管理者および管理者アクセス ポリシーの管理

ロールベース アクセス コントロール

Cisco ISE では、管理者に対して特定のシステム動作の権限を許可または拒否するロールベース アクセス コントロール（RBAC）ポリシーを定義することができます。これらの RBAC ポリシーは、個々の管理者の ID、または管理者が属する管理者グループの ID に基づいて定義されます。

さらにセキュリティを強化し、管理者ポータルにアクセスできる者を制御するために、次を実行します。

- リモート クライアントの IP アドレスに基づいて管理アクセスを設定します。
- 管理アカウントの強力なパスワード ポリシーを定義します。
- 管理 GUI セッションのセッション タイムアウトを設定します。

Cisco ISE 管理者

Cisco ISE 管理者は管理者ポータルを使用して次の操作を行います。

- 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。

管理者は、コマンドラインインターフェイス（CLI）またはWebベースのインターフェイスから Cisco ISE にアクセスできます。Cisco ISE のセットアップ中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 管理者ユーザ（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ユーザと呼ばれます。このデフォルトのadminユーザアカウントは削除できませんが、他の管理者が編集できます（このアカウントのパスワードを有効、無効、または変更するオプションを含む）。

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と見なすことができます。

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。これらの管理者グループはシステムで事前に定義されています。これについては、次の項で説明します。

関連トピック

Cisco ISE 管理者グループ （3 ページ）

CLI 管理者と Web ベースの管理者の権限の比較

CLI 管理者は Cisco ISE アプリケーションの開始と停止、ソフトウェア 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行うことができます。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の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。

新しい Cisco ISE 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 つ以上のロールの割り当てることができます。

[管理者ユーザ（Admin Users）] ページを使用して、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。

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 次のいずれかを実行します。

- 新しいユーザの作成（Create New User）

  [新しいユーザの作成（Create New User）] を選択すると、空白の [管理者ユーザ（Admin User）] ページが表示され、設定する必要があります。

- 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、このリストでクリックしてユーザを選択することができ、対応する [管理者ユーザ（Admin User）] ページが表示されます。

ステップ 3 [管理者（Administrator）] 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

Cisco ISE 管理者 （1 ページ）
CLI 管理者と Web ベースの管理者の権限の比較 （2 ページ）
Cisco ISE 管理者グループ （3 ページ）
管理者アクセスの設定 （20 ページ）
読み取り専用管理ポリシー
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
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 でロールベース アクセス コントロール（RBAC）グループとも呼ばれ、同じ管理者グループに属する多数の管理者が含まれます。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。

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。

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（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く）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。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（Permissions）	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 livelogs 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（Permissions）	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、livelogs、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 livelogs 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（Permissions）	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 • NDG 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、livelogs、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（Permissions）	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、livelogs、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（Permissions）	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、livelogs、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（Permissions）	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任意の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。

管理者グループロール	アクセス レベル	権限（Permissions）	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（Permissions）	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読み取り権限 • [管理（Administration）] > [システム（System）] メニュー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 ISE を使用したネットワーク内の	

管理者グループロール	アクセス レベル	権限（Permissions）	制約事項
		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 プロトコル設定をイネーブルにする権限。	
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
TACACS+ Admin	フル アクセス	次へのアクセス： • 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）] ページ。	—

関連トピック

Cisco ISE 管理者 （1 ページ）

管理者グループの作成

[管理者グループ（Admin Groups）] ページでは、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、[名前（Name）] および [説明（Description）] 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、属性セレクタで指定した外部 ID ストアに含まれているクレデンシャルに対して認証を行います。[外部（External）] を選択した後、Cisco ISE による外部グループ情報のインポート元になる ID ストアを指定します。

ステップ 4 [追加（Add）] をクリックして、ユーザを [管理者グループ ユーザ（Admin Group Users）] テーブルに追加します。[ユーザ（Users）] リストで、管理者グループに追加するユーザを選択します。

ステップ 5 ユーザを [管理者グループ ユーザ（Admin Group Users）] テーブルから削除するには、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。

ステップ 6 [送信（Submit）] をクリックして、作成した管理者グループに対して行った変更を Cisco ISE データベースに保存します。

（注） 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 ソースとして選択する必要があります。内部 ID ストアを選択すると認証が失敗します。

関連トピック

Cisco ISE 管理者グループ （3 ページ）

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大であり、管理アクセスがネットワークでの Cisco ISE の管理を許可されたユーザに制限されるようにする必要があります。

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。

Cisco ISE のロールベース アクセス コントロール

ロールベース アクセス コントロール ポリシー（管理者アクセスと呼ばれる）は自分で定義するアクセス コントロール ポリシーで、Cisco ISE 管理インターフェイスへのアクセスを制限できます。これらの管理者アクセスポリシーによって、個々の管理者ユーザまたは管理者グループに適用する指定のロールベースアクセス権限設定を使用し、管理者単位または管理者グループ単位でアクセスの量とタイプをカスタマイズすることができます。

ロールベース アクセスにより、各エンティティがアクセスできる対象が決まり、アクセス コントロール ポリシーにより制御されます。また、ロールベース アクセスにより、使用中の管理ロール、エンティティが属している管理者グループ、およびエンティティのロールに基づいて適用される対応する権限と設定も決まります。

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次のデータへの読み取り/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。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。

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 ポリシーを作成することで実現できます。

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） スーパー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。その他の管理ユーザの場合、この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）] > [認証（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) 目的のレベルまでメニュー項目をクリックして展開し、権限を作成するメニュー項目をクリックします。

b) [メニュー アクセス（Menu Access）] 領域の [権限（Permissions）] 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）] ページ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） 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。管理グループには当てはまりません。

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。データ アクセス権限により、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 ポリシーを作成します。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。

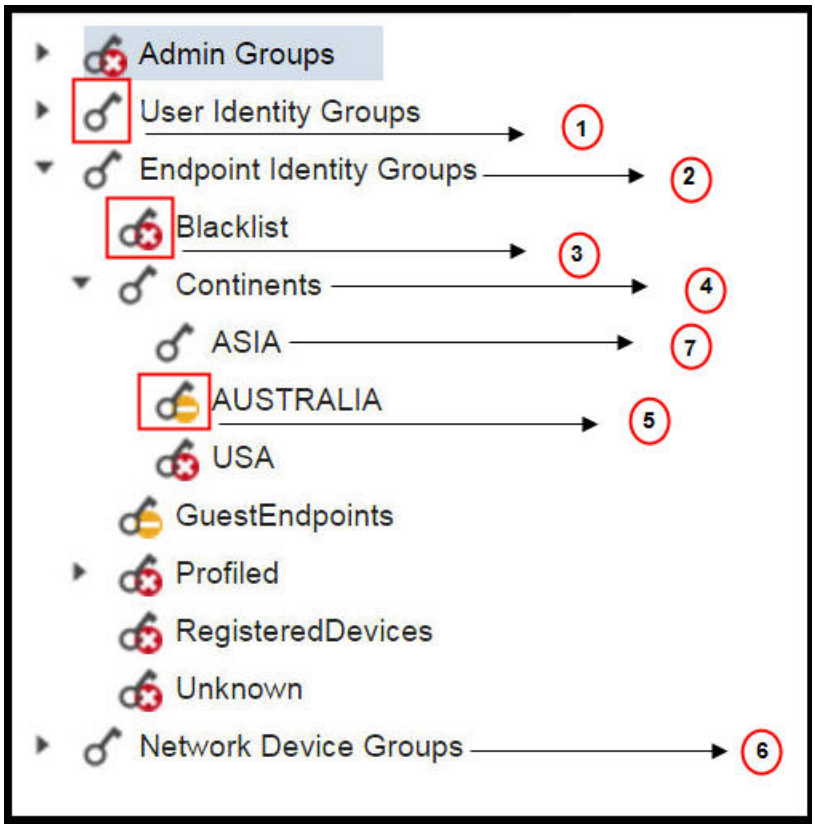
管理者グループに付与することができる、フルアクセス、アクセスなし、読み取り専用という名前の 3 つのデータ アクセス権限があります。

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/削除操作を実行することはできません。

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（**Label**）	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。
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。

ラベル（Label）	説明
[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。

管理者のアクセス ポリシーの設定

管理者アクセス（RBAC）ポリシーは if-then 形式で表され、ここで if は RBAC 管理者グループの値、および then は RBAC 権限の値になります。

[RBAC ポリシー（RBAC policies）] ページ（[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）]）には、デフォルト ポリシーのリストが含まれています。これらのデフォルト ポリシーは編集または削除できません。[RBAC ポリシー（RBAC policies）] ページでは、特に職場の管理者グループ用にカスタム RBAC ポリシーを作成し、パーソナライズされた管理者グループに適用できます。

制限付きメニュー アクセスを割り当てるときには、データ アクセス権限により、指定されているメニューを使用するために必要なデータに管理者がアクセスできることを確認してくださ

い。たとえばデバイス ポータルへのメニュー アクセスを付与するが、エンドポイント ID グループへのデータ アクセスを許可しないと、管理者はポータルを変更できません。

始める前に

- RBAC ポリシーを定義するすべての管理者グループを作成していることを確認します。
- これらの管理者グループが、個々の管理者ユーザにマッピングされていることを確認します。
- メニュー アクセス権限やデータ アクセス権限など、RBAC 権限を設定していることを確認します。

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）] > [ポリシー（Policy）]** を選択します。

[RBAC ポリシー（RBAC Policies）] ページには、デフォルトの管理者グループ用にすぐに使用できる定義済みの一連のポリシーが含まれています。これらのデフォルト ポリシーは編集または削除できません。

ステップ 2 デフォルト RBAC ポリシー ルールのいずれかの隣にある [操作（Action）] をクリックします。

ここでは、新しい RBAC ポリシーを挿入し、既存の RBAC ポリシーを複製し、既存の RBAC ポリシーを削除できます。

ステップ 3 [新しいポリシーの挿入（Insert New Policy）] をクリックします。

ステップ 4 [ルール名（Rule Name）]、[RBAC グループ（RBAC Group(s)）]、および [権限（Permissions）] フィールドに値を入力します。

RBAC ポリシーの作成時に、複数のメニュー アクセス権限とデータ アクセス権限を選択することはできません。

ステップ 5 [保存（Save）] をクリックします。

関連トピック

RBAC ポリシー （14 ページ）
デフォルトのメニュー アクセス権限 （15 ページ）
メニュー アクセス権限の設定 （15 ページ）
デフォルトのデータ アクセス権限 （16 ページ）
データ アクセス権限の設定 （19 ページ）

管理者アクセスの設定

Cisco ISE では、セキュリティ強化のために管理者アカウントにルールを定義できます。管理インターフェイスへのアクセスを制限したり、強力なパスワードの使用やパスワードの定期的な変更を管理者に強制することができます。Cisco ISE の [管理者アカウントの設定（Administrator

Account Settings）] で定義するパスワード ポリシーは、すべての管理者アカウントに適用されます。

Cisco ISE では、管理者パスワードでの UTF-8 文字の使用はサポートされていません。

同時管理セッションとログイン バナーの最大数の設定

同時管理 GUI または CLI（SSH）セッションの最大数、および管理 Web または CLI インターフェイスにアクセスする管理者を手助け、ガイドするログインバナーを設定できます。管理者のログイン前後に表示されるログインバナーを設定できます。デフォルトでは、これらのログイン バナーは無効になっています。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [設定（Settings）] > [アクセス（Access）] > [セッション（Session）]** を選択します。

ステップ 2 GUI および CLI インターフェイスを介した同時管理セッションの、許可する最大数を入力します。同時管理 GUI セッションの有効範囲は 1 ～ 20 です。同時管理 CLI セッションの有効範囲は 1 ～ 10 です。

ステップ 3 Cisco ISE で管理者がログインする前にメッセージを表示する場合は、[プリログイン バナー（Pre-login banner）] チェックボックスをオンにして、テキスト ボックスにメッセージを入力します。

ステップ 4 Cisco ISE で管理者がログインした後にメッセージを表示する場合は、[ポストログイン バナー（Post-login banner）] チェックボックスをオンにして、テキスト ボックスにメッセージを入力します。

ステップ 5 [保存（Save）] をクリックします。

関連トピック

IP アドレスの選択からの Cisco ISE への管理アクセスの許可 （21 ページ）

IP アドレスの選択からの Cisco ISE への管理アクセスの許可

Cisco ISE では、管理者が Cisco ISE 管理インターフェイスにアクセスできる IP アドレスのリストを設定することができます。

管理者アクセス コントロール設定は、管理ペルソナ、ポリシー サービス ペルソナ、またはモニタリング ペルソナを担う Cisco ISE ノードに対してのみ適用できます。これらの制限はプライマリ ノードからセカンダリ ノードに複製されます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

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

ステップ 2 [リストにある IP アドレスだけに接続を許可（Allow only listed IP addresses to connect）] を選択します。

ステップ 3 [アクセス制限の IP リストの設定（Configure IP List for Access Restriction）] 領域で、[追加（Add）] をクリックします。

ステップ 4 [IP アドレス（IP Address）] フィールドに IP アドレスをクラスレス ドメイン間ルーティング（CIDR）形式で入力します。

ステップ 5 [CIDR 形式のネットマスク（Netmask in CIDR format）] フィールドにサブネット マスクを入力します。

ステップ 6 [OK] をクリックします。このプロセスを繰り返して、他の IP アドレス範囲をこのリストに追加します。

ステップ 7 [保存（Save）] をクリックして、変更内容を保存します。

関連トピック

管理者アクセスの設定 （20 ページ）

管理者アカウントのパスワード ポリシーの設定

Cisco ISE では、セキュリティ向上のために管理者アカウントにパスワード ポリシーを作成することもできます。必要な管理者認証がパスワードベースか、クライアント証明書ベースかを定義できます。ここで定義したパスワード ポリシーは、Cisco ISE のすべての管理者アカウントに適用されます。

（注） Cisco ISE では、管理者パスワードでの UTF-8 文字の使用はサポートされていません。

始める前に

- 次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。
- 自動フェールオーバー設定が展開でイネーブルになっている場合はオフにします。認証方式を変更すると、アプリケーション サーバ プロセスが再起動されます。これらのサービスが再起動されるまで遅延が発生する場合があります。このサービスの再起動の遅延により、セカンダリ管理ノードの自動フェールオーバーが開始される場合があります。

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

ステップ 2 次の認証方式のいずれかを選択します。

- パスワードベース：管理者ログインで標準のユーザ ID およびパスワード クレデンシャルを使用する場合は、[パスワードベース（Password Based）] オプションを選択し、[内部（Internal）] または [外部（External）] のいずれかの認証タイプを指定します。

  （注） LDAP などの外部 ID ストアを設定しており、それを認証ソースとして使用して管理者ユーザにアクセス権を付与する場合は、その ID ソースを [ID ソース（Identity Source）] リスト ボックスから選択する必要があります。

- [クライアント証明書ベース（Client Certificate Based）]：証明書ベースのポリシーを指定する場合は、[クライアント証明書ベース（Client Certificate Based）] オプションを選択し、既存の証明書認証プロファイルを選択します。

ステップ 3 [パスワード ポリシー（Password Policy）] タブをクリックし、値を入力します。

ステップ 4 [保存（Save）] をクリックして、管理者パスワード ポリシーを保存します。

（注） 外部 ID ストアを使用してログイン時に管理者を認証する場合は、管理者プロファイルに適用されるパスワード ポリシーにこの設定値が設定されている場合でも、外部 ID ストアが依然として管理者のユーザ名とパスワードを認証することに留意してください。

関連トピック

管理者アクセスの設定 （20 ページ）
管理者パスワード ポリシーの設定
管理者アカウントのアカウント無効化ポリシーの設定 （23 ページ）

管理者アカウントのアカウント無効化ポリシーの設定

Cisco ISE では、設定した連続日数の間に管理者アカウントが認証されなかった場合は、管理者アカウントを無効に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）] > [認証（Authentication）] > [アカウント無効化ポリシー（Account Disable Policy）] の順に選択します。

ステップ 2 [非アクティブになってから n 日後にアカウントを無効にする（Disable account after n days of inactivity）] チェックボックスをオンにして、日数を入力します。

このオプションでは、管理者アカウントが連続する日数非アクティブだった場合に管理者アカウントを無効にすることができます。ただし、[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [管理者（Administrators）] > [管理ユーザ（Admin Users）] の [非アクティブ アカウントを無効化しない（Inactive Account Never Disabled）] オプションを使用して、このアカウント無効化ポリシーから個々の管理者アカウントを除外することができます。

ステップ 3 [保存（Save）] をクリックして、管理者のグローバル アカウント無効化ポリシーを設定します。

管理者のセッション タイムアウトの設定

Cisco ISE を使用すると、管理 GUI セッションが非アクティブであっても依然として接続状態である時間を決定できます。分単位の時間を指定することができ、その時間が経過すると Cisco ISE は管理者をログアウトします。セッションのタイムアウト後、管理者は、Cisco ISE 管理者ポータルにアクセスするには再びログインする必要があります。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [設定（Settings）] > [セッション（Session）] > [セッションのタイムアウト（Session Timeout）]** を選択します。

ステップ 2 アクティビティがない場合に管理者をログアウトするまでに Cisco ISE が待機する時間（分）を入力します。デフォルト値は 60 分です。有効な範囲は 6 ～ 100 分です。

ステップ 3 [保存（Save）] をクリックします。

関連トピック

管理者アクセスの設定 （20 ページ）

アクティブな管理セッションの終了

Cisco ISE では、すべてのアクティブな管理セッションが表示され、そこからセッションを選択し、必要が生じた場合はいつでも終了できます。同時管理 GUI セッションの最大数は 20 です。GUI セッションの最大数に達した場合、スーパー管理者グループに属する管理者がログインして一部のセッションを終了できます。

始める前に

次のタスクを実行するには、スーパー管理者である必要があります。

ステップ 1 **[管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [設定（Settings）] > [セッション（Session）] > [セッション情報（Session Info）]** を選択します。

ステップ 2 終了するセッション ID の隣にあるチェックボックスをオンにし、[無効化（Invalidate）] をクリックします。

管理者の名前の変更

Cisco ISE では GUI からユーザ名を変更できます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

ステップ 1 管理者ポータルにログインします。

ステップ 2 Cisco ISE UI の右上にリンクとして表示されるユーザ名をクリックします。

ステップ 3 表示される [管理者ユーザ（Admin User）] ページに新しいユーザ名を入力します。

ステップ 4 変更するアカウントに関するその他の詳細を編集します。

ステップ 5 [保存（Save）] をクリックします。

外部 ID ストアを使用した Cisco ISE への管理アクセス

Cisco ISE では、Active Directory、LDAP、RSA SecureID などの外部 ID ストアを介して管理者を認証できます。外部 ID ストアを介した認証の提供に使用できる次の 2 つのモデルがあります。

- 外部認証および許可：管理者に関してローカル Cisco ISE データベースで指定されたクレデンシャルはなく、許可は、外部 ID ストア グループ メンバーシップのみに基づきます。このモデルは、Active Directory および LDAP 認証で使用されます。
- 外部認証および内部許可：管理者の認証クレデンシャルは外部 ID ソースから取得され、許可および管理者ロール割り当てはローカル Cisco ISE データベースを使用して行われます。このモデルは、RSA SecurID 認証で使用されます。この方法では、外部 ID ストアとローカル Cisco ISE データベースの両方で同じユーザ名を設定する必要があります。

認証プロセス時、Cisco ISE は、外部 ID ストアとの通信が確立されなかった場合や失敗した場合はフォールバックし、内部 ID データベースから認証の実行を試行するように設計されています。また、外部認証が設定されている管理者には、ブラウザを起動してログインセッションを開始すると必ず、ログイン ダイアログの [ID ストア（Identity Store）] ドロップダウン セレクタから [内部（Internal）] を選択して Cisco ISE ローカル データベースを介した認証を要求するオプションが依然として表示されます。

（注） 外部管理者認証を提供するこの方法は、管理者ポータルを介してのみ設定できます。Cisco ISE コマンドライン インターフェイス（CLI）では、これらの機能は設定されません。

ネットワークに既存の外部 ID ストアがまだない場合は、必要な外部 ID ストアをインストールし、これらの ID ストアにアクセスするように Cisco ISE が設定されていることを確認します。

外部認証および許可

デフォルトでは、Cisco ISE によって内部管理者認証が提供されます。外部認証を設定するには、外部 ID ストアで定義している外部管理者アカウントのパスワード ポリシーを作成する必要があります。次に、結果的に外部管理者 RBAC ポリシーの一部となるこのポリシーを外部管理者グループに適用できます。

ネットワークでは、外部 ID ストア経由の認証を提供するほかに、Common Access Card（CAC）認証デバイスを使用する必要もある場合があります。

外部認証を設定するには、次の手順を実行する必要があります。

- 外部 ID ストアを使用してパスワード ベースの認証を設定します。
- 外部管理者グループを作成します。

- 外部管理者グループ用のメニュー アクセスとデータ アクセスの権限を設定します。
- 外部管理者認証の RBAC ポリシーを作成します。

外部認証のプロセス フロー

管理者がログインすると、ログインセッションはそのプロセスにおいて次の手順で処理されます。

1. 管理者が RSA SecurID チャレンジを送信します。
2. RSA SecurID は、チャレンジ応答を返します。
3. 管理者は、ユーザ ID とパスワードを入力する場合と同様に、ユーザ名および RSA SecurID チャレンジ応答を Cisco ISE ログイン ダイアログに入力します。
4. 管理者は、指定した ID ストアが外部 RSA SecurID リソースであることを確認します。
5. 管理者は、[ログイン（Login）] をクリックします。

ログイン時、管理者には、RBAC ポリシーで指定されたメニュー アクセス項目とデータ アクセス項目のみが表示されます。

外部 ID ストアを使用したパスワード ベースの認証の設定

最初に、Active Directory や LDAP などの外部 ID ストアを使用して認証を行う管理者のためのパスワード ベースの認証を設定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）] > [認証（Authentication）]** を選択します。

ステップ 2 [認証方式（Authentication Method）] タブで、[パスワードベース（Password Based）] を選択し、すでに設定されている外部 ID ソースの 1 つを選択します。たとえば、作成した Active Directory インスタンスを選択します。

ステップ 3 外部 ID ストアを使用して認証を行う管理者のためのその他の特定のパスワード ポリシーを設定します。

ステップ 4 [保存（Save）] をクリックします。

関連トピック

外部 ID ストアを使用した Cisco ISE への管理アクセス （25 ページ）
外部認証および許可 （25 ページ）
外部認証のプロセス フロー （26 ページ）

外部管理者グループの作成

外部 Active Directory または LDAP 管理者グループを作成する必要があります。これにより、Cisco ISE は外部 Active Directory または LDAP ID ストアで定義されているユーザ名を使用して、ログイン時に入力した管理者ユーザ名とパスワードを検証します。

Cisco ISE は、外部リソースから Active Directory または LDAP グループ情報をインポートし、それをディクショナリ属性として保存します。次に、この属性を、外部管理者認証方式用の RBAC ポリシーを設定するときのポリシー要素の 1 つとして指定できます。

ステップ 1 [管理（Administration）] > [システム（System）] > [管理者アクセス（Admin Access）] > [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）] をクリックします。

ステップ 3 名前とオプションの説明を入力します。

ステップ 4 [外部（External）] オプション ボタンを選択します。

Active Directory ドメインに接続し、参加している場合は、Active Directory インスタンス名が [名前（Name）] フィールドに表示されます。

ステップ 5 [外部グループ（External Groups）] ドロップダウン リスト ボックスから、この外部管理者グループにマッピングする Active Directory グループを選択します。

追加の Active Directory グループをこの外部管理者グループにマッピングするために「+」記号をクリックします。

ステップ 6 [保存（Save）] をクリックします。

関連トピック

Cisco ISE 管理者グループ （3 ページ）

外部管理者グループのメニュー アクセス権限とデータ アクセス権限の設定

外部管理者グループに割り当てることができるメニュー アクセス権限とデータ アクセス権限を設定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）] > [権限（Permissions）]** を選択します。

ステップ 2 次のいずれかをクリックします。

- [メニュー アクセス（Menu Access）] : 外部管理者グループに属するすべての管理者に、メニューまたはサブメニュー レベルでの権限を付与することができます。メニューアクセス権限によって、アクセスできるサブメニューまたはメニューが決定されます。
- [データ アクセス（Data Access）] : 外部管理者グループに属するすべての管理者に、データ レベルでの権限を付与することができます。データ アクセス権限によって、アクセスできるデータが決定されます。

ステップ 3 外部管理者グループのメニュー アクセス権限とデータ アクセス権限を指定します。

ステップ 4 [保存（Save）] をクリックします。

外部管理者認証の RBAC ポリシーの作成

外部 ID ストアを使用して管理者を認証するように Cisco ISE を設定し、同時にカスタム メニュー アクセス権限とデータ アクセス権限を指定するには、新しい RBAC ポリシーを設定する必要があります。このポリシーには、認証用の外部管理者グループ、および外部認証と許可を管理するための Cisco ISE メニュー アクセス権限とデータ アクセス権限が存在している必要があります。

（注） これらの新しい外部属性を指定するように既存（システムプリセット）の RBAC ポリシーを変更することはできません。「テンプレート」として使用する必要がある既存のポリシーがある場合は、そのポリシーを複製し、名前を変更してから、新しい属性を割り当てます。

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）] > [ポリシー（Policy）]** を選択します。

ステップ 2 ルール名、外部管理者グループ、および権限を指定します。

適切な外部管理者グループが正しい管理者ユーザ ID に割り当てられている必要があることに注意してください。問題の管理者が正しい外部管理者グループに関連付けられていることを確認します。

ステップ 3 [保存（Save）] をクリックします。

管理者としてログインした場合、Cisco ISE RBAC ポリシーが管理者 ID を認証できないと、Cisco ISE では、「認証されていない」ことを示すメッセージが表示され、管理者ポータルにアクセスできません。

関連トピック

RBAC ポリシー （14 ページ）

内部許可を伴う認証に対する外部 ID ストアを使用した管理アクセスの設定

この方法では、外部 ID ストアとローカル Cisco ISE データベースの両方で同じユーザ名を設定する必要があります。外部 RSA SecurID ID ストアを使用して管理者認証を提供するように Cisco ISE を設定している場合、管理者のクレデンシャル認証が RSA ID ストアによって実行されます。ただし、許可（ポリシー アプリケーション）は、依然として Cisco ISE 内部データベースに従って行われます。また、外部認証と許可とは異なる、留意する必要がある次の 2 つの重要な要素があります。

- 管理者の特定の外部管理者グループを指定する必要はありません。
- 外部 ID ストアとローカル Cisco ISE データベースの両方で同じユーザ名を設定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）]** を選択します。

ステップ 2 外部 RSA ID ストアの管理者ユーザ名が Cisco ISE にも存在することを確認します。[パスワード（Password）] の下の [外部（External）] オプションをクリックします。

（注） 外部管理者ユーザ ID のパスワードを指定する必要はなく、特別に設定されている外部管理者グループを関連付けられている RBAC ポリシーに適用する必要もありません。

ステップ 3 [保存（Save）] をクリックします。