de distribution : cliquez ici

Forum de la communauté de développeurs Okta : cliquez ici

Okta Community Toolkit : cliquez ici

Chaîne YouTube OktaDev : cliquez ici

okta

Nouveautés d’Okta Customer Identity

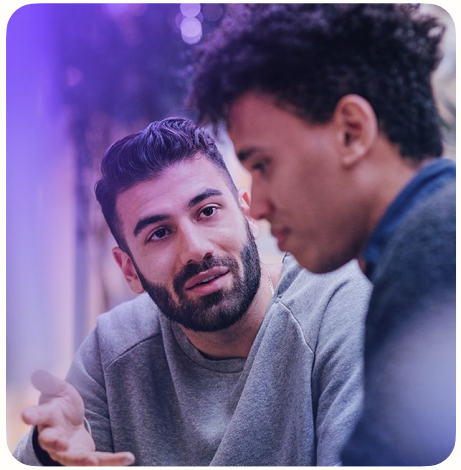
Okta Customer Identity est conçu de telle sorte que la sécurité reste la priorité dans la création d’expériences numériques fluides. La plateforme permet aux entreprises d’accélérer leur croissance, de relever plus facilement les défis de sécurité et de protéger les données métier et clients.

Découvrez nos nouveautés et innovations.

okta

Okta Customer Identity, la solution conçue pour répondre à vos besoins d'identité, aujourd'hui et demain

Une plateforme qui dessert des milliers de clients



Destinée aux équipes IT et sécurité de tous les secteurs

Conçue pour créer des expériences utilisateurs fluides

Fonctionnalités de sécurité avancées offrant la visibilité nécessaire pour détecter les attaques et y répondre

okta

En vedette : Okta Customer Identity

Étendez votre écosystème de sécurité des identités à vos clients et partenaires

Présentation

Okta Customer Identity (OCI) étend les fonctionnalités de sécurité et de gestion des identités fiables que vous utilisez pour vos collaborateurs comme vos utilisateurs externes (clients, partenaires, citoyens, etc.). Cette plateforme complète est conçue pour gérer et sécuriser les identités externes à grande échelle, offrant un accès fluide et sécurisé à vos applications numériques tout en améliorant l'expérience utilisateur.

Défis pour les clients :

De nombreuses organisations utilisent des solutions d'identité fragmentées pour leurs collaborateurs et leurs utilisateurs externes, ce qui engendre une complexité opérationnelle, des failles de sécurité et une expérience utilisateur incohérente. La gestion de systèmes d'identité distincts pour les collaborateurs, les clients et les partenaires crée des silos, élargit la surface d'attaque et freine les initiatives de transformation digitale.

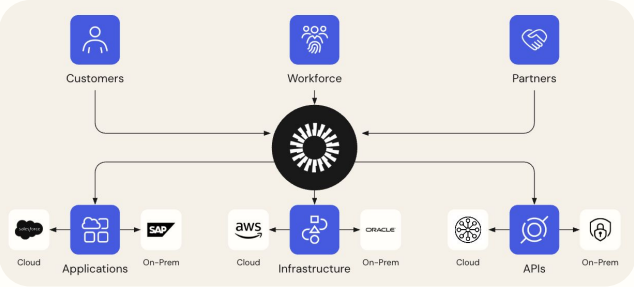
Pourquoi c'est important

- **Plateforme d'identité unifiée :** OCI vous permet de consolider la gestion des identités collaborateurs et clients sur une plateforme Okta unifiée, afin de réduire la complexité, de simplifier les opérations et d'offrir une vue globale de toutes vos identités en renforçant la posture de sécurité et la conformité.
- **Risques réduits et sécurité renforcée :** étendez votre écosystème de sécurité des identités Okta de confiance à vos clients et partenaires, en tirant parti d'une authentification et d'une détection des menaces robustes pour réduire les risques numériques.
- **Expérience utilisateur optimisée et confiance renforcée :** offrez une expérience fluide, cohérente et sécurisée à tous vos utilisateurs (collaborateurs, clients ou partenaires) afin de renforcer la confiance, d'améliorer la fidélité et de stimuler l'engagement avec vos services numériques.

Comment en bénéficier

Contactez votre représentant Okta ou notre équipe commerciale pour discuter de vos besoins spécifiques et découvrir les avantages qu'Okta Customer Identity peut offrir à votre organisation.

En savoir plus



Early Access

En vedette : Protection contre les identifiants compromis

Défendez-vous de façon proactive contre le credential stuffing et l'usurpation de compte (ATO).

Présentation

Compare automatiquement les mots de passe des utilisateurs à un ensemble de données tiers, mis à jour en permanence, qui répertorie les identifiants compromis connus. Cette mesure proactive détermine si le mot de passe d'un des utilisateurs a été exposé lors d'une brèche de données, même si celle-ci s'est produite ailleurs.

Défis pour les clients :

Avec la prolifération des compromissions de données, les attaques de credential stuffing et les usurpations de compte (ATO) constituent des menaces omniprésentes. Les organisations peinent à détecter quand les identifiants de leurs utilisateurs ont été compromis ailleurs sur Internet, ce qui les laisse vulnérables aux cybercriminels qui réutilisent des identifiants volés pour obtenir un accès non autorisé à leurs systèmes.

Pourquoi c'est important

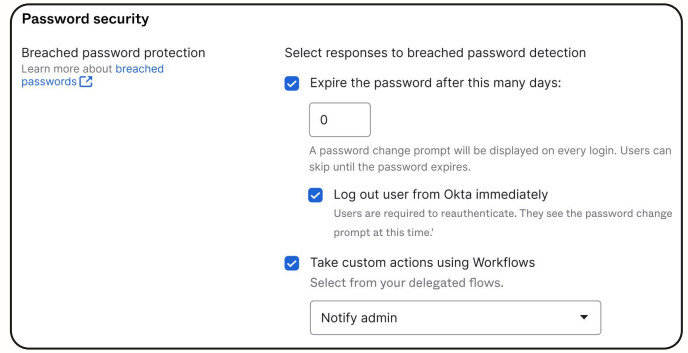
- **Défense proactive contre les menaces :** détecte et réduit automatiquement le risque d'attaques de credential stuffing et d'usurpations de compte (ATO) en identifiant les mots de passe compromis avant qu'ils ne puissent être exploités, afin de protéger vos utilisateurs et vos données.
- **Politiques de sécurité personnalisables :** offrent aux administrateurs un contrôle granulaire pour configurer des réponses spécifiques en cas de détection d'identifiants compromis. Ils peuvent ainsi effectuer des actions de sécurité personnalisées, par exemple en demandant la réinitialisation des mots de passe ou en exigeant une authentification supplémentaire.
- **Posture de sécurité renforcée :** améliore votre posture de sécurité globale en ajoutant un niveau essentiel de défense contre l'un des vecteurs d'attaque les plus courants. Cela permet d'éviter les accès non autorisés et de réduire le risque de brèches de données.

Comment en bénéficier

Cette fonctionnalité est disponible en Early Access.

Contactez votre représentant Okta ou notre équipe commerciale pour discuter de vos besoins spécifiques et découvrir les avantages qu'Okta Customer Identity peut offrir à votre organisation.

En savoir plus



okta

Okta Customer Identity

General Availability

Partage des revendications entre Okta et les IdP externes

Disponible dans tous les SKU || Autorisation FedRAMP Moderate/High/DOD IL4

Améliorez l'expérience utilisateur tout en assurant une sécurité robuste en acceptant et en validant les revendications fiables des IdP externes au niveau du fournisseur de services Okta.

Classic OIE

Partage des revendications entre les organisations Okta

Disponible dans tous les SKU || Autorisation FedRAMP Moderate/High/DOD IL4

Améliorez la fédération des identités en mettant en place un accès fluide et sécurisé aux ressources entre les organisations Okta.

Classic OIE

Nouveaux connecteurs Workflows

Disponible dans Workflows || Autorisation FedRAMP High, prise en charge FedRAMP Moderate, DOD IL4

Intégrez-vous à davantage d'API Okta et d'applications populaires (Coupa, Splunk) pour gérer les utilisateurs et les groupes.

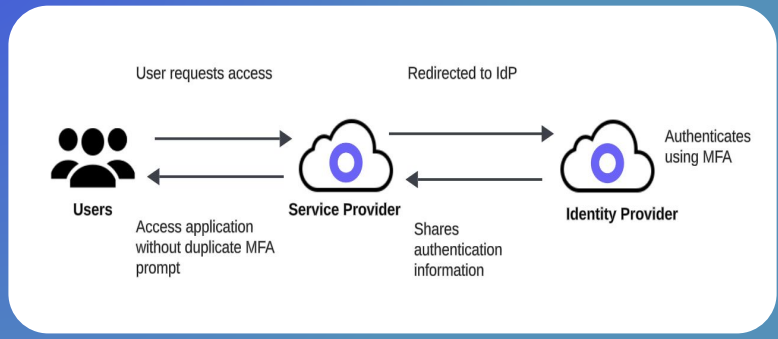
Classic OIE

Conditions d'autorisation pour la création d'un utilisateur

Fonctionnalité de Custom Admin Roles et Secure Partner Access / Disponible dans tous les SKU || Autorisation FedRAMP Moderate/High/DOD IL4

Empêchez les administrateurs délégués ou des partenaires d'attribuer des attributs sensibles, d'appliquer un contrôle d'accès basé sur les attributs (ABAC) et réduisez les risques d'erreurs de configuration pendant l'onboarding des utilisateurs.

Classic OIE



Partage des revendications entre les organisations Okta

Okta Customer Identity

General Availability

Identités non humaines – Visibilité et analyse des risques

Classic OIE

Fonctionnalité d'Identity Security Posture Management (ISPM)

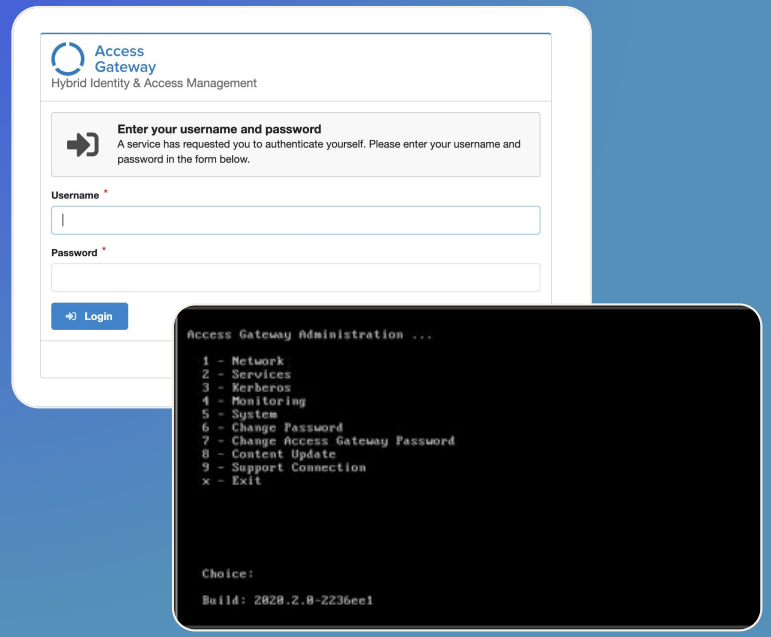
Les équipes sécurité bénéficient de la visibilité nécessaire pour se protéger contre les brèches imputables à des identités non humaines. Identifiez et signalez les comptes de service les plus à risque, les utilisateurs humains disposant d'identifiants associés à des identités non humaines, ainsi que les clés et les tokens non renouvelés.

Modifications apportées à la sécurité dès la conception d'OAG

Classic OIE

Disponible dans Okta Access Gateway. Prise en charge FedRAMP Moderate/High/DOD IL4

La console d'administration OAG sera uniquement accessible sur le réseau local par défaut et forcera la modification du mot de passe administrateur pour la console d'administration et l'interface de ligne de commande destinée à la gestion des administrateurs. Ces changements visent à honorer l'engagement de sécurité dès la conception pris par Okta.



Modifications apportées à la sécurité dès la conception d'OAG

Okta Customer Identity

Early Access

Cohérence entre les requêtes SLO et les IdP externes

Disponible dans tous les SKU || Autorisation FedRAMP Moderate/High/DOD IL4

Renforcez la sécurité des clients Okta Customer Identity (anciennement CIS) qui disposent de terminaux partagés.

OIE

Restrictions réseau pour les tokens

Disponible dans tous les SKU || Autorisation FedRAMP Moderate/High/DOD IL4

Ajoutez des zones spécifiques aux clients sur votre liste d'autorisation afin de réduire le risque d'utilisation abusive des tokens, de protéger les sessions des clients et de défendre les systèmes de back-end contre les attaques DoS et l'épuisement de la limitation du débit.

OIE

Définition de proxys résidentiels comme catégories de services IP

Disponible dans AMFA || Autorisation FedRAMP Moderate/High/DOD IL4

Les zones dynamiques améliorées prennent désormais en charge les proxys résidentiels et les VPN blockchain en tant que catégories de services IP, ce qui permet de bloquer l'accès avant l'évaluation des politiques.

Classic

OIE

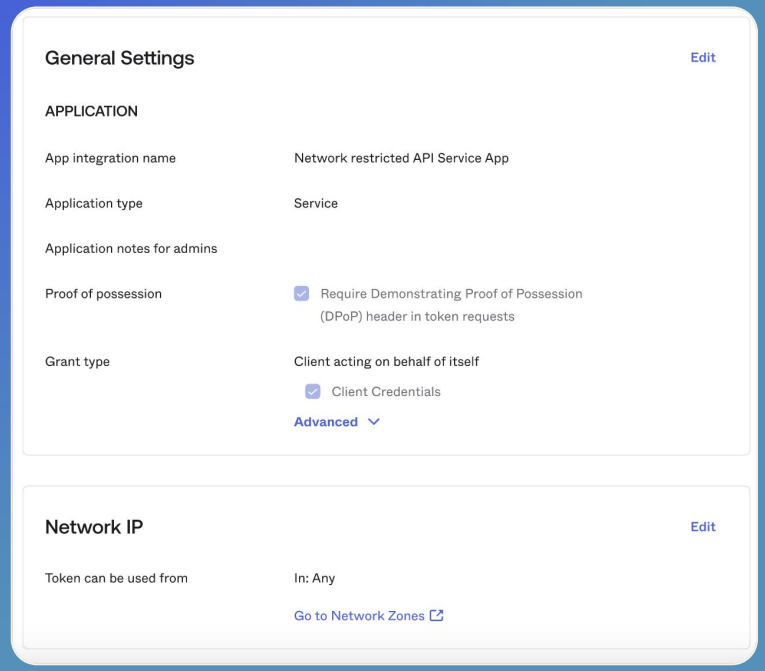
Importations progressives avec DirSync

Disponible dans les intégrations d'annuaires || Autorisation FedRAMP Moderate/High/DOD IL4

Améliorez les importations progressives à partir d'Active Directory pour optimiser la vitesse et l'efficacité des importations, ainsi que réduire les recours à des importations complètes, en vue d'assurer la fluidité des expériences clients.

Classic

OIE



Restrictions réseau pour les tokens

okta

Okta Customer Identity

Early Access

Mise en correspondance des noms pendant la vérification de l'identité

Disponible dans SSO/MFA || Autorisation FedRAMP Moderate/High/DOD IL4

Améliore la précision et l'expérience utilisateur en différenciant clairement les noms légaux et choisis, et en renforçant la confiance et la sécurité lors des workflows d'onboarding, d'authentification, de récupération de comptes et de support.

OIE

Enrichissement du contexte appID pour les applications OIDC et SAML

Disponible dans tous les SKU || Autorisation FedRAMP Moderate/High/DOD IL4

Transmet les détails de l'application (identifiant, nom) aux IdP externes pendant la fédération initiée par Okta (SAML/OIDC), pour une meilleure connaissance situationnelle à la prise de décisions concernant la sécurité et les politiques.

OIE

Redondance des certificats de signature des IdP

Disponible dans tous les SKU ||Autorisation FedRAMP Moderate/High/DOD IL4.

Prenez en charge plusieurs certificats actifs par IdP afin de favoriser une rotation fluide des certificats, en vue de réduire les indisponibilités et les coûts opérationnels tout en renforçant la sécurité.

Classic

OIE

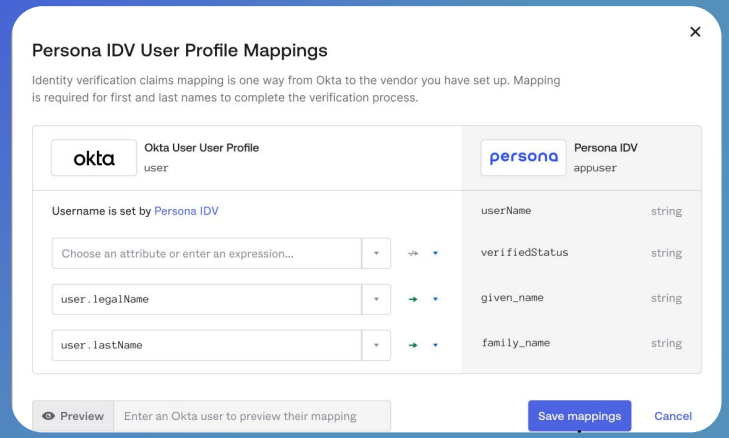
Protection contre les identifiants compromis (phase 2)

Disponible dans tous les SKU

Permet aux administrateurs de personnaliser l'expérience utilisateur et de vérifier les workflows à l'aide de comptes de test, afin de renforcer la sécurité et la confiance opérationnelle.

Classic

OIE



Mise en correspondance des noms pendant la vérification de l'identité

Okta Customer Identity

Early Access

Prise en charge d'Universal Logout pour les applications Okta Customer Identity

Disponible dans tous les SKU || Autorisation FedRAMP Moderate/High/DOD IL4

Intégrez facilement Universal Logout à vos applications Okta Customer Identity (anciennement CIS), sans aucun travail de développement requis.

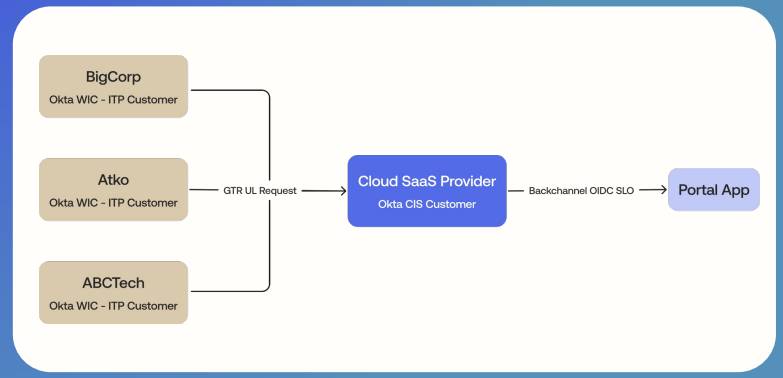
OIE

Gouvernance pour Workflows

Disponible dans Workflows || Prise en charge DOD IL4 pour Okta Identity Governance (OIG). Autorisation FedRAMP High et prise en charge FedRAMP Moderate/DOD IL4 pour Workflows

Tirez parti de la puissance des rôles et des ressources Access Requests et Access Certifications pour Workflows dans OIG afin de simplifier le support client et d'octroyer un accès à durée limitée au moyen de demandes d'accès personnalisées.

OIE



Prise en charge d'Universal Logout pour les applications OCI


okta