

ダイナミック アクセス ロール

次世代のアクセス権限モデルを構築

課題

今日のお客様は、増大するロール（権限の集合）モデルの管理と維持という負担を強いられています。属性とエンタイトルメントの膨大な組み合わせに対応するために、あまりにも多くのロールを構築してきたからです。ビジネス ニーズを満たすためには、新しいロールを作り続けることしか解決策がありません。

現在のロール モデルとアクセス権限モデルでは、ロールの全メンバーに共通のアクセス権限セットを割り当てます。これは、特定のユーザー グループに付与したアクセス権限の管理において、非常に明確でシンプルな方法です。ユーザーにロールが付与されると、そのロールに割り当てられるアクセス権限もすべて付与されます。一方で、このシンプルなアプローチによって課題も生まれます。従来のロール モデルでアクセス権限を定義するには、動的な従業員すべてのアクセス権限を適切に制御するために、何百あるいは何千ものロールを作成する必要があります。

このためロールが急増し、組織の動的なニーズを考慮してアカウントに複数のロールが作成されています。また、アドホックでのアクセス権限付与やエンドユーザーの手作業も増加しています。

ダイナミック アクセス ロール

ダイナミック アクセス ロールを採用することで、アイデンティティ ライフサイクルに関するプロセスの自動化と最初に与えられるべき権限のプロビジョニングのための複雑なロールベースのポリシー制御を、効果的かつより簡単に実装できるようになります。

ダイナミック アクセス ロールにより、コンテキスト属性値に対する評価に基づいて、ロールのメンバーに割り当てるアクセス権限を選択できるようになります。そのため、複雑化された組織においてもロールの数を大幅に削減することが可能です。ロールの適切なメンバーに適切なアクセス権限を割り当てるためのコンテキスト情報とアクセス ポリシーがカプセル化され、多数のロールを単一のロールへと置き換えることができます。

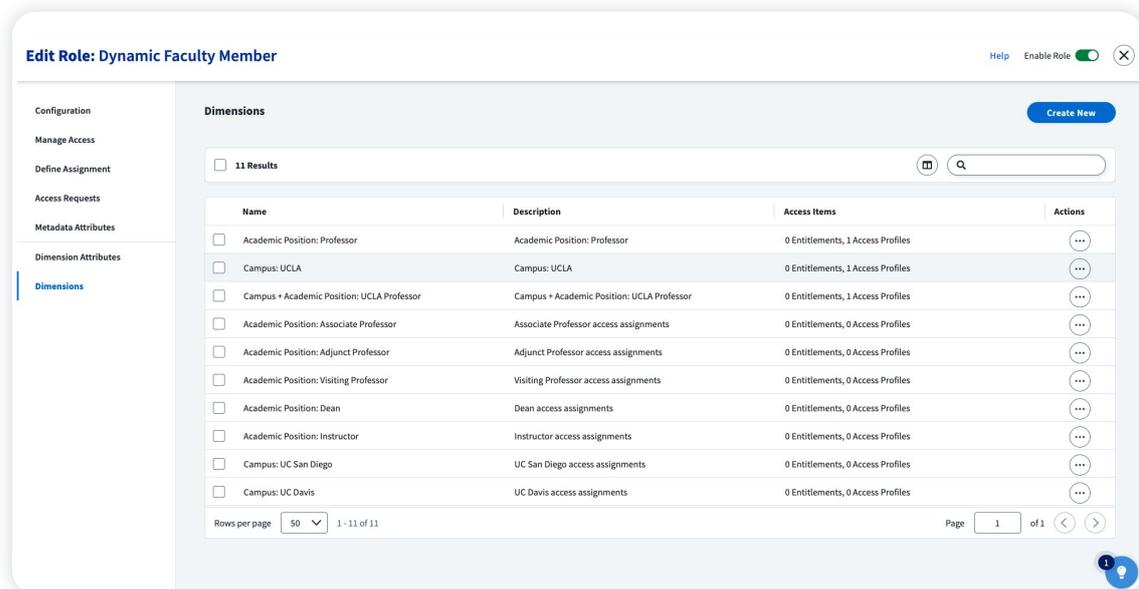
ダイナミック アクセス ロールでは、コンテキストに依存したアクセス ポリシーと整合するロール モデルの作成が可能です。この革新的なアプローチにより、お客様はロールの設計および割り当ての際に、コンテキスト情報を組み込むことができます。これにより、ロールの総数が減り、アクセス権限の可視性と理解が向上し、全体的なコンプライアンスが向上します。

仕組み

標準的なロールは、各ロールのすべてのメンバーにまったく同一のアクセス権限を割り当てるように設計されていますが、このダイナミック アクセス ロールでは、SailPoint Identity Security Cloud の標準的なロールのアクセス権限を、ディメンションによって拡張できます。この機能により、割り当てのコンテキストに基づいて、ロール メンバーにアクセス権限を選択的に割り当てることができます。

たとえば、店舗マネージャーに必要なアクセス権限が店舗の場所と管理レベルによって異なり、500 軒の店舗と3つの管理レベルがある場合、アクセス権限を適切に割り当てるためには1,500種類のロールを個別に作成する必要があります。そこで、ダイナミックアクセス ロールを使用すると、ディメンションでアクセス権限を設定された単一のロールでこれを実現できます。

ダイナミック アクセス ロールは、ディメンション、ディメンション属性、およびディメンション条件を使用して、各ロール メンバーに割り当てるアクセス権限（エンタイトルメントまたはアクセス権限プロファイル）を決定します。各ディメンションにはディメンション属性条件式が含まれており、この式を使用して、ディメンションによるアクセス権限を割り当てる必要があるかどうか決定されます。



自動化された（最初に与えられるべき権限の）割り当ての場合、ディメンション属性値はユーザーの現在のアイデンティティ オブジェクトから取得されます。要求された（アドホックの）割り当ての場合、ロールが要求されるときにディメンション属性値も指定できます。

メリット

- **ロール（権限の集合）の採用：**より多くの企業が SailPoint Identity Security Cloud のロールを採用して、統制されたロールを実現するための柔軟で保守性の高いソリューション
- **ビジネス ユーザーのエンゲージメント：**アクセス権限の技術的な詳細ではなく、ユーザーが理解できる情報（コンテキスト）に基づいたアクセス権限の決定
- **アクセス権限ポリシーと制御を統合：**ディメンションによるアクセス権限を介して、ポリシーをカプセル化
- **ロール モデルの複雑さを見せない：**ビジネス ユーザーが、あいまいな説明ではなく、コンテキストに基づいてアクセス権限を要求し、認証可能に

ダイナミック アクセス ロールで アクセス権限モデルとロール モデルを簡素化

ダイナミック アクセス ロールにより、ユーザーが使いやすい合理化されたロール モデルが実現します。アイデンティティ担当者が有効なアクセス権限モデルを構築、維持、および拡張する方法を変えることができます。組織のロール モデルに必要なロールの数を大幅に削減し、時間を短縮して保守の負担を軽減し、オーバー プロビジョニングされたユーザーを減らすことができます。



SailPoint について

SailPoint は、現代の企業がアイデンティティという視点から、アプリケーションやデータへのアクセス権限を迅速かつ大規模でシームレスに管理・保護することを支援します。当社は、この分野を先導する企業として、セキュアな企業の基盤としてのアイデンティティセキュリティを今後も改良し続けていきます。SailPoint は、今日の動的でアイデンティティを標的にしたサイバー脅威を防御する目的で構築した、インテリジェントで拡張性の高い統合プラットフォームを提供すると同時に、企業の生産性と効率性も向上させます。SailPoint は、世界で最も複雑かつ高度な企業の多くが、ビジネスの変革を推進するセキュアなテクノロジー エコシステムを構築できるよう支援します。

©2024 SailPoint Technologies, Inc. All rights reserved. SailPoint、SailPoint ロゴおよびすべての技術は、SailPoint Technologies, Inc. の米国および他の国における商標または登録商標です。その他すべての製品およびサービスは、個々の所有者の商標です。