リリース概要

2025年第2四半期（4月～6月）の早期アクセス・一般提供について

本資料および本資料に含まれる推奨事項は、法律、プライバシー、セキュリティ、コンプライアンス、またはビジネスに関する助言ではありません。本資料は、一般的な情報提供のみを目的としており、最新のセキュリティ、プライバシー、法律の動向、また関連する問題をすべて反映していないことがあります。本資料の利用者は、自身の責任において、自身の弁護士またはその他の専門アドバイザーから法律、セキュリティ、プライバシー、コンプライアンス、またはビジネスに関する助言を得るものとし、本書に記載された推奨事項に依存すべきではありません。本資料に記載された推奨事項を実施した結果生じるいかなる損失または損害に対しても、Oktaは責任を負いません。Oktaは、これらの資料の内容に関して、いかなる表明、保証、またはその他の保証も行いません。お客様に対するOktaの契約上の保証に関する情報は、okta.com/agreementsをご覧ください。

セーフハーバー

本プレゼンテーションでは、1995年米国私募証券訴訟改革法（Private Securities Litigation Reform Act of 1995）の「セーフハーバー」条項で定義される意味での「将来の見通しに関する記述」について述べられており、これには当社の財務的見通し、事業戦略および計画、市場動向、市場規模、機会、位置付けに関する記述が含まれますが、これらに限定されるものではありません。これらの将来予測に関する記述は、現時点での期待、見積もり、予測、予想に基づいています。「期待する」、「予想する」、「はずである」、「信じる」、「希望する」、「目標とする」、「計画する」、「目標」、「見積もる」、「可能性」、「予測する」、「かもしれない」、「予定する」、「かもしれない」、「可能性がある」、「意図する」、「しなければならない」、およびこれらの用語の活用形や同義、類義表現は、上記の将来的見通しに関する記述を確認することを意図していますが、すべての将来的見通しに関する記述にこれらの識別語が含まれるものではありません。将来予測に関する記述には多くのリスクや不確実性が伴い、その多くには当社が制御できない要因や状況が含まれます。たとえば、世界的な経済状況により、当社製品の需要は過去に減少しており、今後も減少する可能性があります。当社および当社のサードパーティサービスプロバイダーは、過去にサイバーセキュリティインシデントを経験しており、今後もその可能性があります。よって、当社は、過去の期間に経験したビジネスの成長レベルを管理、または維持できない可能性があります。当社の財務的リソースは、当社の競争力を維持、または向上させるのに十分でない可能性があり、それはすなわち、新規顧客の獲得や既存顧客へ製品の継続、販売ができなくなる可能性があるということです。

顧客の伸びは近年鈍化しており、今後も鈍化傾向が継続する可能性があります。つまり、サービス停止など、当社のテクノロジーに関連する中断やパフォーマンスの問題が発生する可能性があります。当社および当社のサードパーティサービスプロバイダーは、適用されるさまざまなプライバシーおよびセキュリティ規定を完全に遵守していない、または遵守していないと見なせるとの指摘を受けた経験があり、今後、同様の事例が発生する可能性があります。そのため当社は、最近の買収や企業結合から期待されるシナジー効果や事業効率を達成できない、買収した企業の統合を成功させることができない、転換社債の償還期限までに償還できない等の可能性があります。当社の業績に影響を与えうる潜在的要因に関する詳細情報は、当社の最新の四半期報告書（Form 10-Q）および証券取引委員会に提出した、その他の書類に記載されています。本プレゼンテーションに含まれる将来予測に関する記述は、本プレゼンテーションの日付時点における当社の見解に過ぎず、当社はこれらの将来予測に関する記述を更新する義務を負わず、また更新する意向もありません。

本資料で参照されている、現時点で一般提供されていない、未取得の、または現在維持されていない製品、製品特性、機能、認定、証明は、予定どおりに提供または取得されない場合、あるいはまったく提供または取得されない場合があります。製品ロードマップは、製品、機能、性能、認証、または証明を提供するという誓約、義務、または約束を示すものではなく、お客様はそれに基づいて購入の決定を行うべきではありません。

© Okta and/or its affiliates. All Rights Reserved.

Oktaは、さまざまな機会を利用して最新のイノベーションと今後の展開をご紹介しています

リリース概要 Webページ

Launch Weekで注目を集めた重要なイノベーションについてさらに掘り下げ、詳細を確認できるリソースはこちら。

営業チームとつながるにはこちら。

Okta製品ロードマップウェビナー

今後の製品リリースを一足先にご覧ください。

Okta製品ロードマップウェビナーには、こちらで登録できます。

リリースハイライト ビデオ + リリースノート

最新の更新内容や機能、改善点について簡単に分かりやすくご紹介します。
ハイライトを見る。

リリースノートはこちら。

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

© Okta and/or its affiliates. All Rights Reserved.

okta

Okta Platformへようこそ
リリース概要

2025年第2四半期

デバイスやAIエージェント、分散環境の増加によってアイデンティティ攻撃対象領域が拡大する中、すべてのアイデンティティの保護がこれまで以上に重要になっています。

今四半期は、その複雑な課題への対処に役立つ新機能が登場します。Okta Workforce Identityの最新の機能拡張で、次のことが可能になります。

- エコシステム全体でデバイスのセキュリティを強化
- ライフサイクル全体で非人間アイデンティティを発見・管理

これらのアップデートによって、プロアクティブでアイデンティティを優先したセキュリティへの取り組みを支援します。なぜなら、アイデンティティはセキュリティの要だからです。

© Okta and/or its affiliates. All Rights Reserved.

概要のナビゲーション

リリース概要は、次のようなコンテンツを含む2つのセクションに分かれています。

Okta Workforce Identity

- Okta Workforce Identityの概要
- スポットライト
- リリース概要
- 開発者向けリソース

Okta Customer Identity

- Okta Customer Identityの概要
- スポットライト
- リリース概要

© Okta and/or its affiliates. All Rights Reserved.

Okta Workforce Identity

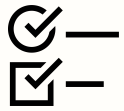
Okta Workforce Identityは、アクセスの決定を自動化し、一貫したポリシーを適用することで、セキュリティ態勢を強化します。このアプローチにより、チームの手作業を減らしてIT運用を簡素化できます。

今四半期のリリースは、この基盤に基づくもので、デバイスやユーザー（AIエージェントを含む）、特権付きリソースなど、最も重要な資産のすべてでガバナンスとセキュリティコントロールを強化します。

スポットライト

Okta Workforce Identity

- 認証前、認証中、認証後のセキュリティ
- Active Directoryアカウント
- Okta AIのアップデートによる Identity Threat Protection
- Cross App Access（AIエージェント向け）
- Okta米国公共部門コンプライアンス ロードマップのアップデート



すべての機能

- Identity Security Posture Management（ISPM）
- アクセス管理
- アイデンティティ管理
- Identity Governance
- Privileged Access
- Platform Services
- Premier Success Plan
- Okta Learning

開発者向けリソース

© Okta and/or its affiliates. All Rights Reserved.

Okta Platformは、アイデンティティセキュリティファブリックを実現

セキュアアイデンティティ製品

ガバナンス
- Okta Identity Governance

態勢管理
- Identity Security Posture Management

Oktaの特権付き管理
- Okta Privileged Access

アクセス管理
- Universal Directory
- シングルサインオン
- Adaptive MFA
- API Access Management
- Okta Access Gateway
- Customer Identity

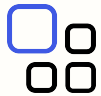
デバイスアクセス
- Okta Device Access

アイデンティティ脅威からの保護
- Identity Threat Protection with Okta AI

セキュアアイデンティティオーケストレーション

安全なアイデンティティ統合

インフラストラクチャ
IaaS  オンプレミスサーバー

アプリケーション
クラウドアプリ  オンプレミスアプリ

API
パブリック  プライベート

アイデンティティ
ディレクトリ  非人間 / AIエージェント

99.99%のアップタイム。月間ログイン数は数百億回以上。計画ダウンタイムなし。

© Okta and/or its affiliates. All Rights Reserved.

okta

スポットライト：認証前、認証中、認証後のセキュリティ

Active Directory アカウント

- 既存のOkta ADエージェントを活用して、特権アカウントを検出
- アクセスポリシーと認証情報の自動ローテーションでADアカウントを保護

Identity Security Posture Managementの強化

- Oktaインスタンス間のマルチテナントアクセス関係とMFAのギャップを視覚化
- アイデンティティエコシステム全体でMFAバイパスとポリシーの弱点を特定

Okta AIの強化による Identity Threat Protection

- 管理者アカウントのセキュリティ強化
- 脅威の検知と対応を環境全体で統一し、リアルタイムに実施

© Okta and/or its affiliates. All Rights Reserved.

早期アクセス

スポットライト：Active Directoryアカウント

Active Directoryアカウントの管理

Active Directory アカウントとは？

この機能では、既存の Okta　ADエージェントを活用したActive　Directory環境への接続や、特権付きADアカウントの検出とそのパスワードの管理、堅牢なアクセスポリシーの作成、すべての管理者とユーザーのアクティビティの監査ができます。

お客様の課題：

一般に、Active　Directoryの特権付きアカウントは管理されておらず、非常に悪用されやすい状態にあります。

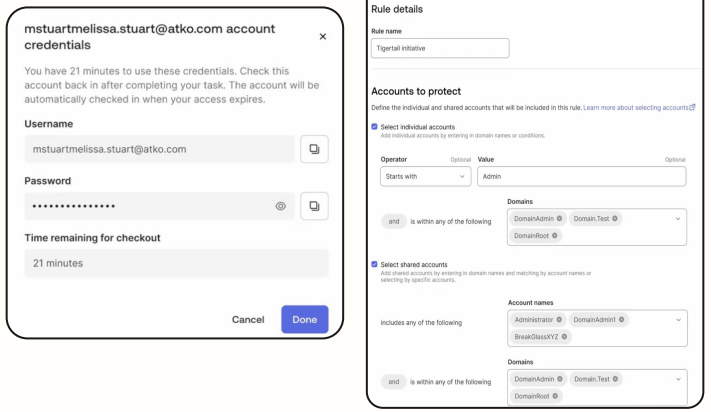
これが重要な理由

コンプライアンスのためにも、セキュリティ態勢の強化のためにも、Active Directoryアカウントを権限のないユーザーから保護する必要があります。ベストプラクティスでは、特権付きアカウントを厳重に管理し、パスワードを定期的にローテーションし、特定のリソースにアクセス可能なユーザーをセキュリティリーダーが把握する必要があるとされています。

入手方法

Okta Privileged Accessで全世界で利用可能です。お客様の環境で機能を有効にするには、CSMまたはAEにご相談ください。

ブログを見る



© Okta and/or its affiliates. All Rights Reserved.

スポットライト:
Okta AIのアップデートによるIdentity Threat Protection

脅威に対する可視性を広げ、技術スタック全体のアクションをリアルタイムで自動化

Identity Threat Protectionとは？

ITPのカスタム管理者ロール - ITP構成を管理するための管理者権限を割り当てることで、最小権限アクセスを適用します。

スーパー管理者ロール向けの ITP検知* - スーパー管理者を標的にした異常な動作を監視、検知して、アカウント乗っ取りの試みを突きとめます。

Palo Alto NetworksとのSSF統合 - アイデンティティシグナルを、Palo Alto NetworkなどのxDRプラットフォームの知見と関連付けることで、検知を向上させ、サイロを削減し、エコシステム全体で組織的なアクションを推進します。

SSFトランスミッター - Oktaのアイデンティティシグナルを使用して、Apple Business Managerなどのサードパーティツールで自動アクション（セッションの無効化、MFAチャレンジなど）をトリガーすることで、インシデント対応ワークフローを加速します。

*Adaptive MFAのお客様にご利用いただけるようになりました

これが重要な理由

これらのアップデートにより、管理者権限の管理を強化し、高い特権を持つアカウントのリスクをさらに詳細に可視化し、環境全体で迅速に先を見越して脅威に対応できるようになります。

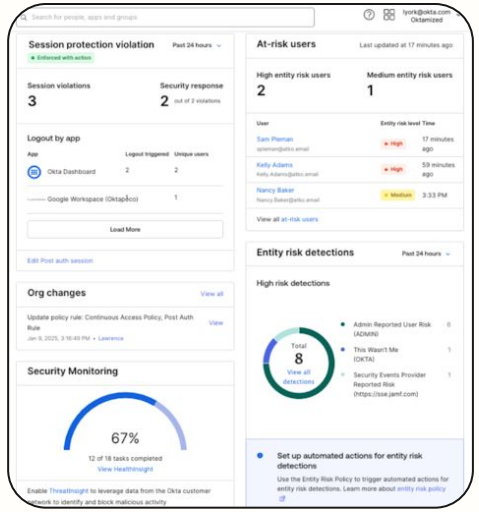
お客様の課題:

管理者への最小権限の適用に苦労している組織が多く、過度な権限を持つロールによって重要な構成が危険にさらされた状態になっています。同時に、スーパー管理者のアクティビティの可視性が十分ではないため、アカウント乗っ取りが検出されないリスクが大きくなっています。アイデンティティシグナルと自動対応機能が統合されていなければ、脅威の検知と対応がばらばらに行われて時間がかかるため、全体的なセキュリティ態勢が弱くなります。

入手方法

- ITPのカスタム管理者ロール、Palo Alto NetworksのSSF統合、SSFトランスミッターは**ITP SKU**で利用できます。
- スーパー管理者ロールのITP検出が、**Adaptive MFA SKU**で利用可能になりました。

詳細を見る



© Okta and/or its affiliates. All Rights Reserved.

スポットライト：Cross App Access（AIエージェント向け）

アプリとAIエージェントの統合の目に見えないレイヤーを保護 – ISVは今すぐ構築を開始可能、
2026年度第3四半期に一部のお客様向けにOktaの機能として提供を開始

Cross App Accessとは？

AIエージェント向けの Cross App Accessは、アプリとAIエージェントの間で信頼できる接続を可能にするプロトコルです。制御と同意を IT管理者に移すことで、IT管理者はどのアプリが接続されているかを判断し、何にアクセスされているかを正確に把握できるようになります。

お客様の課題：

AIエージェントは自主的に動作してタスクを完了させ、意思決定を行い、他のシステムと接続します。許可を求めることはありません。また、AIエージェントは、システム全体に特権付きアクセスの隠れたレイヤーを作っています。そのため新たに差し迫ったセキュリティリスクが引き起こされていますが、従来のアイデンティティツールはそのリスクに対処するように設計されていません。

ISVが導入すべき理由

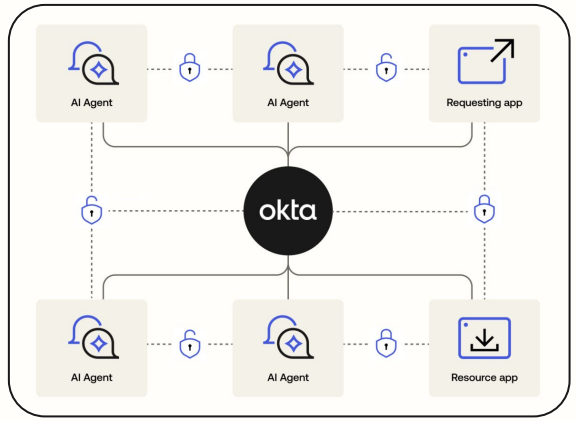
エージェント型 AIのセキュリティを保護するには、ビルダー、アイデンティティプラットフォーム、企業のエコシステムの協力が必要です。そこで、ISVは重要な役割を果たします。

AIエージェントの数が増えて精巧になり、さまざまなシステムでユーザーに代わって行動するようになる中で、AIエージェントが生み出すセキュリティギャップも拡大しています。OktaのCross App Accessは、この新しい現実に最新の監視を提供して、ISVが拡張性のある安全な方法で、自律エージェントとアプリケーションの通信内容を制御できるようにします。そのため、B2B SaaSビルダーは企業の要求を満たしながら、自信を持ってイノベーションを実現できるようになります。

詳細情報

ISVは今すぐ構築を開始できます。顧客早期アクセスは2026年第3四半期に利用可能になります。

- 詳細を見る
- **デジタルイベント「 Identity Summit：エージェント型 AIの保護」にご参加ください**（詳細を見る）



© Okta and/or its affiliates. All Rights Reserved.

スポットライト：Okta米国公共部門コンプライアンスロードマップのアップデート

具体的には？

Oktaの総合プラットフォームは米国公共部門向けに、認証済みで監査に対応した新しいアイデンティティソリューションの提供を開始しました。Identity Governance、Workflows、Threat Protection with Oktaの統合によって、政府機関はアイデンティティ管理のサポートを強化しながら、運用を最新化できます。

お客様の課題：

- モダン化と効率化の目標を目に見える形で達成しながら、同時に厳格なコンプライアンスを実践
- リスクを一定の許容レベル以下に維持
- リソースの制約とスキル不足に対処

これが重要な理由

- Oktaのソリューションが提供する統合プラットフォームで、リアルタイムのサイバーセキュリティ対応とミッションに沿った従業員の生産性を実現できます。
- カスタマイズされたアイデンティティフロー、アクセスパターンに関する継続的なインテリジェンス、比類のない可視性によって、公共部門の組織は脅威を未然に特定して軽減し、運用を合理化して、大きなコスト削減を達成できます。

入手方法

- 発表に関するブログ
- 製品アセスメントのサポートページ
- セルアドオンと同じ製品 SKU
  - Okta for Government Moderate
  - Okta for Government High
  - Okta for US Military

© Okta and/or its affiliates. All Rights Reserved.

Okta Workforce Identityのリリース

Okta Workforce Identityは、ユーザーやデバイスからAIエージェントまで、
すべてのアイデンティティを1つのセキュリティファブリックにまとめます。

最新機能では、このファブリックを拡張して、特権付きADアカウントの強化、セキュリティスタック全体での脅威対策の自動化、管理者に対する最小権限の適用を支援します。

各リリースで利用可能なテクノロジーを、以下で簡単にご確認いただけます*

クラシック | Okta Identity Engine（OIE）

© Okta and/or its affiliates. All Rights Reserved.

***FedRAMP Moderate/High/DOD IL4でサポート:** この製品は期待どおりに機能し、Oktaの公共部門ポートフォリオで完全にサポートされています。
***FedRAMP Moderate/High/DOD IL4認定** :この製品・機能は利用可能で、完全にサポートされており、 FedRAMPまたはDISAの認定を受けています。

Identity Security Posture Management（ISPM）

一般な可用性

非人間アイデンティティ - 可視性とリスク分析

機能：Identity Security Posture Management（ISPM）

リスクの高い主なサービスアカウントや、NHI認証情報を持つ人間のユーザー、ローテーションされていないキーとトークンが検 出・報 告されるため、セキュリティチームは、 NHIによる侵害からの保護に必要な可視性を得ることができます。

クラシック OIE

SFDC AIエージェントの設定ミス

機能：Identity Security Posture Management（ISPM）

SFDC　AIエージェントの危険な設定ミス（過剰な特権付きアクセスや脆弱な認証方法など、不正なデータアクセスやAIエージェントの悪用を可能にする恐れのあるもの）を検出します。

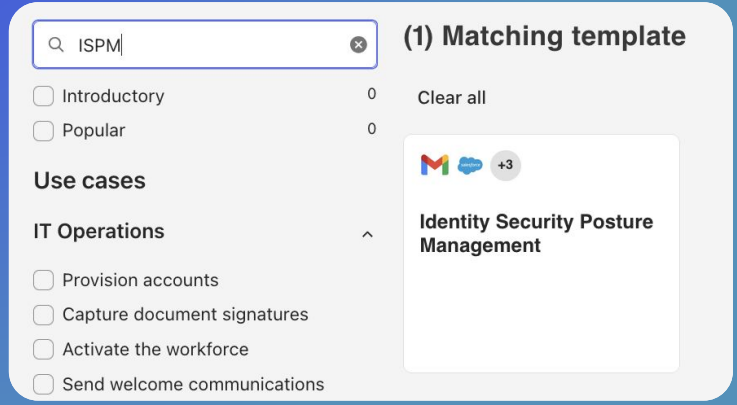
クラシック OIE

自動修復Okta Workflowsテンプレート

機能：Identity Security Posture Management（ISPM）

数回クリックするだけで、お客様が自動修復アクションをトリガーできるようになりました。アカウントの一時停止、パスワードのリセット、MFAの強制または登録などの修復手順を開始する公式ワークフローが、ISPMの機能に加わりました。

クラシック OIE



自動修復 Okta Workflowsテンプレート

© Okta and/or its affiliates. All Rights Reserved.

Identity Security Posture Management（ISPM）

早期アクセス

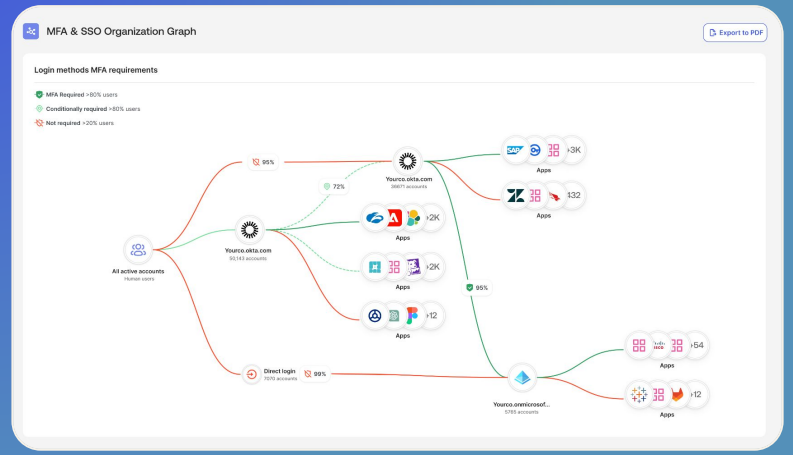
MFAとSSOの分析 - ダッシュボードとグラフ

機能：Identity Security Posture Management（ISPM）

詳細なMFA、要素、SSOの分析をエクスポート可能なダッシュボードで確認できるため、主な傾向とリスクを特定するのに役立ちます。

クラシック

OIE



MFAとSSOの分析 - ダッシュボードとグラフ

© Okta and/or its affiliates. All Rights Reserved.

アクセス管理

一般な可用性

認証方法参照（AMR）クレームマッピング

多要素認証で利用可能。 | FedRAMP Moderate/High/DOD IL4認定

すべての管理者アカウントに MFAが必須であるため、Org2Org管理者は、AMRクレームを使用して、強力なセキュリティを維持しながらユーザーエクスペリエンスを改善できます。

詳細を見る

OIE

Okta Org間でのクレーム共有

すべてのSKUで利用可能。 | FedRAMP Moderate/High/DOD IL4認定

全Okta Orgのリソースへ安全かつシームレスにアクセスできるようにすることで、アイデンティティ連携を強化します。

詳細を見る

クラシック

OIE

Oktaと外部IdP間でのクレーム共有

すべてのSKUで利用可能。 | FedRAMP Moderate/High/DOD IL4認定

セキュリティを損なうことなく、Oktaとサードパーティ IdPのリソースへ安全かつシームレスにアクセスできるようにすることで、アイデンティティ連携を強化します。

詳細を見る：SAML | OIDC

クラシック

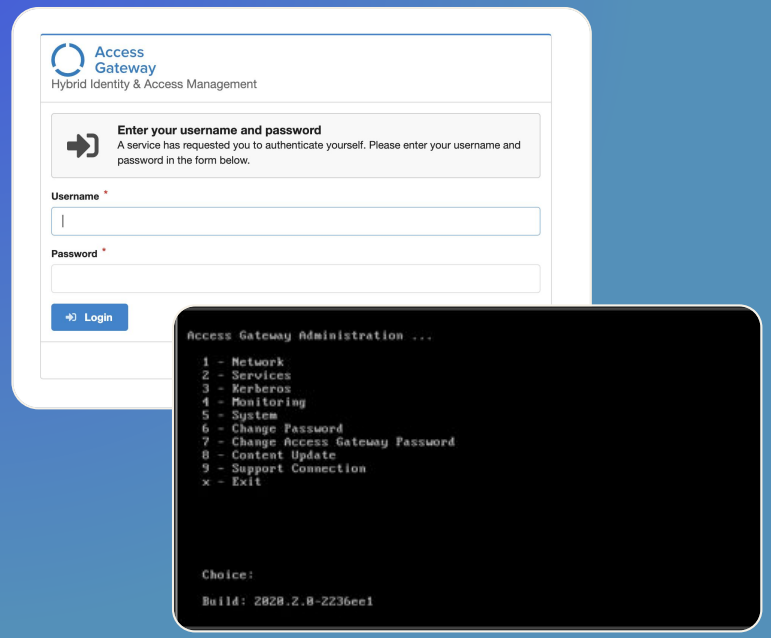
OIE

OAGのセキュアバイデザインな変更

Okta Access Gatewayで利用可能。 | FedRAMP Moderate/High/DOD IL4でサポート

OAG管理コンソールは、デフォルトではローカルネットワーク上でのみアクセス可能で、管理コンソールと管理者管理 CLIのどちらも管理者パスワードの変更を強制するようになります。これらの変更は、Oktaのセキュアバイデザインによる取り組みを遵守するためのものです。

OIE



OAGのセキュアバイデザインな変更

© Okta and/or its affiliates. All Rights Reserved.

アクセス管理

一般な可用性

macOS向けのデスクトップMFA回復

Okta Device Accessで利用可能。 | FedRAMP Moderate/High/DOD IL4認定

電話やセキュリティキーなどを紛失した場合でも、管理者がエンドユーザーに時間制限付きの復旧コードを安全に提供し、デバイスへのログインを可能にすることで、生産性の中断を防ぎます。

詳細を見る

OIE

アサーションとトークンクレームのエンタイトルメント

Okta Identity Governance（OIG）で利用可能。 | DOD IL4でサポート

管理者がSAMLアサーション属性とOpenID Connectトークンでカスタムクレームを構成できるようになったため、最小権限を適用してグループへの依存を減らすことができます。

詳細を見る

クラシック

OIE

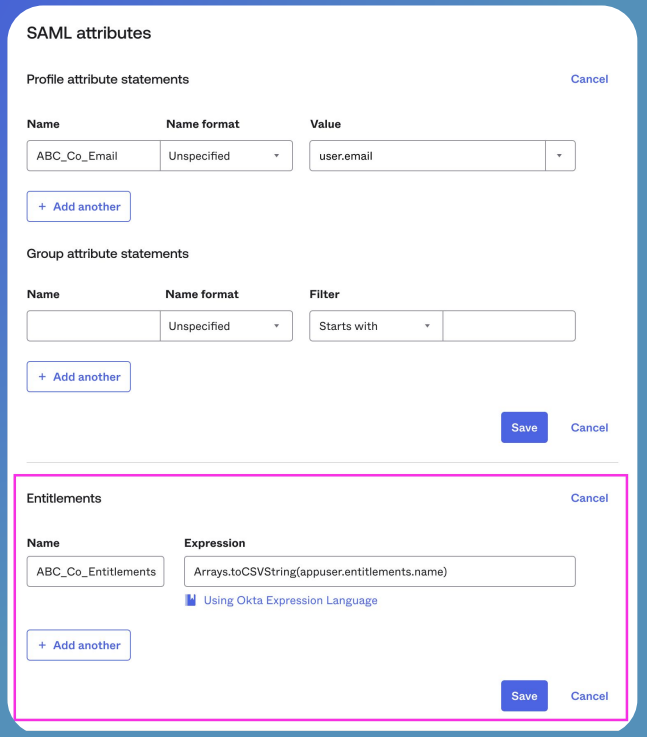
アイデンティティプロバイダーにアクセスするためのきめ細かい管理者許可

Okta Identity Engine（OIE）で利用可能。 | FedRAMP Moderate/High/DOD IL4認定

きめ細かな管理者権限を使用して、管理者が特定の IdPを他の管理者に割り当てられるようになりました。権限のあるユーザーにのみ IdPの構成へのアクセスを許可することで、セキュリティ態勢を改善できます。

クラシック

OIE



アサーションとトークンクレームのエンタイトルメント

© Okta and/or its affiliates. All Rights Reserved.

アクセス管理

一般な可用性

ポリシーの更新を保護されたアクションにする

すべてのSKUで利用可能。 | FedRAMP Moderate/High/DOD IL4認定

管理コンソールでアプリサインオンポリシー、グローバルサインオンポリシー、ITPポリシー、アカウント管理ポリシーを更新する際、管理者は、ステップアップ認証の完了を求められます。これによって、攻撃者に管理セッションにアクセスされたとしても、更新されることは防げます。

クラシック OIE

Okta Verifyの同一デバイス登録

すべてのSKUで利用可能。 | FedRAMP Moderate/High/DOD IL4認定

デスクトップとモバイルデバイスで Okta VerifyとFastPassのエンドユーザーエンロールメントフローを改善します。

クラシック OIE

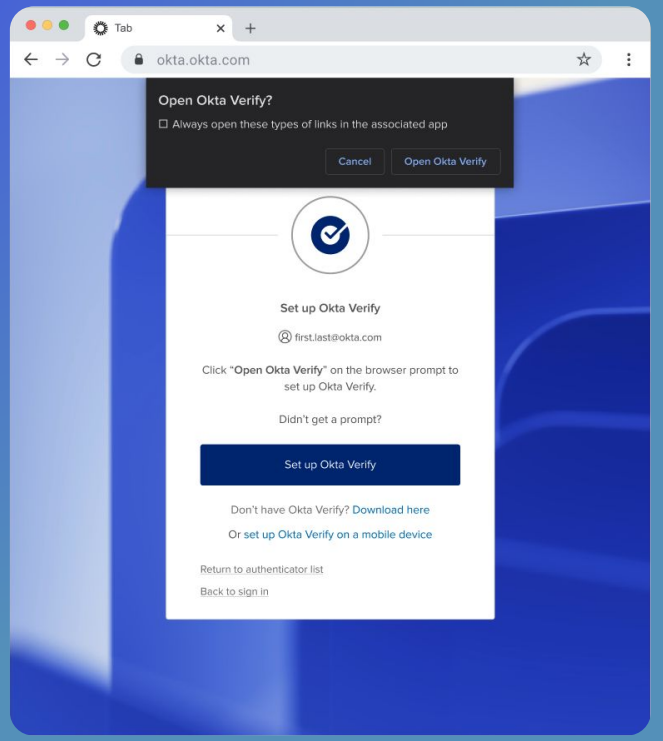
iOS向けOkta Verifyトラブルシューター

すべてのSKUで利用可能。 | FedRAMP Moderate/High/DOD IL4認定

ユーザーが Okta Verifyアプリ内でプッシュ通知と FastPassの問題をトラブルシューティングできるようになります。

詳細を見る

クラシック OIE



Okta Verifyの同一デバイス登録

© Okta and/or its affiliates. All Rights Reserved.

アクセス管理

早期アクセス

Advanced Posture Checks

AMFAで利用可能。 ‖ FedRAMP Moderate/High/DOD IL4認定

WindowsやmacOSの任意のデバイス属性やセキュリティ設定からデバイスコンテキストを収集して評価できるため、認証中のゼロトラストセキュリティをさらに強化できます。

詳細を見る

OIE

Android Device Trustによるデバイス保証

AMFA/ASSOで利用可能。 ‖ FedRAMP Moderate/High/DOD IL4認定

デバイス保証ポリシーの一環として、Androidでさまざまな追加のデバイスチェックを適用します。

詳細を見る

OIE

OIDC/SAMLアプリケーション向けにappIDコンテキストを拡張

すべてのSKUで利用可能。 ‖ FedRAMP Moderate/High/DOD IL4認定

Oktaが開始するフェデレーション（SAML/OIDC）中にアプリケーションの詳細（ID、名前）を外部IdPに渡し、IdPでのセキュリティとポリシーの決定を強化します。

クラシック

OIE

侵害された認証情報の保護（フェーズ2）

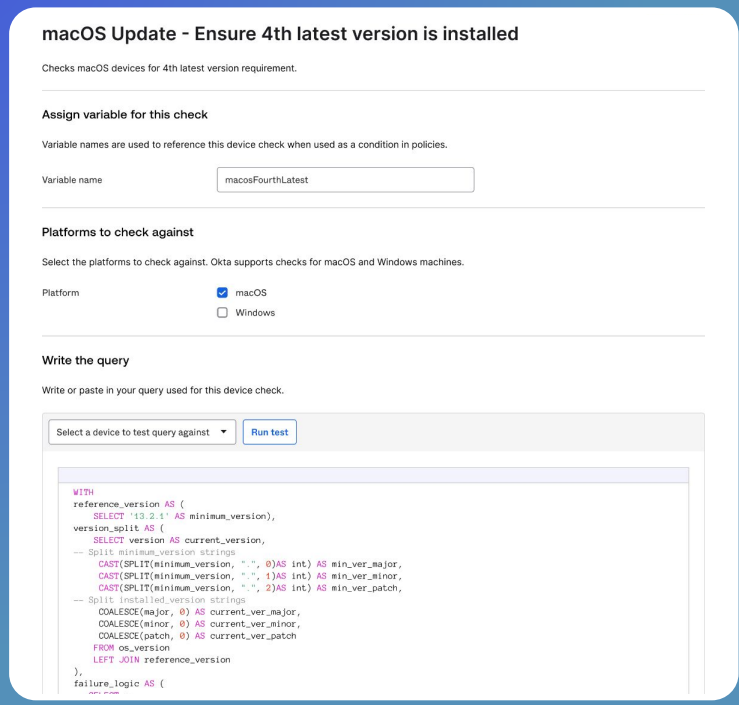
すべてのSKUで利用可能。

侵害された認証情報のイベントへの対応をカスタマイズ可能で、管理者がテストアカウントを使用して、侵害された認証情報フローを検証できます。

詳細を見る

クラシック

OIE



Advanced Posture Checks

© Okta and/or its affiliates. All Rights Reserved.

アクセス管理

早期アクセス

カスタムFIDO2 AAGUID

MFA/AMFAで利用可能。 FedRAMP Moderate/High/DOD IL4認定

FIDO2（WebAuthn）グループで使用するために、承認された AAGUIDベースの認証者（ブラウザーのパスワードマネージャーなど）を追加できるようになります。

クラシック OIE

IPサービスカテゴリとしてのレジデンシャルプロキシ

AMFAで利用可能。 FedRAMP Moderate/High/DOD IL4認定

拡張動的ゾーンが、IPサービスカテゴリとしてレジデンシャルプロキシとブロックチェーン VPNをサポートするようになったため、組織はポリシー評価の前にアクセスをブロックできるようになります。

詳細を見る

クラシック OIE

ID検証の名前の一致

SSO/MFAで利用可能。 FedRAMP Moderate/High/DOD IL4認定

正当な名前と優先される名前を区別しながら、 ID検証中に検証可能なクレームマッピングを実行します。

詳細を見る

OIE

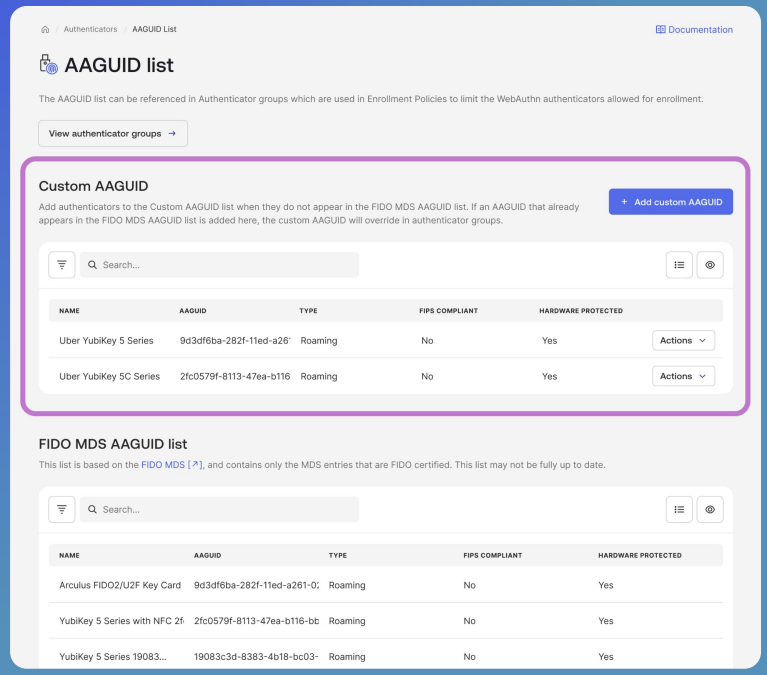
Microsoft EAMサポート（外部認証方式）

MFA/AMFAで利用可能。 FedRAMP Moderate/High/DOD IL4認定

Entra IDで保護されたアプリケーションにユーザーがアクセスする際に、 Oktaを使用してMFAなどの保証要件を満たすことができます。

詳細を見る

OIE



カスタムAAGUID

© Okta and/or its affiliates. All Rights Reserved.

okta

アクセス管理

早期アクセス

トークンエンドポイントのネットワーク制限

すべてのSKUで利用可能。 | FedRAMP Moderate/High/DOD IL4認定

クライアントごとにネットワークゾーンを許可リストに登録して、トークンリクエストを信頼できる IP に制限し、反射攻撃やトークン窃取、DoS、レート制限の過剰使用から保護することで、セキュリティを強化します。

詳細を見る

OIE

OAGの自動更新

Access Gatewayで利用可能。 | FedRAMP Moderate/High/DOD IL4でサポート

お客様が自動更新を有効にして、OAGデプロイメントで必ず最新バージョンが実行されるようにできます。

詳細を見る

OIE

IdP署名証明書の重複

すべてのSKUで利用可能。 | FedRAMP Moderate/High/DOD IL4認定

IdPごとに複数のアクティブな署名証明書に対応できるため、セキュリティを向上させながら、シームレスな証明書のローテーションや、ダウンタイムの短縮、運用オーバーヘッドの削減が可能になります。

詳細を見る

クラシック

OIE

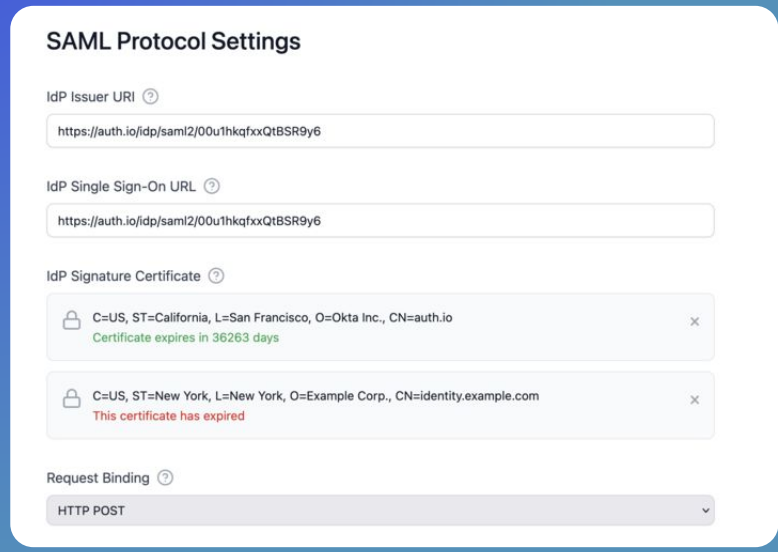
Okta Customer IdentityアプリのUniversal Logout対応

すべてのSKUで利用可能。 | FedRAMP Moderate/High/DOD IL4認定

Universal LogoutをOkta Customer Identity（旧CIS）アプリに簡単に統合できます。開発作業は一切必要ありません。

詳細を見る

OIE



IdP署名証明書の重複

© Okta and/or its affiliates. All Rights Reserved.

アクセス管理

早期アクセス

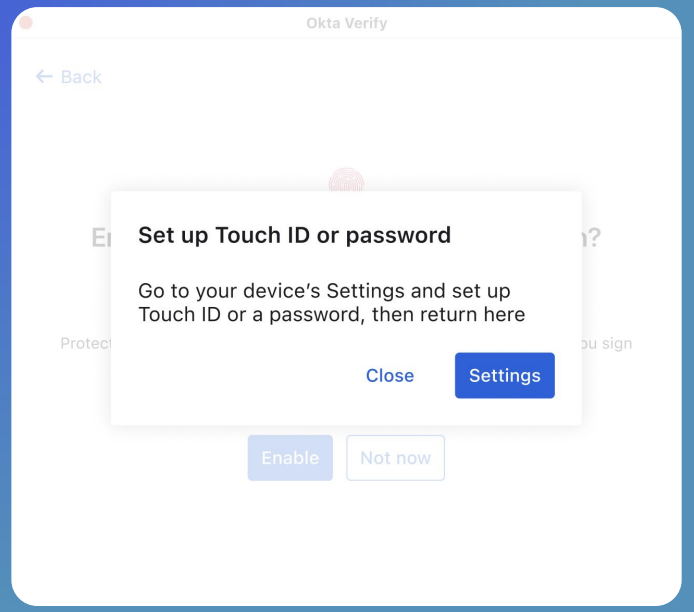
ユーザー確認の修復

MFA/AMFAで利用可能。 FedRAMP Moderate/High/DOD IL4認定

ユーザー確認を有効化またはステップアップして認証ポリシーの要件を満たすようエンドユーザーをガイドします。

クラシック

OIE



ユーザー確認の修復

© Okta and/or its affiliates. All Rights Reserved.

ID 管理

一般な可用性

LDAPエージェントのエンドツーエンド暗号化

ディレクトリ統合で利用可能。 | FedRAMP Moderate/High/DOD IL4でサポート

セキュリティのレイヤーを追加し、LDAPエージェント設定ファイルを監視したり、OktaとLDAPエージェント間の各ペイロードをメッセージレベルで暗号化したりします。

クラシック
OIE

エンタイトルメント管理のためのOINアプリ - Splunk、Zoho Mail

Okta Identity Governance（OIG）で利用可能。 | DOD IL4でサポート

Splunk、Zoho Mail、Crowdstrike、Oracle IAMの4つのOINアプリとすぐに統合し、バンドル、ポリシー、ルールを使用して Okta内でエンタイトルメントを検出、インポート、保存、管理できます。

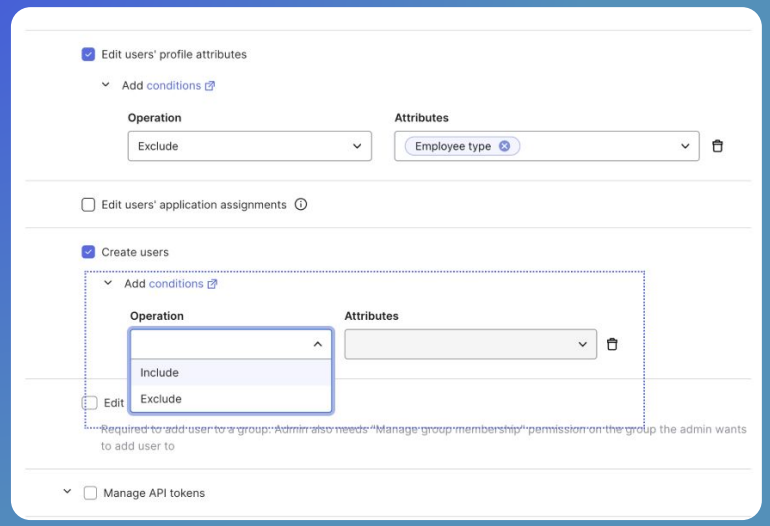
クラシック
OIE

ユーザー作成の権限条件

カスタム管理者ロール、Secure Partner Accessの機能 / Secure Partner Accessで利用可能。 | FedRAMP Moderate/High/DOD IL4認定

委任された管理者またはパートナー管理者が、重要なシステムへのアクセスを意図せずに許可する可能性のある機密性の高い属性値（ロールや部門など）を割り当てるのを防ぎます。適切な管理者のみが、認証に関連するアイデンティティ属性を設定できるようになるため、属性ベースのアクセスコントロールポリシーを適用するのに役立ちます。特に管理を委任している環境で、ユーザーのオンボーディング中に設定ミスが発生するリスクを軽減します。

クラシック
OIE



ユーザー作成の権限条件

© Okta and/or its affiliates. All Rights Reserved.

アイデンティティ管理

早期アクセス

DirSyncによる増分インポート

ディレクトリ統合で利用可能。 | FedRAMP Moderate/High/DOD IL4認定

Active Directoryからの増分インポートが進歩して、インポートがより高速で効率的になるため、フルインポートに頼る場面を減らすことができます。

詳細を見る

クラシック
OIE

Oracle EBS用のオンプレミスコネクター

Okta Identity Governance（OIG）で利用可能。 | DOD IL4でサポート

オンプレミスアプリケーションのアイデンティティガバナンスを簡素化し、レガシーシステムと最新のアプリケーションスタックを橋渡しして、セキュリティの強化、シームレスな自動化、コンプライアンスを実現します。

詳細を見る

クラシック
OIE

DirSyncによる増分インポート

© Okta and/or its affiliates. All Rights Reserved.

Identity Governance

一般な可用性

Access Requestの使いやすさ向上と新デザイン

クラシック OIE

Access Governanceで利用可能。 DOD IL4でサポート

Oktaのファーストパーティアプリ全体で UIに一貫性があるため、操作が容易になります。新デザインのインクルーシブなレイアウトでアクセシビリティ 対 応 をサポートします。使い慣れたOktaのデザインパターンに合わせることで、ユーザーの手間を軽減できます。

詳細を見る

新しいLCM/Okta Identity Governance（OIG）の統合

クラシック OIE

すべてのSKUで利用可能。LCMはFedRAMP Moderate/High/DOD IL4認定、OIGはDOD IL4でサポート

より多くの人事システムや一般的なアプリケーション（ Splunk）と統合し、ユーザー、グループ、エンタイトルメントを管理します。

詳細を見る

リソースコレクション

クラシック OIE

Okta Identity Governance（OIG） - Access Governanceで利用可能。 DOD IL4でサポート

複数のアプリやグループをパッケージ化することでエンタイトルメント管理を合理化し、ユーザーが適 切 なアクセス 権 を 迅 速 かつ 効 率 的 に 受 け 取 れるようにすると 同 時 に、要求と承認者にとっての複雑さを軽減します。

詳細を見る

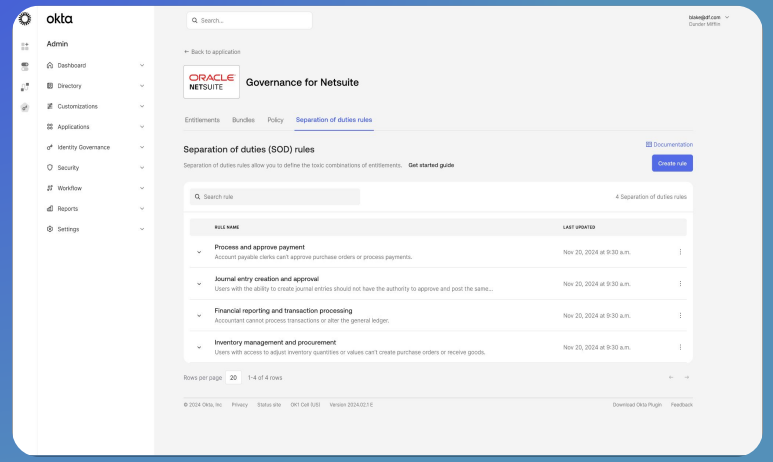
職務の分離

クラシック OIE

Okta Identity Governance（OIG） - Access Governanceで利用可能。 DOD IL4でサポート

エンタイトルメントの有害な組み合わせを定義するルールを作成し、認定キャンペーンを実行して、ユーザーに対して存在する有害な組み合わせを修正します。

詳細を見る



職務の分離

© Okta and/or its affiliates. All Rights Reserved.

Privileged Access

早期アクセス

Active Directoryアカウント

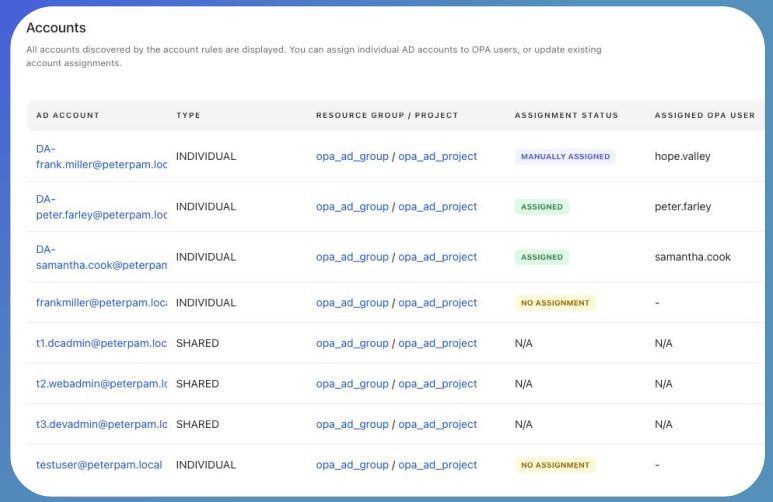
Okta Privileged Accessで利用可能

運用の複雑さを増やすことなく、特権付き Active Directoryアカウントのパスワードを管理できます。既存の Okta Active Directoryエージェントを使用して、ADアカウントの検出、アクセスポリシーの作成、認証情報のローテーションの自動化、すべての管理者とユーザーのアクティビティの監査を行います。

詳細を見る

クラシック

OIE



Active Directoryアカウント

© Okta and/or its affiliates. All Rights Reserved.

Platform Services

一般な可用性

アクセシビリティACR

アセスメント：VPATSは、FedRAMP Moderate/High/DOD IL4など、すべてのOkta環境に対応

お客様向け製品のアクセシビリティの現状を可視化します。また、特に　FedとSledのお客様の法的要件とコンプライアンス要件を満たすのにも役立ちます。

詳細を見る

クラシック OIE

動的リソースセット

すべてのSKUで利用可能。‖FedRAMP Moderate/High/DOD IL4認定

お客様が機密性の高いリソースへのアクセスを少数の管理者に指定できるようになります。

詳細を見る

クラシック OIE

新しいWorkflowsコネクター

Workflowsで利用可能。‖FedRAMP High認定、FedRAMP Moderate、DOD IL4でサポート

より多くのOkta APIや一般的なアプリケーション（ Coupa、Splunk）と統合して、ユーザーとグループを管理できます。

詳細を見る

クラシック OIE

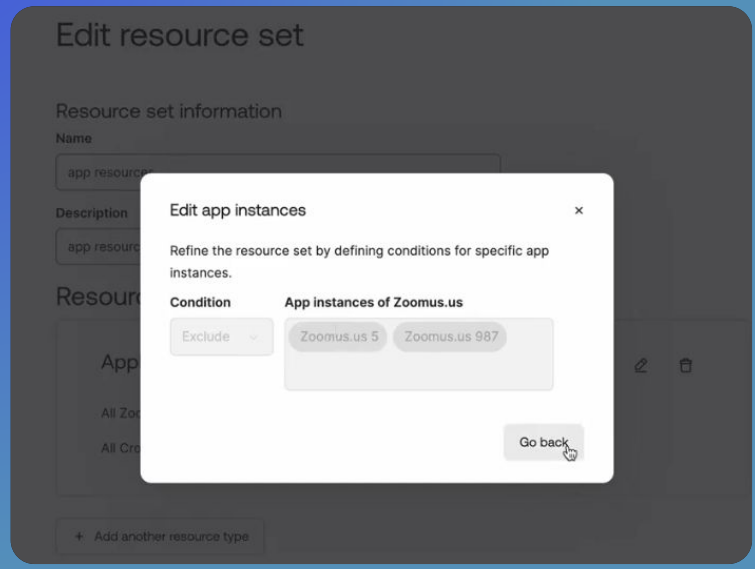
Workflows向けOkta ITPコネクター

Workflowsで利用可能。‖FedRAMP High認定、FedRAMP Moderate、DOD IL4でサポート

Okta ITPコネクターを使用して、ITPイベントのデバッグや監査と、ユーザーリスクレベルの作成や更新ができます。

詳細を見る

クラシック OIE



動的リソースセット

© Okta and/or its affiliates. All Rights Reserved.

Platform Services

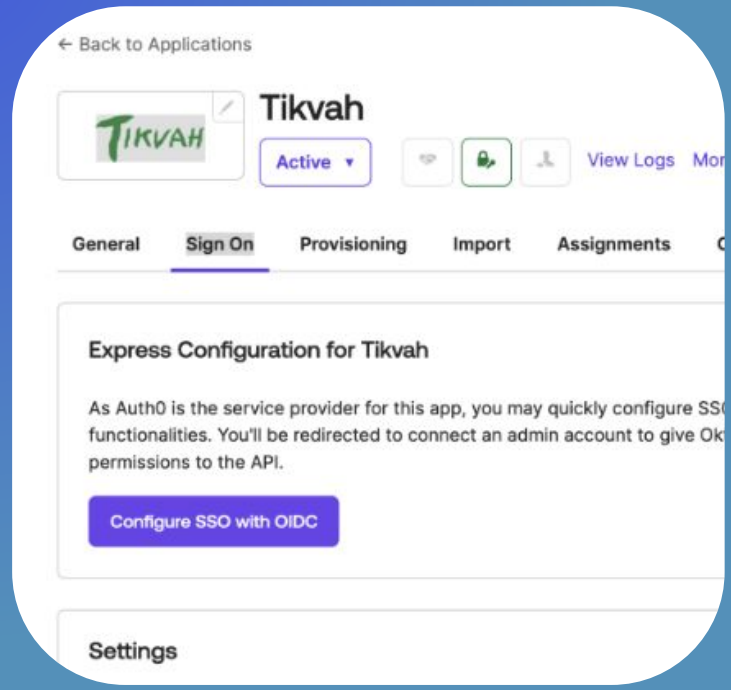
一般な可用性

Oktane ISVバンドルの機能：エクスプレス構成

すべてのSKUで利用可能。

エクスプレス構成を使用すると、エンタープライズのお客様は、OINカタログで公開されているAuth0対応のOIDCアプリのインスタンスをOkta orgにすばやく追加できます。このプロセスでは、OktaとAuth0間の自動データ共有を使用します。

OIE



エクスプレス構成

© Okta and/or its affiliates. All Rights Reserved.

Platform Services

早期アクセス

Workflowsのガバナンス

Workflowsで利用可能。Okta Identity Governance（OIG）はDOD IL4でサポート。WorkflowsはFedRAMP High認定、FedRAMP Moderate/DOD IL4でサポート

OIG Access RequestsとWorkflowsのロールとリソースの認定機能を活用して、ロールの割り当てを合理化し、カスタマイズされたアクセスリクエストの期限付きのアクセス権を付与できます。

OIE

ISVバンドル：プログラムのアクティブ化

Okta Platform（Okta Integration Network）で利用可能。

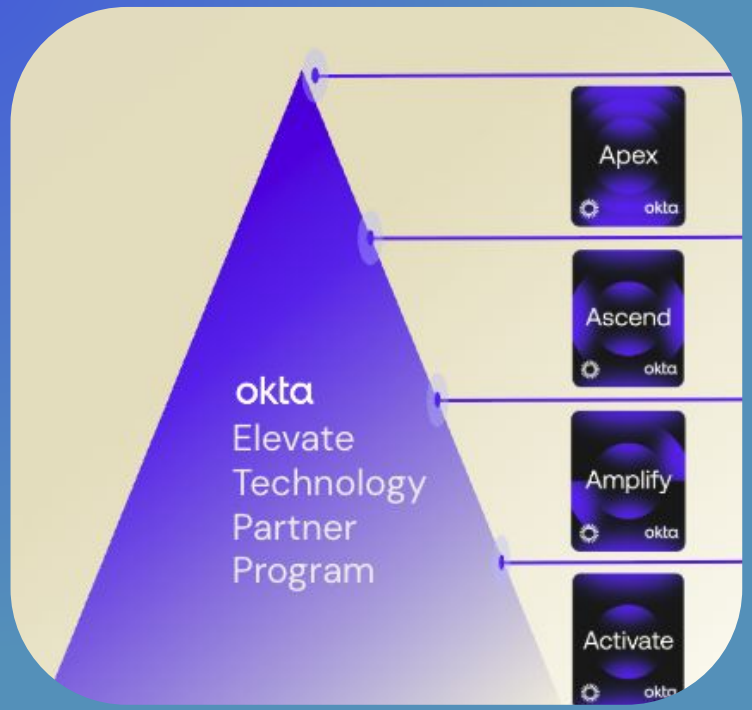
ISVが、SSOとLCMの統合を構築、公開、保守するだけで、Oktaによる可視性、有効化サポート、セルフサービスマーケティングのメリットを活用できるようにするプログラムです。

詳細を見る

ISVバンドル：secureintegrations.dev

すべてのSKUで利用可能。

標準に重点を置いたマイクロサイトで、すでに承認されている IPSIEレベルを含めた更新情報など、正確な構築方法を開発者に案内します。



プログラムのアクティブ化

© Okta and/or its affiliates. All Rights Reserved.

Premier Success Plan

一般な可用性

アイデンティティ成熟度のチェックリスト

Silver Premier Success Planで利用可能

選択したビジネス目標と最近の導入データに基づいてアイデンティティ成熟度を高める方法を説明したセルフサービス式のステップバイステップのチェックリスト、および追加のイベントと教育リソース。

詳細を見る

OIE

アイデンティティ成熟プラン

Gold Premier Success Planで利用可能

選択したビジネス目標と最近の導入データに基づいた、アイデンティティ成熟度を高めるためのパーソナライズされた推奨事項、およびオンデマンドのアクティブ化測定基準、 CSMとのコラボレーション、Okta学習パスの推奨、その他の教育リソース。

詳細を見る

OIE

エキスパートラーニングパス

Silver/Gold Premier Success Planで利用可能

限定のオンデマンドカタログや、専門家によるライブ学習セッション、認定バウチャーを利用できます。シルバーのお客様にはエキスパートラーニングパスが 1枚、ゴールドのお客様にはエキスパートラーニングパスが 6枚提供されます。

詳細を見る

クラシック

OIE

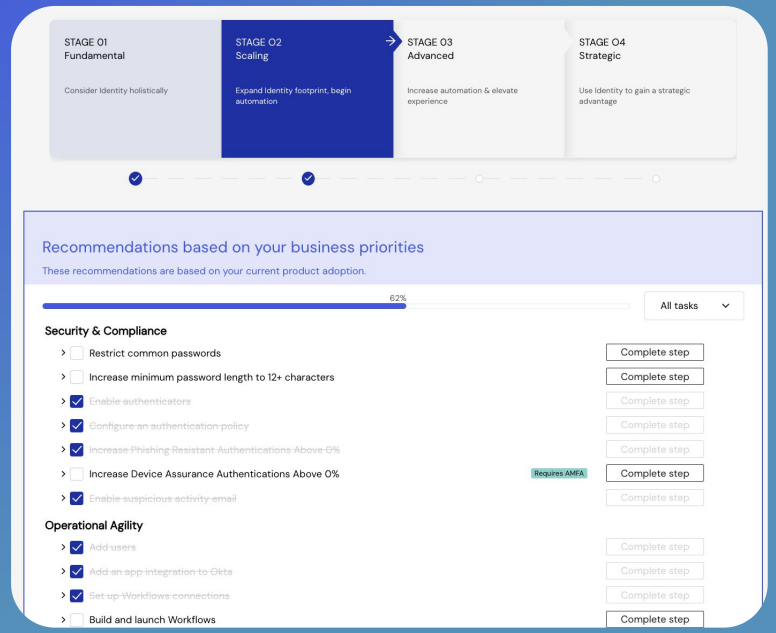
専任のテクニカルアカウントマネージャー

Gold Premier Success Planのアドオンとして利用可能

お客様の製品とアーキテクチャについて広範な知識を持つテクニカルアドバイザーが、お客様に合わせた導入と最適化の長期的戦略を提供します。

クラシック

OIE



アイデンティティ成熟度のチェックリスト

© Okta and/or its affiliates. All Rights Reserved.

Okta Learning

一般な可用性

セキュリティシリーズI- 新しいOSICコース

クラシック

OIE

公開カタログで利用可能

アイデンティティの設定ミスは、攻撃者や不注意な内部関係者にとって侵入口となるため、最初から正しいアイデンティティ構成にすることが重要です。このプランでは、 OktaのSecure Identity Commitment（OSIC）の一環として主な重点領域と守るべきベストプラクティスを示します。

詳細を見る

新しいOktaスキルバッジ - デバイスのセキュリティと管理の最適化

OIE

公開カタログで利用可能

Oktaがさまざまなデバイス管理ソリューションと統合して、デスクトップとモバイルデバイスを保護・管理する方法をご紹介します。それぞれに合わせたセキュリティ構成と詳細な認証プロセスによって、デバイスのセキュリティを強化し管理タスクを効率化して、より安全で生産性の高い職場を実現します。

詳細を見る

新しいOktaスキルバッジ！アイデンティティを意識した統合によるBYODの管理

OIE

公開カタログで利用可能

Oktaのアイデンティティを優先したアプローチを活用してプラットフォーム固有のBYOD（Bring Your Own Device：自分のデバイスを持ち込むこと）戦略を実装することで、組織のモバイルセキュリティ環境を変革し、企業データとユーザーのプライバシーの両方を保護します。さらに、パスを修了すると Oktaスキルバッジを獲得できます。

詳細を見る

新規：ThreatInsightを使用して脅威を軽減 - セキュリティシリーズI

© Okta and/or its affiliates. All Rights Reserved.

開発者向けリソース

Okta Workforce Identity

Oktaを使用すると、ユーザーに好まれるエクスペリエンスを構築・統合・提供できます。最新リリースのアップデート、厳選されたガイド、ビルドに関するコミュニティからのフィードバックをご覧ください。

リソース

Oktaアーキテクチャセンター: こちらをクリック

エンタープライズ対応ワークショップ: こちらをクリック

開発者ブログ: こちらをクリック

言語とSDK: こちらをクリック

スタートガイド: こちらをクリック

リリースノート: こちらをクリック

Okta開発者コミュニティフォーラム: こちらをクリック

Oktaコミュニティツールキット - アプリSHOWCASE: こちらをクリック

OktaDev YouTubeチャンネル: こちらをクリック

© Okta and/or its affiliates. All Rights Reserved.

okta

Okta Customer Identityのリリース

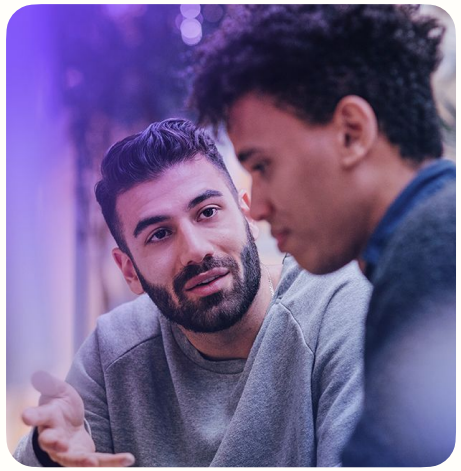
Okta Customer Identityは、シームレスなデジタルエクスペリエンスを提供する上で、セキュリティを最優先することを保証します。このサービスによって、組織は成長を加速し、変化するセキュリティ課題に対処し、顧客とビジネスデータを保護することができます。

最新リリースの詳細をご覧ください。

© Okta and/or its affiliates. All Rights Reserved.

Okta Customer Identityは、現在だけでなく将来のアイデンティティニーズにも応えます

Okta Customer Identity は数千のお客様を支えています



さまざまな業界の IT・セキュリティチーム向け

シームレスなユーザーエクスペリエンスを促進する設計

高度なセキュリティ機能による可視化で、攻撃を検出・対応

© Okta and/or its affiliates. All Rights Reserved.

一般な可用性

スポットライト：Okta Customer Identity

アイデンティティセキュリティファブリックを顧客とパートナーに拡張

Okta Customer Identity とは？

Okta Customer Identity（OCI）は、信頼できるアイデンティティのセキュリティと管理の機能を、従業員向けの使用から顧客やパートナー、市民などの外部ユーザーに拡張します。外部のアイデンティティを大規模に管理し保護するために設計されたこの総合 プラットフォームは、デジタルアプリへのシームレスで安全なアクセスを提供しながら、ユーザーエクスペリエンスを向上します。

お客様の課題：

多くの組織では、従業員と外部ユーザー向けにばらばらのアイデンティティソリューションを使用しているため、運用の複雑さ、セキュリティのギャップ、一貫性 のないユーザーエクスペリエンスにつながっています。従業員、顧客、パートナー用に別々のアイデンティティシステムを運用すると、サイロの発生や攻撃対象領域の拡大につながり、デジタルトランスフォーメーションの取り組みの妨げとなります。

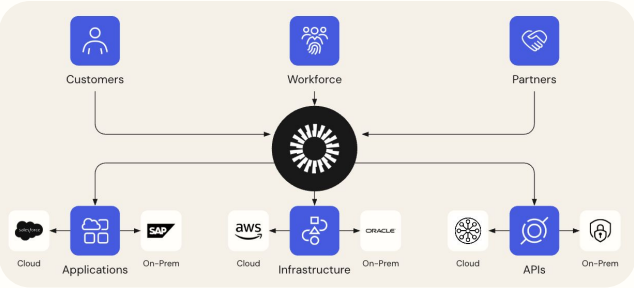
これが重要な理由

- **統 合 アイデンティティプラットフォーム：** OCIを使用すると、従業員と顧客のアイデンティティ管理を単一の統合 Oktaプラットフォームに集約できます。そのため、複雑さを軽減し、運用を合理 化 できるほか、すべてのアイデンティティの全体像を把握できるため、セキュリティ態勢とコンプライアンスを向上することが可能です。
- **リスクの軽減とセキュリティの強化：** 信頼性の高 いOktaのアイデンティティセキュリティファブリックを顧客やパートナーに拡張することで、堅牢な認証と脅威検知を活用して、デジタルエコシステム全体のリスクを最小限に抑えられます。
- **ユーザーエクスペリエンスと信頼性の向上：** 従業員、顧客、パートナーを問わず、すべてのユーザーに一貫性があり、安全で、手間のないエクスペリエンスを提供します。その結果、信頼の構築、ロイヤルティの醸成、デジタルサービスへのエンゲージメント向上を実現できます。

入手方法

固有のニーズを検討したうえで、Okta Customer Identityで貴社がどのようなメリットを得られるかを確認するには、Oktaの担当者または営業チームにご連絡ください。

詳細を見る



© Okta and/or its affiliates. All Rights Reserved.

早期アクセス

スポットライト：侵害された認証情報の保護

クレデンシャルスタッフィングとアカウント乗っ取りを未然に防ぎます。

侵害された認証情報の保護とは？

継続的に更新される、侵害された既知の認証情報に関するサードパーティのデータセットと、ユーザーのパスワードを自動的に照合します。この予防的な対策によって、他の場所で侵害が発生した場合でも、データ侵害でユーザーのパスワードが漏えいすると特定できます。

お客様の課題：

データ侵害が頻繁に発生する時代に、クレデンシャルスタッフィングやアカウント乗っ取り（ATO）攻撃は脅威として蔓延しています。組織は、ユーザーの認証情報がインターネット上の他の場所で侵害された場合の検出に苦労しており、盗んだ認証情報を再利用してシステムに不正アクセスする攻撃者に対して脆弱になっています。

これが重要な理由

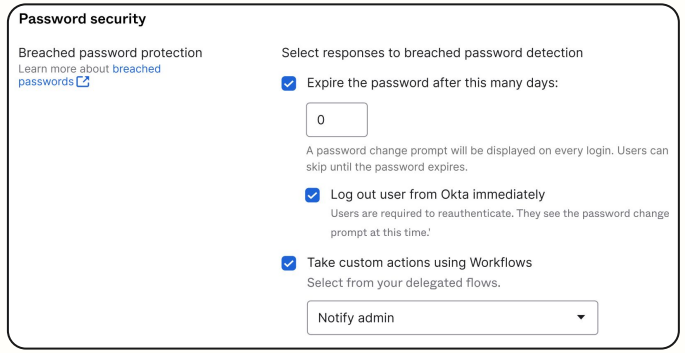
- **予防的な脅威防御**：侵害されたパスワードが悪用される前に特定することで、クレデンシャルスタッフィングやアカウント乗っ取り攻撃のリスクを自動的に検出して軽減し、ユーザーとデータを保護します。
- **カスタマイズ可能なセキュリティポリシー**：管理者はきめ細かな制御を行って、認証情報の侵害が検出された場合に取る特定の対応を設定できます。これによって、パスワードのリセット要求や追加の認証要求など、自社に合わせたセキュリティアクションが可能になります。
- **セキュリティ態勢の強化**：最も一般的な攻撃ベクトルの1つに対して重要な防御レイヤーを追加することで、全体的なセキュリティ態勢を改善します。そのため、不正アクセスを防ぎ、データ侵害の可能性を減らすことができます。

入手方法

この機能は早期アクセスで利用可能です。

固有のニーズを検討したうえで、Okta Customer Identityで貴社がどのようなメリットを得られるかを確認するには、Oktaの担当者または営業チームにご連絡ください。

詳細を見る



© Okta and/or its affiliates. All Rights Reserved.

okta

Okta Customer Identity

一般な可用性

Oktaと外部IdP間でのクレーム共有

すべてのSKUで利用可能。‖FedRAMP Moderate/High/DOD IL4認定

Oktaサービスプロバイダーで外部 IdPからの信頼できるクレームを受け入れて検証することで、強力なセキュリティを維持しながらユーザーエクスペリエンスを向上できます。

クラシック
OIE

Okta Org間でのクレーム共有

すべてのSKUで利用可能。‖FedRAMP Moderate/High/DOD IL4認定

全Okta Orgのリソースへ安全かつシームレスにアクセスできるようにすることで、アイデンティティ連携を強化します。

クラシック
OIE

新しいWorkflowsコネクター

Workflowsで利用可能。‖FedRAMP High認定、FedRAMP Moderate、DOD IL4でサポート

より多くの Okta APIや一般的なアプリケーション（ Coupa、Splunk）と統合して、ユーザーとグループを管理できます。

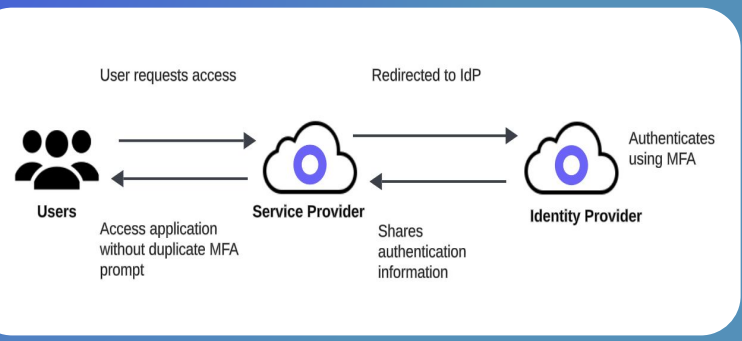
クラシック
OIE

ユーザー作成の権限条件

カスタム管理者ロール、Secure Partner Accessの機能 / すべてのSKUで利用可能。‖FedRAMP Moderate/High/DOD IL4認定

委任された管理者またはパートナー管理者が機密性の高い属性値を割り当てるのを防ぐため、属性ベースのアクセスコントロールポリシーを適用し、ユーザーのオンボーディング中に設定ミスが発生するリスクを軽減できます。

クラシック
OIE



Okta Org間でのクレーム共有

© Okta and/or its affiliates. All Rights Reserved.

Okta Customer Identity

一般な可用性

非人間アイデンティティ（NHI）- 可視性とリスク分析

クラシック

OIE

機能：Identity Security Posture Management（ISPM）

セキュリティチームは、NHIによる侵害からの保護に必要な可視性を得ることができます。リスクの高い主なサービスアカウントや、NHI認証情報を持つ人間のユーザー、ローテーションされていないキーとトークンが検出・報告されます。

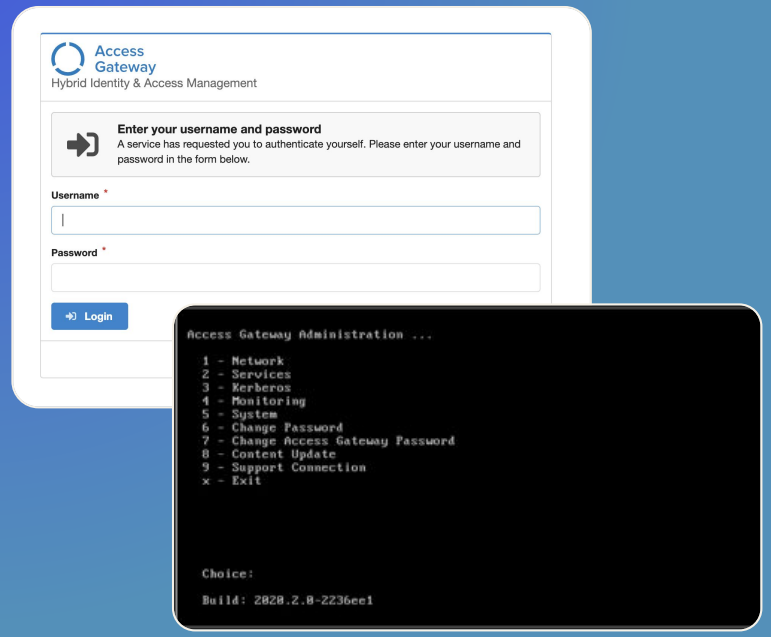
OAGのセキュアバイデザインな変更

クラシック

OIE

Okta Access Gatewayで利用可能。FedRAMP Moderate/High/DOD IL4でサポート

OAG管理コンソールは、デフォルトではローカルネットワーク上でのみアクセス可能で、管理コンソールと管理者管理CLIのどちらも管理者パスワードの変更を強制するようになります。これらの変更は、Oktaのセキュアバイデザインによる取り組みを遵守するためのものです。



OAGのセキュアバイデザインな変更

© Okta and/or its affiliates. All Rights Reserved.

Okta Customer Identity

早期アクセス

SLOリクエストを外部IdPへカスケード

すべてのSKUで利用可能。 FedRAMP Moderate/High/DOD IL4認定

デバイスのユースケースを共有している、 Okta Customer Identity（旧CIS）のお客様のセキュリティを強化します。

OIE

トークンエンドポイントのネットワーク制限

すべてのSKUで利用可能。 FedRAMP Moderate/High/DOD IL4認定

クライアント固有の許可リストに登録されたゾーンを有効にして、トークン悪用のリスクを最小限に抑え、顧客セッションを保護し、バックエンドシステムを DoS攻撃やレート制限の枯渇から保護します。

OIE

IPサービスカテゴリとしてのレジデンシャルプロキシ

AMFAで利用可能。 FedRAMP Moderate/High/DOD IL4認定

拡張動的ゾーンが、IPサービスカテゴリとしてレジデンシャルプロキシとブロックチェーンVPNをサポートするようになったため、組織はポリシー評価の前にアクセスをブロックできるようになります。

クラシック

OIE

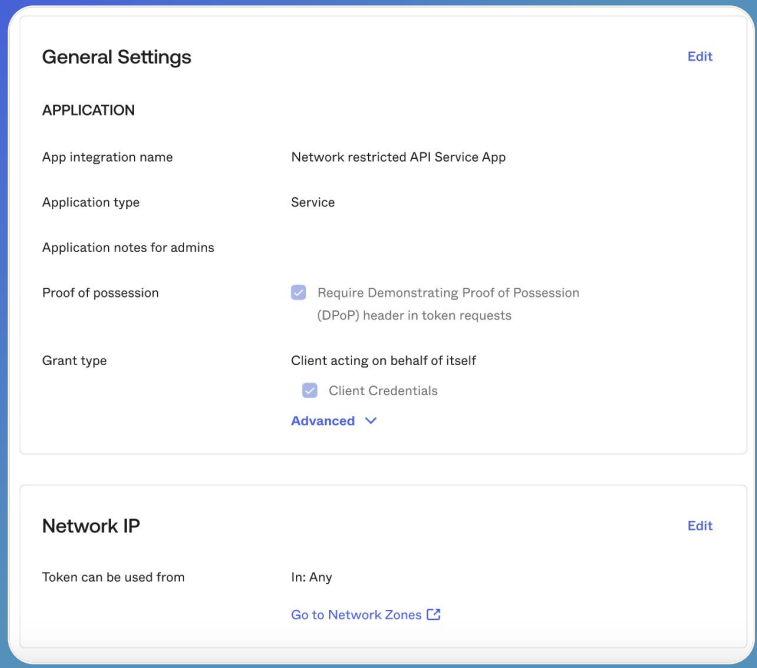
DirSyncによる増分インポート

ディレクトリ統合で利用可能。 FedRAMP Moderate/High/DOD IL4認定

Active Directoryからの増分インポートが進歩して、インポートがより高速で効率的になるため、フルインポートに頼る場面を減らすことができます。これは、シームレスなカスタマーエクスペリエンスを提供するために重要です。

クラシック

OIE



トークンエンドポイントのネットワーク制限

© Okta and/or its affiliates. All Rights Reserved.

Okta Customer Identity

早期アクセス

ID検証の名前の一致

SSO/MFAで利用可能。 | FedRAMP Moderate/High/DOD IL4認定

正当な名前と優先される名前を明確に区別することで精度とユーザーエクスペリエンスを向上させ、オンボーディング、認証、アカウント回復、サポートワークフロー全体で信頼性とセキュリティを強化します。

OIE

OIDC/SAMLアプリケーション向けにappIDコンテキストを拡張

すべてのSKUで利用可能。 | FedRAMP Moderate/High/DOD IL4認定

Oktaが開始するフェデレーション（SAML/OIDC）中にアプリケーションの詳細（ID、名前）を外部IdPに渡し、IdPでのセキュリティとポリシーの決定を強化します。

OIE

IdP署名証明書の重複

すべてのSKUで利用可能。 | FedRAMP Moderate/High/DOD IL4認定。

IdPごとに複数のアクティブな証明書に対応できるため、セキュリティを向上させながら、シームレスな証明書のローテーションや、ダウンタイムの削減、運用オーバーヘッドの削減が可能になります。

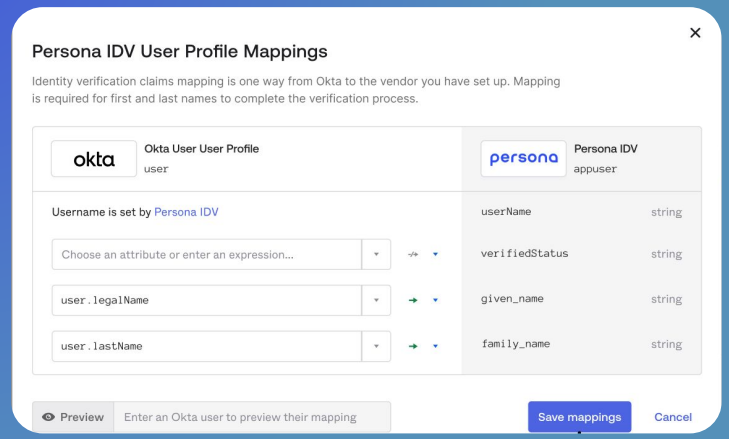
クラシック
OIE

侵害された認証情報の保護（フェーズ2）

すべてのSKUで利用可能。

管理者がテストアカウントを使用してユーザーエクスペリエンスを調整し、ワークフローを検証できるため、セキュリティと運用の信頼性の両方を高められます。

クラシック
OIE



ID検証の名前の一致

© Okta and/or its affiliates. All Rights Reserved.

Okta Customer Identity

早期アクセス

Okta Customer IdentityアプリのUniversal Logout対応

すべてのSKUで利用可能。‖FedRAMP Moderate/High/DOD IL4認定

Universal LogoutをOkta Customer Identity（旧CIS）アプリに簡単に統合できます。
開発作業は一切必要ありません。

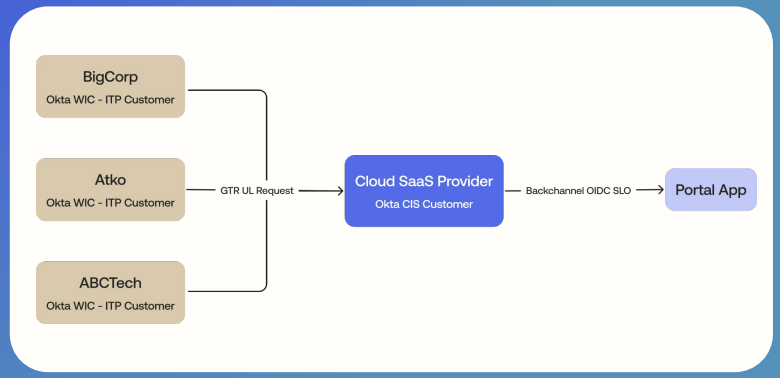
OIE

Workflowsのガバナンス

Workflowsで利用可能。‖Okta Identity Governance（OIG）はDOD IL4でサポート。WorkflowsはFedRAMP High認定、FedRAMP Moderate/DOD IL4でサポート

OIG Access RequestsとWorkflowsのロールとリソースの認定機能を活用して、
カスタマーサポートを合理化し、カスタマイズされたアクセスリクエストで
期限付きアクセス権を付与できます。

OIE



OCIアプリのUniversal Logout対応

© Okta and/or its affiliates. All Rights Reserved.


okta