

Cisco Access Manager

目次

概要	3
主なメリット	3
ネットワークにアイデンティティを組み込む	5
接続するものすべてをセグメント化して保護	5
ゼロトラストをキャンパスからクラウドに拡張	5
サポート対象のネットワークデバイス	6

従来のアクセス制御ソリューションのようなアプライアンス、複雑さ、オーバーヘッドを伴うことなく、アイデンティティベースのゼロトラストセキュリティを実現します。

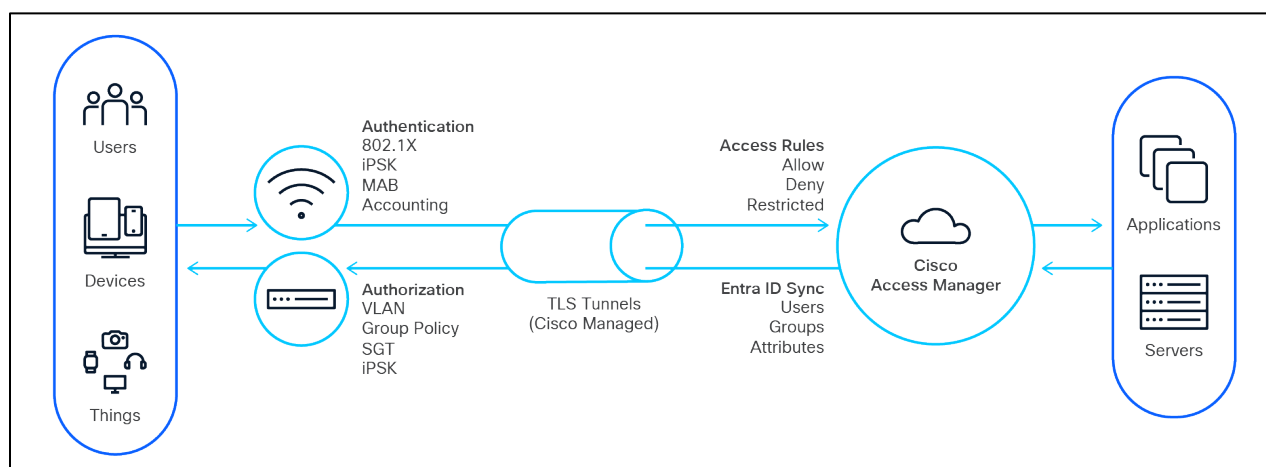
概要

Cisco Meraki ダッシュボード内で純粋な Software-as-a-Service (SaaS) として提供される Cisco Access Manager は、アイデンティティをボルトオンシステムではなく、ネットワークのネイティブ属性にします。ユーザーと端末は一度認証されますが、アイデンティティはネットワーク インフラストラクチャ全体を移動し、キャンパスからクラウドまでの関連するすべてのポイントで自動的に適用されます。

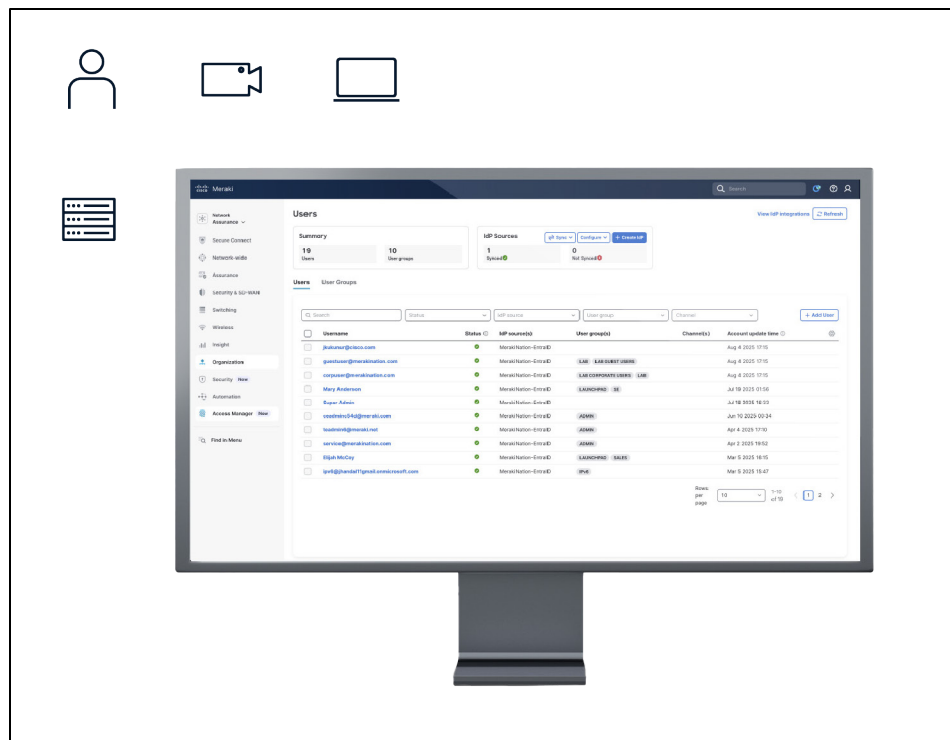
承認されたユーザーと端末のみがリソースにアクセスできるようにするための強力で拡張性のある、柔軟な方法を提供します。これにより、IT チームは、Microsoft Entra ID (旧 Azure AD) などの外部統合からのユーザーアイデンティティ、端末アイデンティティ、ネットワークコンテキスト、およびアイデンティティとセキュリティコンテキストに基づいて、ユーザーと端末のネットワークアクセスを簡単に適用およびモニターできます。

主なメリット

- 既存の Cisco Meraki インフラストラクチャを使用して、**アイデンティティベースのアクセスを数分でデプロイできます**
- ネットワークに接続するすべてのユーザーとデバイスの**安全を確保し、保護します**
- アイデンティティベースのセグメンテーションで**攻撃者のラテラルムーブメントを阻止します**
- 自動ポリシー適用により、**ゼロトラスト要件を迅速に満たせます**
- オンプレミスのハードウェアとメンテナンスサイクルを廃止することで、**コストを削減し、IT リソースを解放できます**
- Cisco Meraki ダッシュボードで**エンドツーエンドのセキュリティアーキテクチャを管理できます**



機能	利点
管理対象端末向けの証明書認証 (EAP-TLS)	ユーザーの操作を必要としない強力でシームレスな認証を提供し、検証済みのデバイスとユーザーアイデンティティに基づいた TrustSec を介して、詳細なアクセス制御とマイクロセグメンテーションを可能にします。
管理対象端末向けのユーザー名とパスワードベースの認証 (EAP-TTLS)	Microsoft EntraID と統合することで、アイデンティティに基づいたマイクロセグメンテーションとポリシーの適用を可能にしつつ、従来のクレデンシャルベースの認証を優先または必要とする組織にも対応します。
管理対象外端末向けの MAC 認証バイパス (MAB)	組織は、端末 MAC アドレスまたは端末グループに基づいて、IoT、OT、およびその他の管理対象外端末までアイデンティティベースのアクセス制御を拡張できます。オプションで、ワイヤレス端末にアイデンティティ事前共有キー (iPSK) を使用することにより、セキュリティが向上し、ネットワークのセグメンテーションを維持し、リスクを軽減できます。
複数認証オプション	同一ポートでの複数の認証方式 (802.1X、MAB) のサポートにより、複数の端末を並行して認証し、接続されたユーザーまたはデバイスのアイデンティティを定期的に再認証することで、手動による操作なく、継続的な信頼性を確保できます。
柔軟なアクセス制御	ダイナミック VLAN、ACL、グループポリシー、TrustSec ベースのマイクロセグメンテーションを含む L2 ~ L7 の承認オプションを提供します。
組み込みの認証フォールバックメカニズム	有線 (RADIUS キャッシング、ゲスト VLAN) およびワイヤレス (拡張ローカル認証) ネットワーク用の既存のフォールバックメカニズムを活用して、クラウドへの接続が失われた場合に安全なアクセスとビジネスの継続性を提供します。
認証局 (CA) の統合	外部認証局 (PKI) インフラストラクチャと統合し、証明書失効リスト (CRL) チェックを提供することで、パスワードベースの攻撃や中間者脅威から保護する証明書ベースの相互認証オプションによる堅牢なセキュリティを可能にします。



ネットワークにアイデンティティを組み込む

既存のネットワークに組み込まれた純粋な Software-as-a-Service (SaaS) のアイデンティティベースのアクセスは、ハードウェア インフラストラクチャ、外部サーバー、および複雑なデプロイメントを不要にし、リーンのITチームにエンタープライズクラスのセキュリティを提供します。

- オンプレミス インフラストラクチャ不要の純粋な Software-as-a-Service (SaaS)。
- Entra ID とのネイティブ統合。
- クラウドネイティブの拡張性、可用性、および復元力。

接続するものすべてをセグメント化して保護

アイデンティティに基づいたセグメンテーションにより、サポート対象のすべてのインフラストラクチャ全体でユーザー、端末、モノを保護することができ、あらゆるポイントでネイティブに適用されるため、ボトルネックが解消され、適応型ゼロトラスト保護が広範囲に実現します。

- TrustSec ポリシーを使用したダイナミックなアイデンティティベースのセグメンテーション。
- コンテキスト認識型アクセス制御は、ユーザーの動作、振る舞い、および場所に適応します。
- サポート対象のすべてのデバイスにネイティブに適用されるアイデンティティベースのセグメンテーション。

ゼロトラストをキャンパスからクラウドに拡張

Cisco Meraki ダッシュボードは、アイデンティティベースのフレームワークと可視性を統合して、ゼロトラストをキャンパスからクラウドに拡張し、すべての環境で一貫したアイデンティティベースのセキュリティと継続的な検証を提供します。

- Cisco Access Manager、Cisco Secure Access、Cisco Application Centric Infrastructure (ACI) 、および Cisco Identity Services Engine (ISE) の間で共有される共通アイデンティティ フレームワーク
- Cisco XDRは、すべての Cisco Meraki 管理対象デバイスからのテレメトリを関連付けます。
- アイデンティティベースのアクセス、クラウドセキュリティ、および脅威検出用の統合型 Cisco Meraki ダッシュボード。

サポート対象のネットワークデバイス

Cisco Access Manager (CAM) では現在、すべてのネットワークにアクセスするデバイスが Cisco Meraki ダッシュボードのセキュアな管理トンネルと通信する必要があります。Cisco Meraki 管理トンネルに対応していないデバイス（シスコまたはシスコ以外）はサポート対象ではありません。デバイスは、最新の安定したソフトウェアバージョンを使用している必要があります。

モデル	802.1X	MAB	VLAN	GPACL	TrustSec (AdP)	URLリダイレクト
ワイヤレス						
MR20、MR70	●	●	●	●		●
MR28/30H/33/42/42E/52/53/53E/74/84 MR36/36H/44/45/46/46E/55/56/57/76/78/86 CW91xx	●	●	●	●	802.11ac Wave2+	●
スイッチング						
MS120、MS125、MS130	●	●	●			
MS130X/R、MS150	●	●	●	MS18	●	
MS210、MS225、MS250、MS350、MS355	●	●	●	●		●
MS390、C9K-M	●	●	●	●	●	●
MX および Z					SGT トランスポートのみ	

Cisco Access Manager ライセンスは、同時にアクティブな端末セッションの数に基づき、また、Cisco Meraki 同時終了、サブスクリプション、Cisco 統合型ライセンスモデル、および Cisco Meraki ネットワーク エンタープライズ契約に基づき注文できます。

Cisco Access Manager のライセンスの詳細については、<link to licensing guide> を参照してください。