CHAPTER 6

管理者および管理者アクセス ポリシーの管理

Cisco Identity Services Engine (ISE) 管理者は、管理ユーザとも呼ばれ、Cisco ISE 管理者ポータルを使用して、特定のタイプの管理タスクを管理および実行します。

この章では、Cisco ISE が管理者、および管理者によるロールベース アクセス コントロール ポリシー（RBAC）、権限、および設定へのアクセスを管理する方法について説明します。

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、次を実行できます。

- 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。

この章の内容は、次のとおりです。

- 「Cisco ISE 管理者」（P.6-1）
- 「Cisco ISE 管理者グループ」（P.6-3）
- 「Cisco ISE への管理アクセス」（P.6-7）

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内容を実行します。

- 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を管理します。
- 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を管理します。
- 管理者およびユーザ 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を使用して 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 への管理者アクセスのみを対象としています。このロールは、CLI 管理者ユーザ（CLI 管理者とも呼ばれる）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 であり、パスワードはセットアップ時に定義されます。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、別の管理者によって編集できます（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。

関連項目

- 「Cisco ISE 管理者グループ」（P.6-3）
- 「新しい Cisco ISE 管理者の作成」（P.6-2）

CLI 管理者と Web ベース管理者の権限

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 管理者の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ための Web ベースの管理者を作成することを推奨します。

新しい Cisco ISE 管理者の作成

Cisco ISE 管理者には、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、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）] 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　次のいずれかを選択します。

- **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（Administrators）] 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、# $ ' ( ) * + - ./ @ _ です。

認証のために RSA または RADIUS 外部 ID ソースを使用し、認証のための内部 ID ソースで同じ管理者アカウントを作成している場合のみ、[外部（External）] チェックボックスをオンにします。

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。

関連項目

- 「Cisco ISE 管理者」（P.6-1）
- 「Cisco ISE 管理者グループ」（P.6-3）

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。

読み取り専用機能は、Cisco ISE のいずれの管理者アクセスにも使用できません。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 6-1　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
ヘルプデスク管理者	クエリー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
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値の設定（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 レベルのコンフィギュレーションのタスクを実行できません

表 6-1　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 （続き）

管理者グループ ロール	アクセス レベル	権限	制約事項
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または ID 管理またはシステムレベルのコンフィギュレーションのタスクを実行できません
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または ID 管理またはシステムレベルのコンフィギュレーションのタスクを実行できません
ポリシー管理者	認証、許可、ポスチャ、プロファイラ、およびクライアントのプロビジョニングに関連する、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	Cisco ISE のすべての ID 管理またはシステムレベルのコンフィギュレーションのタスクを実行できません

表 6-1　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 （続き）

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の有効化または無効化 • 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コンフィギュレーションのタスクを実行できません
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。	—

表 6-1　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 （続き）

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。	[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の有効化または無効化 • 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	Cisco ISE のすべてのポリシー管理またはシステムレベルのコンフィギュレーションのタスクを実行できません
外部 RESTful サービス（ERS）管理者 [1]	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）ゲスト	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できます	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。

1. ERS API の詳細については、『*Cisco Identity Services Engine API Reference Guide, Release 1.2*』を参照してください

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。

はじめる前に

外部管理者グループ タイプを設定するには、「外部 ID ソースとしての Active Directory」（P.14-9）、「LDAP」（P.14-20）、「RADIUS トークン ID ソース」（P.14-27）、および「RSA ID ソース」（P.14-33）にあるガイドラインに従って 1 つ以上の外部 ID ストアを指定しておく必要があります。

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文字は、スペース、# $ & ' ( ) * + - ./ @ _ です。

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 ベースに格納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　ユーザを [管理者グループ ユーザ（Admin Group Users）] テーブルに追加するには、[追加（Add）] をクリックします。[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。

関連項目

- 「Cisco ISE 管理者グループ」（P.6-3）
- 「外部 ID ソースとしての Active Directory」（P.14-9）
- 「LDAP」（P.14-20）
- 「RADIUS トークン ID ソース」（P.14-27）
- 「RSA ID ソース」（P.14-33）

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 でのロールベース アクセス コントロール（RBAC）」（P.6-8）
- 「管理者アクセスの設定」（P.6-13）

Cisco ISE でのロールベース アクセス コントロール（RBAC）

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 ポリシーにより、個々の管理者ユーザまたは管理者グループに適用される指定のロールベース アクセス権限設定を使用して、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。

関連項目

「Cisco ISE 管理者グループ」（P.6-3）

ロールベースの権限

Cisco ISE では、メニューとデータのレベルで権限を設定することができ、メニュー アクセス権限とデータ アクセス権限と呼ばれます。

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。この機能を使用すると、メニュー レベルのアクセス権を制限または有効化するように、権限を作成できます。

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フル 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、ユーザの 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、管理者グループに基づいてメニュー項目や ID グループ データ要素へのアクセスを管理者に許可したり拒否することができます。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。

関連項目

- 「Cisco ISE でのロールベース アクセス コントロール（RBAC）」（P.6-8）
- 「デフォルトのメニュー アクセス権限」（P.6-8）
- 「デフォルトのデータ アクセス権限」（P.6-11）

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。表 6-2 に、デフォルトのメニュー アクセス権限を示します。

事前定義されたメニュー 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 アクセス権限も作成できます。

表 6-2　デフォルトのメニュー アクセス権限

メニュー アクセス名	RBAC グループ	許容されるメニュー項目セット [1]
スーパー管理者のメニュー アクセス	スーパー管理者	• [操作（Operations）] > [すべて（All）] メニュー項目 • [ポリシー（Policy）] > [すべて（All）] メニュー項目 • [管理（Administration）] > [すべて（All）] メニュー項目
ポリシー管理者のメニュー アクセス	ポリシー管理者	• [操作（Operations）] > [すべて（All）] メニュー項目 • [ポリシー（Policy）] > [すべて（All）] メニュー項目 • [管理（Administration）] > – [ID の管理（Identity Management）] > [すべて（All）] メニュー項目 – [システム（System）] > [設定（Settings）]
ヘルプ デスク管理者のメニュー アクセス	ヘルプデスク管理者	• [操作（Operations）] > [すべて（All）] メニュー項目
ID 管理者のメニュー アクセス	ID 管理者	• [操作（Operations）] > [すべて（All）] メニュー項目 • [管理（Administration）] > – [ID の管理（Identity Management）] > [すべて（All）] メニュー項目
ネットワーク デバイス メニュー アクセス	ネットワーク デバイス管理者	• [操作（Operations）] > [すべて（All）] メニュー項目 • [管理（Administration）] > – [ネットワーク リソース（Network Resources）] > [すべて（All）] メニュー項目
システム管理者のメニュー アクセス	システム管理者	• [操作（Operations）] > [認証、アラーム、レポート、およびトラブルシューティング（Authentication, Alarms, Reports, and Troubleshoot）] • [管理（Administration）] > – [システム（System）] > [すべて（All）] メニュー項目

表 6-2　デフォルトのメニュー アクセス権限 （続き）

メニュー アクセス名	RBAC グループ	許容されるメニュー項目セット [1]
RBAC 管理者のメニュー アクセス	RBAC 管理者	• [操作（Operations）] > [エンドポイント保護サービス（Endpoint Protection Service）] を除く [すべて（All）] メニュー項目 • [管理（Administration）] > – [管理者アクセス（Admin Access）] > [すべて（All）] メニュー項目
MnT 管理者のメニュー アクセス	MnT 管理者	• [操作（Operations）] > [すべて（All）] メニュー項目

1. 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。

関連項目

- 「Cisco ISE でのロールベース アクセス コントロール（RBAC）」（P.6-8）
- 「メニュー アクセス権限の設定」（P.6-10）
- 「デフォルトのデータ アクセス権限」（P.6-11）

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できます。管理者のロールに応じて、特定のメニュー オプションだけへのアクセスを許可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）] > [メニュー アクセス（Menu Access）] を選択します。

ステップ 2　[追加（Add）] をクリックして、[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。

関連項目

- 「Cisco ISE でのロールベース アクセス コントロール（RBAC）」（P.6-8）
- 「ロールベースの権限」（P.6-8）
- 「デフォルトのメニュー アクセス権限」（P.6-8）
- 「デフォルトのデータ アクセス権限」（P.6-11）

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。表 6-3 に、デフォルトのデータ アクセス権限を示します。

RBAC ポリシーは、管理者（RBAC）グループ、メニュー アクセス、およびデータ 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 ポリシーは次の形式になります。

admin_group= *スーパー管理者*の場合、*SuperAdmin メニュー アクセス*権限 + *SuperAdmin データ アクセス*権限を割り当てます。

事前定義されたデータ アクセス権限とは別に、Cisco ISE では、RBAC ポリシーに関連付けることができるカスタム データ アクセス権限も作成できます。

表 6-3　デフォルトのデータ アクセス権限

データ アクセス名	RBAC グループ	許容される管理者グループ	許容されるネットワーク デバイス グループ
スーパー管理者のデータ アクセス	スーパー管理者	• 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	• すべてのロケーション • すべてのデバイス タイプ
ポリシー管理者のデータ アクセス	ポリシー管理者	• ユーザ ID グループ • エンドポイント ID グループ	なし
ID 管理者のデータ アクセス	ID 管理者	• ユーザ ID グループ • エンドポイント ID グループ	なし
ネットワーク管理者のデータ アクセス	ネットワーク デバイス管理者	なし	• すべてのロケーション • すべてのデバイス タイプ
システム管理者のデータ アクセス	システム管理者	• 管理者グループ	なし
RBAC 管理者のデータ アクセス	RBAC 管理者	• 管理者グループ	なし

関連項目

- 「Cisco ISE でのロールベース アクセス コントロール（RBAC）」（P.6-8）
- 「データ アクセス権限の設定」（P.6-12）
- 「ロールベースの権限」（P.6-8）
- 「デフォルトのメニュー アクセス権限」（P.6-8）

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できます。管理者のロールに基づいて、データ選択のみのアクセス権を指定するように選択できます。

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）] をクリックして、[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 アクセス権（Full 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。

関連項目

- 「Cisco ISE でのロールベース アクセス コントロール（RBAC）」（P.6-8）
- 「ロールベースの権限」（P.6-8）
- 「デフォルトのメニュー アクセス権限」（P.6-8）
- 「デフォルトのデータ アクセス権限」（P.6-11）

管理者アクセス 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、変更または削除できません。このページでは、職場専用の管理者グループのカスタム 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することもできます。

はじめる前に

- 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。
- 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）] > [許可（Authorization）] > [ポリシー（Policy）] を選択します。

RBAC の [ポリシー（Policy）] ページには、デフォルトの管理グループ用にすぐに使用できる事前定義されたポリシーのセットが含まれています。

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。

関連項目

- 「管理者グループの作成」（P.6-6）
- 「Cisco ISE 管理者」（P.6-1）
- 「デフォルトのメニュー アクセス権限」（P.6-8）

管理者アクセスの設定

Cisco ISE を使用すると、セキュリティ向上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 [管理者アカウント設定（Administrator Account Settings）] で定義したパスワード 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、UTF-8 文字を使用した管理者パスワードはサポートしません。次の管理アクセス設定ができます。

- 「同時管理セッションの最大数およびログイン バナーの設定」（P.6-13）
- 「選択 IP アドレスから Cisco ISE への管理アクセスの許可」（P.6-14）
- 「管理者アカウントのパスワード ポリシーの設定」（P.6-14）
- 「管理者のセッション タイムアウトの設定」（P.6-15）

同時管理セッションの最大数およびログイン バナーの設定

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。管理者がログインする前とログインした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 バナーは無効です。

はじめる前に

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。

関連項目

- 「管理者アクセスの設定」（P.6-13）
- 「選択 IP アドレスから Cisco ISE への管理アクセスの許可」（P.6-14）

選択 IP アドレスから 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。これらの制限は、インライン ポスチャ ノードには適用できません。

はじめる前に

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 アドレス（IP Access>）] を選択します。

ステップ 2　[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 3　[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 4　[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 5　[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 6　変更を保存するには、[保存（Save）] をクリックします。

関連項目

- 「Cisco ISE 管理者」（P.6-1）
- 「Cisco ISE 管理者グループ」（P.6-3）

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、UTF-8 文字を使用した管理者パスワードはサポートしません。

はじめる前に

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）] > [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：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）] タブで、管理者パスワード ポリシーの設定に示されているように値を入力します。

（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。

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。

関連項目

- 「Cisco ISE 管理者」（P.6-1）
- 「管理者グループの作成」（P.6-6）
- 「外部 ID ストアを使用した Cisco ISE への管理アクセス」（P.6-17）

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。

はじめる前に

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。

関連項目

- 「アクティブな管理セッションの終了」（P.6-16）
- 「Cisco ISE 管理者」（P.6-1）
- 「管理者グループの作成」（P.6-6）
- 「セッション タイムアウトとセッション情報の設定」（P.A-19）

アクティブな管理セッションの終了

Cisco ISE はアクティブな管理セッションをすべて表示するので、必要がある場合は、そこから任意のセッションを選択し、いつでも終了させることができます。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はログインし、セッションの一部を終了できます。

はじめる前に

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。

関連項目

「セッション タイムアウトとセッション情報の設定」（P.A-19）

管理者名の変更

Cisco ISE では、GUI からユーザ名を変更することができます。

はじめる前に

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、管理者ポート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。

関連項目

- 「外部認証および許可」（P.6-17）
- 「外部 ID ソースとしての Active Directory」（P.14-9）
- 「LDAP」（P.14-20）
- 「RADIUS トークン ID ソース」（P.14-27）
- 「RSA ID ソース」（P.14-33）

外部認証および許可

デフォルトでは、Cisco ISE は内部管理者認証を提供します。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、次の内容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。
- 外部管理グループを作成します。
- 外部管理者グループのメニュー アクセス権限およびデータ アクセス権限を設定します。
- 外部管理者認証用の RBAC ポリシーを作成します。

関連項目

- 「管理者アカウントのパスワード ポリシーの設定」（P.6-14）
- 「管理者 CAC 認証のための Cisco ISE の設定」（P.5-11）
- 「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」（P.6-18）
- 「外部管理者グループの作成」（P.6-18）
- 「外部管理者グループのメニュー アクセス権限およびデータ アクセス権限の設定」（P.6-19）
- 「外部管理者認証用の RBAC ポリシーの作成」（P.6-19）

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する管理者のパスワード 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、すでに設定しているいずれかの外部 ID ソースを選択します。たとえば、作成した Active Directory インスタンス。

ステップ 3　外部 ID ストアを使用して認証する管理者に必要な他の特定のパスワード ポリシー設定をします。

ステップ 4　[保存（Save）] をクリックします。

関連項目

「管理者パスワード ポリシーの設定」（P.A-18）

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）] > [追加（Add）] を選択します。

ステップ 2　名前と説明（任意）を入力します。

ステップ 3　[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 4　[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 5　[保存（Save）] をクリックします。

関連項目

「管理者グループの作成」（P.6-6）

外部管理者グループのメニュー アクセス権限およびデータ 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：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のレベルで権限を付与できます。メニュー アクセス権限は、管理者がアクセスできるメニューまたはサブメニューまたはメニューを決定します。
- データ アクセス：外部管理者グループに属するすべての管理者に、データのレベルで権限を付与できます。データ アクセス権限は、管理者がアクセスできるデータを決定します。

ステップ 3　外部管理者グループのメニュー アクセス権限またはデータ 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。

関連項目

- 「メニュー アクセス権限の設定」（P.6-10）
- 「デフォルトのデータ アクセス権限」（P.6-11）

外部管理者認証用の 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 のメニュー 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。

関連項目

- 「Cisco ISE 管理者グループ」（P.6-3）
- 「外部 ID ストアを使用した Cisco ISE への管理アクセス」（P.6-17）

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てください。

（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。

関連項目

「新しい Cisco ISE 管理者の作成」（P.6-2）

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、プロセスで次の手順を通過します。

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。

関連項目

「外部 ID ストアを使用した Cisco ISE への管理アクセス」（P.6-17）