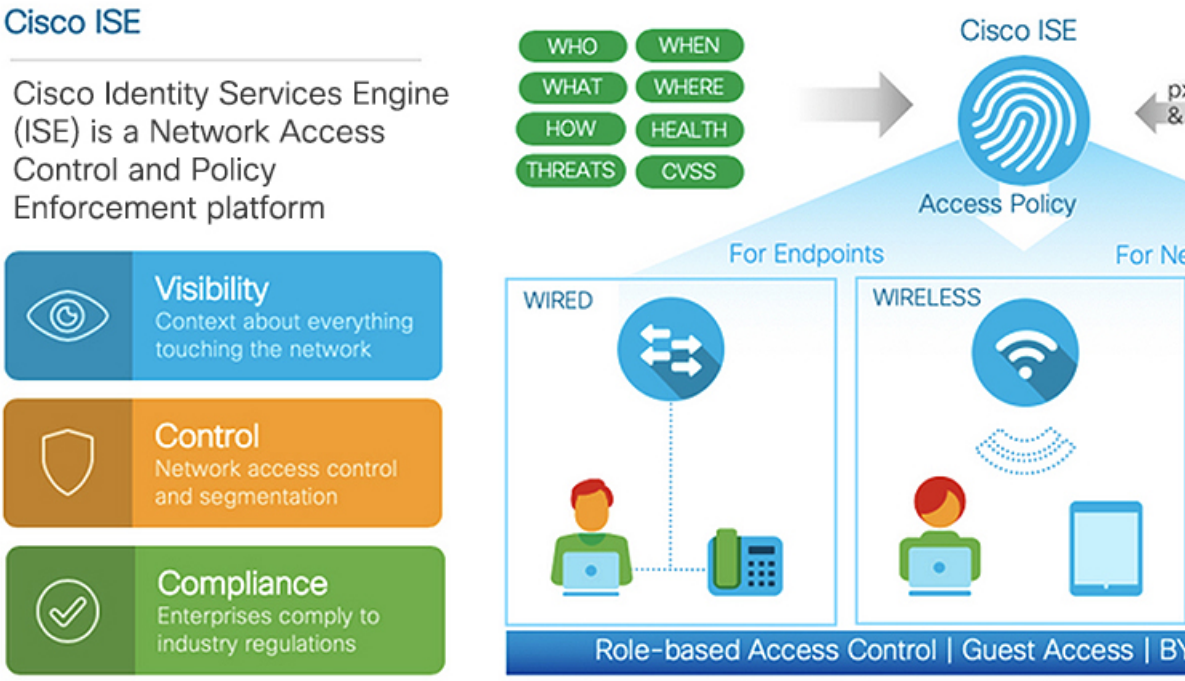
概要

Cisco ISE の概要



Cisco Identity Services Engine（ISE）は、アイデンティティベースのネットワーク アクセス コントロールおよびポリシー適用システムです。企業におけるエンドポイントのアクセスコント

ロールとネットワークデバイスの管理を可能にする共通のポリシーエンジンとして機能します。

Cisco ISE を活用すると、コンプライアンスを確保し、インフラストラクチャのセキュリティを強化し、サービス運用を合理化することができます。

Cisco ISE 管理者は、ユーザ/ユーザグループ（誰が）、デバイスタイプ（何を）、アクセス時間（いつ）、アクセスロケーション（どこで）、アクセスタイプ（有線、ワイヤレス、または VPN）（どのように）、ネットワークの脅威と脆弱性といった、ネットワークのリアルタイムのコンテキストデータを収集できます。

その後、Cisco ISE 管理者は、この情報を使用してネットワークガバナンス上の決定を下すことができます。また、アイデンティティデータをさまざまなネットワーク要素に結び付けて、ネットワークのアクセスと使用率を管理するポリシーを作成することもできます。

Cisco ISE の機能

Cisco ISE は、次の機能を備えています。

- **デバイス管理**：Cisco ISE は、TACACS+ セキュリティプロトコルを使用して、ネットワークデバイスの設定を制御および監査します。これによって、どのネットワークデバイスに誰がアクセスできて関連するネットワーク設定を変更できるかについて、きめ細かい制御が容易になります。ネットワークデバイスは、デバイス管理者の操作の認証と許可のために Cisco ISE にクエリを行うように設定できます。また、これらのデバイスは、アカウンティングメッセージを Cisco ISE に送信して、そのような操作を記録します。
- **ゲストおよびセキュアワイヤレス**：Cisco ISE を使用すると、ビジター、請負業者、コンサルタント、および顧客にセキュアなネットワークアクセスを提供できます。Web ベースポータルとモバイルポータルを使用して、企業のネットワークと内部リソースに対するゲストのオンボーディングを行うことができます。さまざまなタイプのゲストのアクセス権限を定義し、スポンサーを割り当てて、ゲストアカウントを作成および管理することができます。
- **個人所有デバイスの持ち込み（BYOD）**：Cisco ISE を使用すると、従業員とゲストが、企業ネットワークで個人のデバイスを安全に使用できるようになります。BYOD 機能のエンドユーザは、設定された手順でデバイスを追加できます。これにより、事前定義された認証とネットワークアクセスレベルがプロビジョニングされます。
- **アセットの可視性**：Cisco ISE を使用すると、ワイヤレス、有線、および VPN 接続の全体にわたって、一貫性のある方法で、ネットワーク上のユーザとデバイスを可視化し、制御することができます。Cisco ISE は、プローブとデバイスセンサーを使用して、デバイスがネットワークに接続する方法をリッスンします。その後、広範囲にわたる Cisco ISE プロファイルデータベースによって、デバイスが分類されます。これにより、適切なレベルのネットワークアクセスを許可するために必要な可視性とコンテキストが提供されます。
- **セキュアな有線アクセス**：Cisco ISE は、さまざまな認証プロトコルを使用して、ネットワークデバイスとエンドポイントにセキュアな有線ネットワークアクセスを提供します。

これには、802.1X、RADIUS、MAB、Web ベース、EasyConnect、および外部エージェント対応の認証方式が含まれます（これらに限定されない）。

- **セグメンテーション**：Cisco ISE は、ネットワークデバイスとエンドポイントに関するコンテキストデータを使用して、ネットワークセグメンテーションを容易にします。Cisco ISE がセキュアなネットワークセグメンテーションを実現する方法には、セキュリティグループタグ、アクセスコントロールリスト、ネットワークアクセスプロトコル、ポリシーセット（認可、アクセス、認証を定義）などがあります。
- **ポスチャまたはコンプライアンス**：Cisco ISE を使用すると、エンドポイントにネットワークへの接続を許可する前に、そのエンドポイントのコンプライアンス（ポスチャとも呼ばれる）をチェックすることができます。エンドポイントがポスチャサービスに適したポスチャエージェントを確実に受け取るようにすることができます。
- **脅威の封じ込め**：Cisco ISE がエンドポイントから脅威または脆弱性の属性を検出すると、適応型ネットワーク制御ポリシーが送信され、エンドポイントのアクセスレベルが動的に変更されます。脅威または脆弱性が評価され、対処されると、エンドポイントは元のアクセスポリシーに戻されます。
- **セキュリティエコシステム統合**：pxGrid 機能により、Cisco ISE は、接続されたネットワークデバイス、サードパーティベンダー、またはシスコパートナーシステムと、コンテキスト依存情報、ポリシー、設定データなどを安全に共有できます。

Cisco ISE 管理者

管理者は、次の目的で管理者ポータルを使用できます。

- 展開、ヘルプデスク操作、ネットワークデバイス、およびノードのモニタリングとトラブルシューティングの管理。
- Cisco ISE のサービス、ポリシー、管理者アカウント、およびシステム設定と操作の管理。
- 管理者パスワードおよびユーザ パスワードを変更します。

CLI 管理者は、Cisco ISE アプリケーションの起動と停止、ソフトウェアのパッチとアップグレードの適用、Cisco ISE アプライアンスのリロードとシャットダウン、およびすべてのシステム ログとアプリケーション ログの表示を実行できます。CLI 管理者には特別な権限が付与されているため、CLI 管理者クレデンシャルを保護し、Cisco ISE 展開を設定および管理する Web ベースの管理者を作成することが推奨されます。

セットアップ時に設定したユーザ名とパスワードは、CLI への管理アクセスにのみ使用されます。このロールは、CLI 管理ユーザ（CLI 管理者）と見なされます。デフォルトでは、CLI 管理ユーザのユーザ名は admin、パスワードはセットアップで定義したパスワードです。デフォルトのパスワードはありません。この CLI 管理ユーザはデフォルトの admin ユーザであり、このユーザアカウントは削除できません。ただし、このアカウントのパスワードを有効化、無効化、または変更するオプションなど、他の管理者によって編集できます。

管理者を作成するか、または既存のユーザを管理者ロールに昇格できます。管理者は、対応する管理者権限を無効にすることで、単純なネットワーク ユーザ ステータスに降格することもできます。

管理者は、Cisco ISE システムを設定および操作するローカル権限を持つユーザです。

管理者は、1 つ以上の管理者グループに割り当てられます。

関連トピック

Cisco ISE 管理者グループ （6 ページ）

CLI 管理者への外部 ID ストアの使用の強制

外部 ID ソースによる認証は、内部データベースを使用するよりも安全性が高くなります。CLI 管理者向け RBAC は、外部 ID ストアをサポートしています。

前提条件

管理者ユーザを定義し、管理者グループに追加しておく必要があります。管理者はスーパー管理者である必要があります。

AD ユーザディレクトリでのユーザの属性の定義

Active Directory を実行している Windows サーバで、CLI 管理者として設定する予定の各ユーザの属性を変更します。

1. [サーバマネージャ（Server Manager）] ウィンドウを開き、[サーバマネージャ（Server Manager）]>[ロール（Roles）]>[Active Directory ドメインサービス（Active Directory Domain Services）] > [Active Directory のユーザとコンピュータ（Active Directory Users And Computers）] > [[ad.adserver] <ad_server>.local] に移動します。
2. [表示（View）] メニューで [高度な機能（Advanced Features）] を有効にし、ユーザの属性を編集できるようにします。
3. 管理者ユーザが含まれている Active Directory グループに移動し、そのユーザを見つけます。
4. ユーザをダブルクリックして [プロパティ（Properties）] ウィンドウを開き、[属性エディタ（Attribute Editor）] を選択します。
5. 任意の属性をクリックし、「gid」と入力して、属性 `gidNumber` を見つけます。gidNumber 属性が見つからない場合は、[フィルタ（Filter）]ボタンをクリックし、[値が設定されている属性のみを表示（Show only attributes that have values）] をオフにします。
6. 属性名をダブルクリックして、各属性を編集します。各ユーザの設定を無効にする場合：
   - `uidNumber` に 60000 よりも大きな値を割り当てます。この値が一意であることを確認します。
   - `gidNumber` に 110 または 111 を割り当てます。

- gidNumber 110 は管理者ユーザを表し、111 は読み取り専用ユーザを示します。
- 割り当ての後に uidNumber を変更しないでください。
- gidNumber を変更した場合は、SSH 接続を行う前に 5 分以上待機してください。

AD ドメインへの管理者 CLI ユーザの参加

Cisco ISE CLI に接続し、**identity-store** コマンドを実行して管理者ユーザを ID ストアに割り当てます。たとえば、CLI 管理者ユーザを adpool1 として ISE に定義されている Active Directory にマッピングするには、 **identity-store active-directory domain-name adpool1 user admincliuser** を実行します。

参加が完了したら、Cisco ISE CLI に接続し、管理者 CLI ユーザとしてログインして設定を確認します。

このコマンドで使用するドメインが以前に ISE ノードに参加していた場合は、管理者コンソールでドメインに再参加する必要があります。

1. [管理（Administration）] > [IDの管理（Identity Management）] > [外部IDソース（External Identity Sources）] に移動します。
2. 左側のペインで、[Active Directory] を選択し、Active Directory の名前を選択します。
3. 右側のペインでは、AD 接続のステータスが [動作中（Operational）] と表示される場合があります。ただし、MS RPC または Kerberos のいずれかを使用して [テストユーザ（Test User）] との接続をテストすると、エラーが表示されます。
4. 管理者 CLI ユーザとして Cisco ISE CLI にこの時点でもログインできることを確認します。

新しい管理者の作成

Cisco ISE 管理者は、特定の管理タスクを実行するために、特定のロールが割り当てられたアカウントが必要です。管理者アカウントを作成して、管理者が実行する必要がある管理タスクに基づいて 1 つ以上のロールを割り当てることができます。

[管理者ユーザ（Admin Users）] ウィンドウを使用して、Cisco ISE 管理者の属性の表示、作成、変更、削除、ステータスの変更、複製、または検索を実行できます。

（注） 管理者ユーザのドメインが CLI と GUI の両方で同じである場合は、CLI で Active Directory アクセスを設定してから GUI に参加することをお勧めします。それ以外の場合は、そのドメインへの認証の失敗を回避するために、GUI からドメインに再参加する必要があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [管理者（Administrators）] > [管理者ユーザ（Admin Users）] > [追加（Add）]** を選択します。

ステップ 2 ドロップダウンリストから、次のオプションのいずれかを選択します。

- **管理者ユーザの作成**

  [管理者ユーザの作成（Create an Admin User）] を選択した場合は、[新しい管理者（New Administrator）] ウィンドウが表示され、新しい管理者ユーザのアカウント情報を設定できます。

- **ネットワーク アクセス ユーザからの選択（Select from Network Access Users）**

  [ネットワークアクセスユーザからの選択（Select from Network Access Users）] を選択した場合、現在のユーザのリストが表示され、そこからユーザを選択できます。このユーザに対応する [管理者ユーザ（Admin User）] ウィンドウが表示されます。

ステップ 3 フィールドに値を入力します。[名前（Name）] フィールドでサポートされる文字は次のとおりです：# $ ’ ( ) * + -。/ @ _。

ステップ 4 [送信（Submit）] をクリックして、新しい管理者を Cisco ISE 内部データベースに作成します。

関連トピック

読み取り専用管理ポリシー （26 ページ）
内部読み取り専用管理者の作成
読み取り専用管理者のメニュー アクセスのカスタマイズ （27 ページ）
外部グループを読み取り専用管理者グループにマッピング

Cisco ISE 管理者グループ

管理者グループは、Cisco ISE のロールベース アクセス コントロール（RBAC）グループです。同じグループに属するすべての管理者は、共通の ID を共有し、同じ権限を持ちます。特定の管理者グループのメンバーとしての管理者の ID は、許可ポリシーの条件として使用できます。管理者は、複数の管理者グループに属することができます。

どのアクセスレベルの管理者アカウントでも、管理者がアクセスできるすべてのウィンドウの、権限を持つオブジェクトを変更または削除できます。

Cisco ISE セキュリティモデルでは、管理者が、その管理者が持っている同じ権限セットが含まれる管理者グループを作成することが制限されます。付与される権限は、Cisco ISE データベースで定義されているユーザの管理ロールに基づいています。このようにして、管理者グループは、Cisco ISE システムにアクセスするための権限を定義する基礎を形成します。

次の表に、Cisco ISE で事前定義された管理者グループ、およびこれらのグループのメンバーが実行できるタスクを示します。

表 *1 : Cisco ISE* 管理者グループ、アクセス レベル、権限、および制約事項

管理者グループロール	アクセス レベル	権限	制約事項
カスタマイズ管理者	スポンサー、ゲスト、およびパーソナルデバイスポータルの管理。	• ゲストおよびスポンサー アクセスの設定。 • ゲスト アクセス設定の管理。 • エンドユーザ Web ポータルの管理。	• Cisco ISE のすべてのポリシー管理、ID 管理、またはシステムレベルの設定タスクを実行できません。 • レポートを表示できません。
ヘルプデスク管理者	クエリのモニタリングおよびトラブルシューティング操作	• すべてのレポートの実行。 • すべてのトラブルシューティング フローの実行。 • Cisco ISE ダッシュボードとライブログの表示。 • アラームの表示。	レポート、トラブルシューティング フロー、ライブ認証、またはアラームの作成、更新、または削除は実行できません。

管理者グループロール	アクセス レベル	権限	制約事項
ID 管理者	• ユーザアカウントおよびエンドポイントの管理。 • ID ソースの管理。	• ユーザアカウントおよびエンドポイントの追加、編集、および削除。 • ID ソースの追加、編集、および削除。 • ID ソース順序の追加、編集、および削除。 • ユーザアカウントの一般的な設定（属性およびパスワードポリシー）。 • Cisco ISE ダッシュボード、ライブログ、アラーム、およびレポートの表示。 • すべてのトラブルシューティングフローの実行。	Cisco ISE のすべてのポリシー管理またはシステムレベルの設定タスクを実行できません。
MnT 管理者	すべてのモニタリングおよびトラブルシューティング操作の実行。	• すべてのレポートの管理（実行、作成、および削除）。 • すべてのトラブルシューティングフローの実行。 • Cisco ISE ダッシュボードとライブログの表示。 • アラームの管理（作成、更新、表示、および削除）。	Cisco ISE のすべてのポリシー管理、ID管理、またはシステムレベルの設定タスクを実行できません。

管理者グループロール	アクセス レベル	権限	制約事項
ネットワークデバイス管理者	Cisco ISE ネットワークデバイスとネットワーク デバイス リポジトリを管理します。	• ネットワーク デバイスに対する読み取りおよび書き込み権限 • ネットワーク デバイス グループおよびすべてのネットワーク リソース オブジェクト タイプに対する読み取りおよび書き込み権限。 • Cisco ISE ダッシュボード、ライブログ、アラーム、およびレポートの表示。 • すべてのトラブルシューティング フローの実行。	Cisco ISE のすべてのポリシー管理、ID管理、またはシステムレベルの設定タスクを実行できません。

管理者グループロール	アクセス レベル	権限	制約事項
ポリシー管理者	認証、許可、ポスチャ、プロファイラ、クライアント プロビジョニング、およびワークセンターに関連する、ネットワーク上のすべての Cisco ISE サービスのポリシーを作成および管理します。	• ポリシーで使用されるすべての要素（許可プロファイル、NDG、条件など）に対する読み取りおよび書き込み権限。 • ID、エンドポイント、および ID グループ（ユーザ ID グループおよびエンドポイント ID グループ）に対する読み取りおよび書き込み権限。 • サービスポリシーおよび設定に対する読み取りおよび書き込み権限。 • Cisco ISE ダッシュボード、ライブログ、アラーム、およびレポートの表示。 • すべてのトラブルシューティング フローの実行。 • デバイス管理：デバイス管理ワークセンターにアクセスします。TACACS ポリシーの条件および結果に関する権限。TACACS プロキシおよびプロキシシーケンスのネットワークデバイス権限。	Cisco ISE のすべての ID 管理またはシステム レベルの設定タスクを実行できません。 デバイス管理：ワークセンターへのアクセスは下位リンクへのアクセスを保証していません。

管理者グループロール	アクセス レベル	権限	制約事項
RBAC 管理者	エンドポイント保護サービス適応型ネットワーク制御を除く、[操作（Operations）] メニューの下のすべてのタスク、および [管理（Administration）] の下のいくつかのメニュー項目への部分的なアクセス。	• 認証の詳細の表示。 • エンドポイント保護サービス適応型ネットワーク制御の有効化/無効化 • アラームの作成、編集、および削除、レポートの生成と表示、Cisco ISE を使用したネットワーク内の問題のトラブルシューティング。 • 管理者アカウント設定および管理者グループ設定に対する読み取り権限 • RBAC ポリシーページに加えて、管理者アクセスおよびデータ アクセス権限に対する表示権限 • Cisco ISE ダッシュボード、ライブログ、アラーム、およびレポートの表示。 • すべてのトラブルシューティング フローの実行。	Cisco ISE のすべての ID管理またはシステム レベルの設定タスクを実行できません。

管理者グループロール	アクセス レベル	権限	制約事項
読み取り専用管理者	ISE GUI への読み取り専用アクセス。		

管理者グループロール	アクセス レベル	権限	制約事項
		• データのフィルタリング、クエリーの実行、オプションの保存、印刷、データのエクスポートなど、ダッシュボード、レポート、およびライブログまたはセッションの機能の表示および使用。 • 自分のアカウントのパスワードの変更。 • グローバル検索、レポート、およびライブログまたはセッションを使用した ISE への照会。 • 属性に基づいたデータのフィルタリングと保存。 • 認証ポリシー、プロファイル ポリシー、ユーザ、エンドポイント、ネットワーク デバイス、ネットワーク デバイス グループ、ID（グループを含む）、およびその他の構成に関するデータのエクスポート。 • レポート クエリのカスタマイズ、保存、印刷、およびエクスポート。	• 許可ポリシー、認証ポリシー、ポスチャポリシー、プロファイラポリシー、エンドポイント、ユーザなど、オブジェクトの作成、更新、削除、インポート、検疫、およびモバイルデバイス管理（MDM）アクションなどの構成変更の実行。 • バックアップおよび復元、ノードの登録または登録解除、ノードの同期化、ノードグループの作成、編集、削除、またはパッチのアップグレードおよびインストールなどのシステム操作の実行。 • ポリシー、ネットワーク デバイス、ネットワーク デバイス グループ、ID（グループを含む）、およびその他の設定に関するデータのインポート。 • CoA、エンドポイントのデバッグ、収集フィルタの変更、ライブセッションデータの抑止のバイパス、PAN-HA フェールオーバー設定の変

管理者グループロール	アクセス レベル	権限	制約事項
		• カスタム レポート クエリの生成、結果の保存、印刷、またはエクスポート。 • 今後の参照用に UI 設定の保存。 • **[操作（Operations）]** > **[トラブルシューティング（Troubleshoot）]** > **[ログのダウンロード（Download Logs）]** ウィンドウから ise-psc-log などのログのダウンロード。	更、Cisco ISE ノードのペルソナまたはサービスの編集などの操作の実行。 • パフォーマンスに重大な影響を与える可能性のあるコマンドの実行。たとえば、**[操作（Operations）]** > **[トラブルシューティング（Troubleshoot）]** > **[診断ツール（Diagnostic Tools）]** > **[一般的なツール（General Tools）]** ウィンドウの TCP ダンプへのアクセスは制限されています。 • サポート バンドルの生成。

管理者グループロール	アクセス レベル	権限	制約事項
スーパー管理者	すべての Cisco ISE 管理機能。デフォルトの管理者アカウントは、このグループに属します。	すべての Cisco ISE リソースに対する作成、読み取り、更新、削除、および実行（CRUDX）権限。 （注） スーパー管理者ユーザは、デフォルトのシステム生成 RBAC ポリシーおよび権限は変更できません。これを行うには、ニーズに基づいた必要な権限が含まれた新しい RBAC ポリシーを作成し、これらのポリシーを管理者グループにマッピングする必要があります。 デバイス管理：デバイス管理ワークセンターにアクセスします。TACACS ポリシーの条件および結果に関する権限。TACACS プロキシおよびプロキシシーケンスのネットワークデバイス権限。さらに、TACACS グローバルプロトコル設定をイネーブルにする権限。	• デバイス管理：ワークセンターへのアクセスは下位リンクへのアクセスを保証していません。 • 他の管理者ユーザを変更または削除できるのは、デフォルトの上級管理者グループの管理者ユーザのみです。上級管理者グループのメニューとデータのアクセス権限で複製された管理者グループに含まれる外部からマッピングされたユーザであっても、管理者ユーザを変更または削除することはできません。

管理者グループロール	アクセス レベル	権限	制約事項
システム管理者	すべての Cisco ISE 設定およびメンテナンスのタスク。		Cisco ISE のすべてのポリシー管理またはシステムレベルの設定タスクを実行できません。

管理者グループロール	アクセス レベル	権限	制約事項
		[操作（Operations）] タブの下のすべてのアクティビティを実行するためのフルアクセス（読み取りおよび書き込み権限）、および [管理（Administration）] タブの下のいくつかのメニュー項目への部分的なアクセス。 • 管理者アカウント設定および管理者グループ設定に対する読み取り権限。 • RBAC ポリシー ウィンドウに加えて、管理者アクセスおよびデータアクセス権限に対する読み取り権限。 • **[管理（Administration）]> [システム（System）]** のすべてのオプションに対する読み取りおよび書き込み権限。 • 認証の詳細の表示。 • エンドポイント保護サービス適応型ネットワーク制御の有効化/無効化 • アラームの作成、編集、および削除、レポートの生成と表示、Cisco	

管理者グループロール	アクセス レベル	権限	制約事項
		ISE を使用したネットワーク内の問題のトラブルシューティング。 • デバイス管理：TACACS グローバルプロトコル設定を有効にする権限。	
昇格されたシステム管理者（Cisco ISE リリース 2.6、パッチ 2 以降で使用可能）	すべての Cisco ISE 設定およびメンテナンスのタスク。	昇格されたシステム管理者は、システム管理者のすべての権限があるほか、管理者ユーザを作成できます。	• ネットワーク管理者ユーザを作成または削除することはできません。 • ネットワーク管理者グループを管理することはできません。
外部 RESTful サービス（ERS）管理者	GET、POST、DELETE、PUT など、すべての ERS API 要求へのフル アクセス	• ERS API 要求の作成、読み取り、更新、および削除。	ロールは、内部ユーザ、ID グループ、エンドポイント、エンドポイントグループ、および SGT をサポートする ERS 許可のみを対象としています
外部 RESTful サービス（ERS）オペレータ	ERS API への読み取り専用アクセス、GET のみ	• ERS API 要求の読み取りのみ可能	ロールは、内部ユーザ、ID グループ、エンドポイント、エンドポイントグループ、および SGT をサポートする ERS 許可のみを対象としています。

管理者グループロール	アクセス レベル	権限	制約事項
TACACS+ Admin	フル アクセス	アクセス先： • デバイス管理ワーク センター。 • 展開（Deployment）：TACACS+ サービスを有効にします。 • 外部 ID ストア。 • **[操作（Operations）] > [TACACSライブログ（TACACS Live Logs）]** ウィンドウ。	—

関連トピック

Cisco ISE 管理者 （3 ページ）

管理者グループの作成

[管理者グループ（Admin Groups）] ウィンドウでは、Cisco ISE ネットワーク管理者グループを表示、作成、変更、削除、複製、またはフィルタリングできます。

始める前に

外部管理者グループ タイプを設定するには、1 つ以上の外部 ID ストアが指定されている必要があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [管理者（Administrators）] > [管理者グループ（Admin Groups）]** を選択します。

ステップ 2 [追加（Add）] をクリックして名前と説明を入力します。

[名前（Name）] フィールドでサポートされる特殊文字は次のとおりです：スペース、# $ & ‘ ( ) * + -。/ @ _。

ステップ 3 設定する管理者グループのタイプを次のように指定します。

- [内部（Internal）]：このグループタイプに割り当てられた管理者は、Cisco ISE 内部データベースに保存されたクレデンシャルに対して認証を行います。

- [外部（External）]：このグループに割り当てられた管理者は、[管理（Administration）]>[システム（System）]>[管理者アクセス（Admin Access）]>[認証（Authentication）]>[認証方式（Authentication Method）] ウィンドウで選択した外部 ID ストアに保存されているクレデンシャルに対して認証を行います。必要に応じて、外部グループを指定できます。

内部ユーザに認証用の外部 ID ストアが設定されている場合、内部ユーザは ISE 管理者用ポータルにログインするときに、その外部 ID ストアを [ID ソース（Identity Source）] として選択する必要があります。[内部 ID ソース（Internal Identity Source）] を選択すると認証が失敗します。

ステップ 4 [メンバーユーザ（Member Users）] エリアの [追加（Add）] をクリックして、ユーザをこの管理者グループに追加します。

ステップ 5 [送信（Submit）] をクリックします。

ユーザを管理者グループから削除するには、削除するユーザに対応するチェックボックスをオンにして、[削除（Remove）] をクリックします。

Cisco ISE への管理アクセス

Cisco ISE 管理者は、自分が属する管理者グループに基づいてさまざまな管理タスクを実行できます。これらの管理タスクは重要です。ネットワーク内の Cisco ISE の管理が許可されているユーザにのみ、管理アクセス権を付与します。

Cisco ISE では、次のオプションによって Web インターフェイスへの管理アクセスを制御することができます。

管理アクセスの方法

Cisco ISE サーバには、いくつかの方法で接続することができます。管理者ポータルは PAN によって運用されます。ログインには管理者パスワードが必要です。CLI を実行できる SSH またはコンソールを使用すると、他の ISE ペルソナサーバにアクセスできます。ここでは、各接続タイプで利用可能なプロセスとパスワードのオプションについて説明します。

- [管理者パスワード（Admin password）]：インストール時に作成した Cisco ISE 管理者ユーザのタイムアウトは、デフォルトで 45 日間です。**[管理（Administration）]>[システム（System）]>[管理者設定（Admin Settings）]** でパスワードの有効期間をオフにすると、これを回避することができます。[パスワードポリシー（Password Policy）] タブをクリックし、[パスワードの有効期間（Password Lifetime）] で [管理パスワードの有効期限（Administrative passwords expire）] をオフにします。

  この操作を行わないと、パスワードの有効期限が切れます。管理者パスワードは CLI で **application reset-passwd** コマンドを実行してリセットできます。CLI にアクセスするコンソールに接続するか、またはブートオプションメニューにアクセスする ISE イメージファイルを再起動することにより、管理者パスワードをリセットできます。

- [CLI パスワード（CLI password）]：CLI パスワードはインストール時に指定する必要があります。無効なパスワードが原因で CLI へのログインに問題がある場合は、CLI パスワー

ドをリセットできます。コンソールに接続し、**password** CLI コマンドを実行して、パスワードをリセットします。詳細については、「*ISE CLI* リファレンス」を参照してください。

- CLIへのSSHアクセス（SSH access to the CLI）：インストール中またはインストール後に **service sshd** コマンドを使用して、SSHアクセスを有効にすることができます。また、SSH接続でキーを使用するように強制することもできます。この場合、すべてのネットワークデバイスとの SSH 接続でも、このキーが使用されることに注意してください。を参照してくださいSSH キーの検証。SSH キーで Diffie-Hellman アルゴリズムの使用を強制できます。ECDSA キーは、SSH キーではサポートされないことに注意してください。

Cisco ISE でのロールベースの管理者アクセス コントロール

Cisco ISE では、管理権限を制限することでセキュリティを確保するロールベース アクセス コントロール（RBAC）ポリシーが提供されます。RBAC ポリシーは、ロールおよび権限を定義するためにデフォルトの管理者グループに関連付けられています。標準的な権限セット（メニューおよびデータ アクセス）が、事前定義された管理者グループそれぞれとペアになっており、それによって、関連付けられたロールおよび職務機能と整合性がとられています。

ユーザインターフェイスにある一部の機能には、使用するために特定の権限が必要です。ある機能が使用できない場合、または特定のタスクの実行が許可されない場合、その機能を利用するタスクを実行するのに必要な権限が自分の管理者グループにない場合があります。

アクセス レベルに関係なく、すべての管理者アカウントは、管理者がアクセスできるすべてのページの、権限を持つオブジェクトを変更または削除できます。

（注） SuperAdmin または ReadOnlyAdmin の権限を持つシステム定義の管理者ユーザのみが、ユーザグループに含まれていない ID ベースのユーザを表示できます。これらの権限なしで作成した管理者は、それぞれのユーザを表示することはできません。

ロールベースの権限

Cisco ISE は、メニューアクセス権限およびデータアクセス権限と呼ばれる、メニューおよびデータレベルの権限を設定することができます。

メニューアクセス権限により、Cisco ISE管理インターフェイスのメニューおよびサブメニュー項目を表示または非表示にすることができます。この機能によって、メニュー レベルのアクセスを制限または有効にすることができるように権限を作成することができます。

データアクセス権限により、Cisco ISE インターフェイスの管理者グループ、ユーザ ID グループ、エンドポイント ID グループ、ロケーション、およびデバイスタイプのデータへ、読み取り/書き込みアクセス権、読み取り専用アクセス権、またはアクセス権なしを付与できます。

RBAC ポリシー

RBAC ポリシーにより、管理者にメニュー項目やその他の ID グループ データ要素への特定のタイプのアクセスを付与できるかどうかが決定されます。RBACポリシーを使用して、管理者グループに基づく管理者に、メニュー項目または ID グループデータ要素へのアクセスを許可または拒否できます。管理者は、管理者ポータルにログインすると、関連付けられている管理者グループに定義されているポリシーおよび権限に基づいて、メニューおよびデータにアクセスできます。

RBAC ポリシーは、管理者グループをメニュー アクセス権限とデータ アクセス権限にマッピングします。たとえば、ネットワーク管理者に[管理者アクセス（Admin Access）]操作メニューおよびポリシーデータ要素を表示しないようにすることができます。これは、ネットワーク管理者が関連付けられるカスタムRBACポリシーを管理者グループに作成することで実現できます。

（注） 管理者アクセス用にカスタマイズされたRBACポリシーを使用している場合は、特定のデータアクセスに関連するすべてのメニュー アクセスが提供されていることを確認します。たとえば、ID またはポリシー管理者のデータ アクセス権を持つエンドポイントを追加または削除するには、[ワークセンター（Work Center）] > [ネットワークアクセス（Network Access）] と [管理（Administration）] > [IDの管理（Identity Management）] のメニュー アクセスを指定する必要があります。

デフォルトのメニュー アクセス権限

Cisco ISE では、事前定義された一連の管理者グループに関連付けられた、すぐに使用できる権限セットが用意されています。事前定義済みの管理者グループ権限により、任意の管理者グループのメンバーが、管理インターフェイス内のメニュー項目へのフルアクセス権または制限されたアクセス権（メニューアクセスと呼ばれます）を持つように権限を設定したり、その他の管理者グループのデータ アクセス要素の使用（データ アクセスと呼ばれます）を管理者グループに委任するように権限を設定したりできます。これらの権限は、さまざまな管理者グループ用の RBAC ポリシーの策定にさらに使用できる再利用可能なエンティティです。Cisco ISE では、デフォルトの RBAC ポリシーですでに使用されている一連のシステム定義メニュー アクセス権限が用意されています。定義済みのメニュー アクセス権限とは別に、Cisco ISE では RBAC ポリシーで使用できるカスタム メニュー アクセス権限を作成することができます。キーアイコンはメニューとサブメニューのメニューアクセス権限を表し、クロス付きのキーアイコンは異なる RBAC グループのアクセス権限がないことを表します。

（注） 上級管理者ユーザの場合、すべてのメニュー項目が使用可能です。その他の管理者ユーザの場合、[メニューアクセス権限（Menu Access Privileges）] カラムのすべてのメニュー項目はスタンドアロン展開、および分散展開におけるプライマリノードで使用可能です。分散展開のセカンダリノードの場合、[管理（Administration）] タブの下のメニュー項目は使用不可です。

メニュー アクセス権限の設定

Cisco ISE では、RBAC ポリシーにマッピングできるカスタム メニュー アクセス権限を作成することができます。管理者のロールに応じて、管理者の特定のメニュー オプションのみへのアクセスを許可できます。

ステップ 1 **[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [許可（Authorization）] > [権限（Permissions）] > [メニュー アクセス（Menu Access）]** を選択します。

ステップ 2 [追加（Add）] をクリックし、[名前（Name）] フィールドおよび [説明（Description）] フィールドに値を入力します。

a) [ISEナビゲーション構造（ISE Navigation Structure）] メニューを目的のレベルまで展開し、権限を作成するオプションをクリックします。

b) [メニューアクセスの権限（Permissions for Menu Access）] ペインで [表示（Show）] をクリックします。

ステップ 3 [送信（Submit）] をクリックします。

データ アクセス権限を付与するための前提条件

RBAC 管理者がオブジェクト（たとえば「ユーザ ID グループ」データ型の「従業員」）へのフルアクセス権限を持っている場合、管理者はそのグループに属するユーザの表示、追加、更新、削除を行うことができます。管理者に [ユーザ（Users）] ウィンドウのメニューのアクセス権限が付与されていることを確認します（[管理（Administration）] > [IDの管理（Identity Management）] > [ID（Identities）] > [ユーザ（Users）]）。これは、ネットワークデバイスとエンドポイントオブジェクトに当てはまります（ネットワーク デバイス グループおよびエンドポイント ID グループのデータ型に付与されたアクセス権限に基づく）。

デフォルトのネットワーク デバイス グループ オブジェクト（すべてのデバイス タイプおよびすべてのロケーション）に属するネットワーク デバイスのデータ アクセスを有効にしたり、制限したりすることはできません。これらのデフォルト ネットワーク デバイス グループ オブジェクトの下に作成されたオブジェクトに対するフルアクセスデータ権限が付与される場合、すべてのネットワークデバイスが表示されます。このため、デフォルト ネットワーク デバイス グループ オブジェクトに依存しない、ネットワーク デバイス グループのデータ型の階層を別個に作成することをお勧めします。制限付きアクセスを作成するには、新たに作成されたネットワーク デバイス グループに、ネットワーク デバイス オブジェクトを割り当てる必要があります。

（注） 管理者グループに対してではなく、ユーザ ID グループ、ネットワーク デバイス グループ、およびエンドポイント ID グループに関してのみ、データアクセス権限を有効にしたり制限したりできます。

デフォルトのデータ アクセス権限

Cisco ISE では、事前定義されたデータ アクセス権限のセットが付属しています。これらの権限により、複数の管理者が、同じユーザ母集団内でデータアクセス権限を持つことができます。データ アクセス権限の使用を 1 つ以上の管理者グループに対して有効化または制限することができます。このプロセスにより、1 つの管理者グループの管理者に対する自律委任制御が可能となり、選択的関連付けを介して選択済みの管理者グループのデータ アクセス権限を再利用できます。データアクセス権限の範囲は、フルアクセス権から、選択された管理者グループまたはネットワーク デバイス グループを表示するためのアクセス権なしまでとなります。RBAC ポリシーは、管理者（RBAC）グループ、メニューアクセス、データ アクセス権限に基づいて定義されます。最初に、メニューアクセス権限とデータアクセス権限を作成し、次に、対応するメニューアクセス権限とデータアクセス権限に管理者グループを関連付ける RBAC ポリシーを作成する必要があります。RBAC ポリシーには、次の形式を使用します。admin_group=Super Admin の場合、スーパー管理者メニューアクセス権限とスーパー管理者データアクセス権限を割り当てます。定義済みのデータ アクセス権限とは別に、Cisco ISE では RBAC ポリシーと関連付けることができるカスタム データ アクセス権限を作成することができます。

管理者グループに付与することができる、フルアクセス、アクセスなし、読み取り専用という名前の 3 つのデータアクセス権限があります。

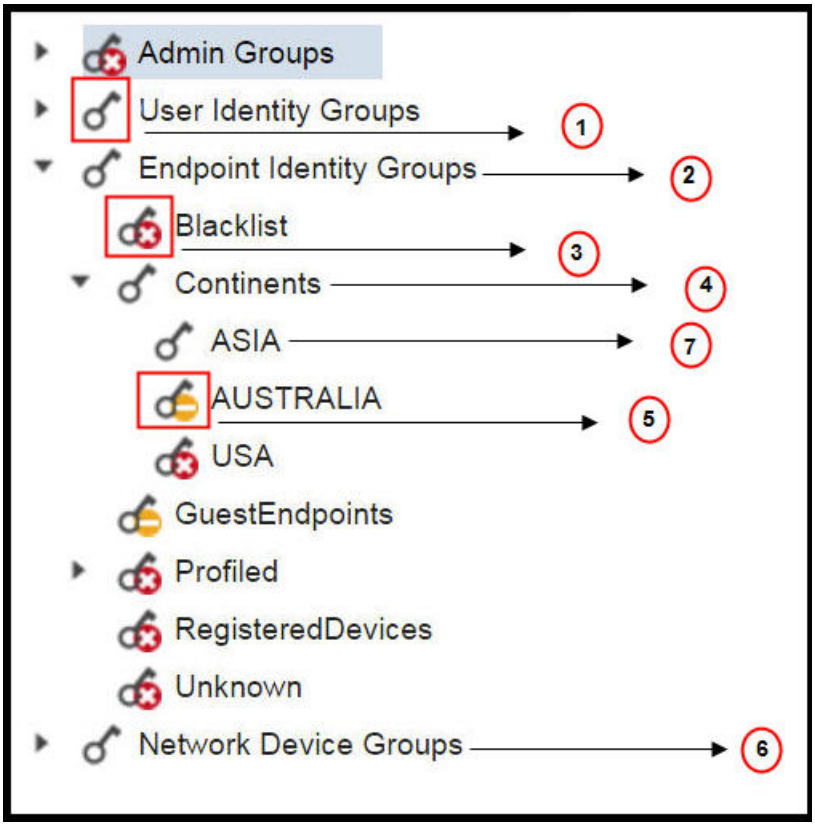
読み取り専用権限は次の管理者グループに付与できます。

- [管理（Administration）] > [管理者アクセス（Admin Access）] > [管理者（Administrators）] > [管理者グループ（Admin Groups）]
- [管理（Administration）] > [グループ（Groups）] > [ユーザ ID グループ（User Identity Group）]
- [管理（Administration）] > [グループ（Groups）] > [エンドポイント ID グループ（Endpoint Identity Groups）]
- [ネットワーク可視性（Network Visibility）] > [エンドポイント（Endpoints）]
- [管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス グループ（Network Device Groups）]
- [管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス（Network Devices）]
- [管理（Administration）] > [ID の管理（Identity Management）] > [ID（Identities）]
- [管理（Administration）] > [ID の管理（Identity Management）] > [グループ（Groups）] > [ユーザ ID グループ（User Identity Groups）]
- [管理（Administration）] > [ID の管理（Identity Management）] > [グループ（Groups）] > [エンドポイント ID グループ（Endpoint Identity Groups）]

データタイプ（[エンドポイントIDグループ（Endpoint Identity Groups）] など）に対して読み取り専用権限を持つ場合は、そのデータタイプに CRUD 操作を実行することはできません。オ

ブジェクト（GuestEndpoints など）に対して読み取り専用権限を持つ場合には、そのオブジェクトに編集または削除操作を実行することはできません。

図 *1* : 以下の図に、さまざまな ***RBAC*** グループのための追加のサブメニューまたはオプションを含む ***2*** 番目または ***3*** 番目のレベルのメニューに、データアクセス権限がどのように適用されるかを示します。



ラベル	説明
1	[ユーザ ID グループ（User Identity Groups）] データ タイプのフル アクセスが示されています。
2	[エンドポイントIDグループ（Endpoint Identity Groups）] が、その子（Asia）に付与されている最大の権限（フルアクセス）を得ていることが示されています。
3	オブジェクト（Blacklist）のアクセス権限がないことが示されています。
4	親（Continents）が、その子（Asia）に付与されている最大のアクセス権限を得ていることが示されています。

ラベル	説明
5	オブジェクト（Australia）の読み取り専用アクセスが示されています。
6	親（[ネットワーク デバイス グループ（Network Device Groups）]）にフル アクセスが付与されている場合、子が自動的に権限を継承することが示されています。
7	親（Asia）にフル アクセスが付与されている場合、オブジェクトに権限が明示的に付与されていない限り、オブジェクトがフル アクセス権限を継承することが示されています。

データ アクセス権限の設定

Cisco ISE では、RBAC ポリシーにマッピングできるカスタム データ アクセス権限を作成することができます。管理者のロールに基づいて、データを選択するのみのアクセス権を管理者に提供することができます。

ステップ 1 **[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [許可（Authorization）] > [権限（Permissions）]** を選択します。

ステップ 2 **[権限（Permissions）] > [データ アクセス（Data Access）]** を選択します。

ステップ 3 [追加（Add）] をクリックし、[名前（Name）] フィールドおよび [説明（Description）] フィールドに値を入力します。

a) 管理者グループをクリックして展開し、目的の管理者グループを選択します。

b) [フル アクセス（Full Access）]、[読み取り専用アクセス（Read Only Access）]、または [アクセスなし（No Access）] をクリックします。

ステップ 4 [保存（Save）] をクリックします。

読み取り専用管理ポリシー

デフォルトの読み取り専用管理ポリシーは、[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [RBAC] [許可（Authorization）] > [ポリシー（Policy）] ページで利用できます。このポリシーは、新規インストールとアップグレードされた展開の両方で使用できます。読み取り専用管理ポリシーは、読み取り専用管理者グループに適用されます。デフォルトでは、ネットワーク管理者メニュー アクセス権と読み取り専用データ アクセス権は、読み取り専用管理者に付与されます。

（注） デフォルトの読み取り専用ポリシーは、読み取り専用管理者グループに割り当てられます。読み取り専用管理者グループを使用してカスタムRBACポリシーを作成することはできません。

読み取り専用管理者のメニュー アクセスのカスタマイズ

デフォルトでは、読み取り専用管理者にはネットワーク管理者メニューアクセス権と読み取り専用管理者データ アクセス権が与えられます。ただし、ネットワーク管理者が読み取り専用管理者に [ホーム（Home）] タブと [管理（Administration）] タブのみを表示する必要がある場合、ネットワーク管理者はカスタム メニュー アクセス権を作成したり、デフォルトのアクセス許可を MnT 管理者メニュー アクセス権またはポリシー管理者メニュー アクセス権にカスタマイズすることができます。ネットワーク管理者は、読み取り専用管理ポリシーにマップされた読み取り専用データ アクセスを変更することはできません。

ステップ 1 管理者用ポータルにネットワーク管理者としてログインします。

ステップ 2 **[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [認証（Authorization）] > [権限（Permissions）] > [メニュー アクセス（Menu Access）]** ページに移動します。

ステップ 3 [追加（Add）] をクリックして、[名前（Name）]（MyMenu など）と [説明（Description）] を入力します。

ステップ 4 [メニュー アクセス権限（Menu Access Privileges）] セクションでは、[表示/非表示（Show/Hide）] オプションを選択して、読み取り専用管理者に表示する必要があるオプション（[ホーム（Home）] タブや [管理（Administration）] タブなど）を選択できます。

ステップ 5 [送信（Submit）] をクリックします。
カスタム メニュー アクセス権限は、[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [認証（Authorization）] > [ポリシー（Policy）] ページに表示される、読み取り専用管理ポリシーに対応する [権限（Permissions）] ドロップダウンに表示されます。

ステップ 6 [管理（Administration）]>[システム（System）]>[管理者アクセス（Admin Access）]>[許可（Authorization）] > [RBAC] > [ポリシー（Policy）] ページに移動します。

ステップ 7 **読み取り専用管理ポリシー**に対応する [権限（Permissions）] ドロップダウンをクリックします。

ステップ 8 **[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [認証（Authorization）] > [権限（Permissions）] > [メニュー アクセス（Menu Access）]** ページで作成したデフォルト（MnT 管理者メニュー アクセス権）またはカスタム メニュー アクセス権限（MyMenu）を選択します。

ステップ 9 [保存（Save）] をクリックします。

読み取り専用管理者ポリシーにデータ アクセス権限を選択すると、エラーが発生します。

（注） 読み取り専用管理者用ポータルにログインすると、画面上部に読み取り専用のアイコンが表示され、指定したメニュー オプションのみを表示（データ アクセスなし）できます。