



システム管理者の管理

システム管理者は、ネットワーク内の ACS サーバを展開、設定、管理、および監視します。システム管理者は、ACS 管理インターフェイスを使用して、ACS でさまざまな操作を実行できます。ACS で管理者を定義するとき、パスワードおよびロールまたはロールのセットを割り当てます。ロールによって、さまざまな操作に対する管理者のアクセス権が決定されます。

管理者アカウントを作成するとき、最初にパスワードを割り当てます。管理者は、あとで ACS Web インターフェイスを使用して、このパスワードを変更できます。割り当てられているロールに関係なく、管理者は自分のパスワードを変更できます。

ACS では、次の設定可能なオプションを使用して、管理者パスワードを管理できます。

- **Password Complexity** : パスワードの必要な長さおよび文字タイプを指定します。
- **Password History** : 同じパスワードを繰り返し使用できないようにします。
- **Password Lifetime** : 指定された時間が経過したあと、管理者に対してパスワードの変更を強制します。
- **Account Inactivity** : 指定時間使用されていない管理者アカウントをディセーブルにします。
- **Password Failures** : 管理者アカウントが指定した回数連続してログインに失敗した場合に、そのアカウントをディセーブルにします。

さらに、ACS には、管理者が ACS 管理 Web インターフェイスへのアクセスに使用する IP アドレスおよびセッション継続時間を決定する、設定可能なオプションがあります。セッション継続時間を経過すると、アイドルセッションはシステムからログアウトします。

Monitoring and Report Viewer を使用して、システムへの管理者アクセスを監視できます。システムに現在アクセスしている管理者またはアクセスしようとしている管理者を監視するには、**Administrator Access** レポートを使用します。

Administrator Entitlement レポートを表示すると、管理者が持っているアクセス権、管理者が加えた設定変更、および管理者アクセスの詳細を表示できます。また、**Configuration Change** および **Operational Audit** レポートを使用して、各管理者が実行する特定の操作の詳細を表示することもできます。

ACS Web インターフェイスの **[System Administrator]** セクションでは、次の操作を実行できます。

- 管理者アカウントの作成、編集、複製、または削除
- 他の管理者のパスワード変更
- 事前定義済みのロールの表示
- 管理者へのロールの関連付け
- パスワードの複雑さ、アカウントのライフタイム、非アクティブなアカウントなどの認証設定

- 管理者セッションの設定
- 管理者アクセスの設定

ACS 5.8 に初めてログインすると、事前定義済みの管理者ユーザ名 (*ACSAdmin*) の入力を要求するプロンプトが表示され、事前定義済みのパスワード名 (*default*) を変更することを要求されます。パスワードを変更したあと、システムの設定を開始できます。

事前定義済みの管理者には、すべての ACS リソースに対するスーパー管理者権限 (*Create*、*Read*、*Update*、*Delete*、および *eXecute (CRUDX)*) があります。プライマリ インスタンスにセカンダリ インスタンスを登録すると、プライマリ インスタンスで作成された任意のアカウントを使用できます。プライマリ インスタンスで作成したクレデンシャルは、セカンダリ インスタンスに適用されます。



(注)

インストール後、ACS に初めてログインするときに、ACS Web インターフェイスからログインしてライセンスをインストールする必要があります。インストール後すぐに CLI から ACS にログインすることはできません。

ここでは、次の内容について説明します。

- [管理者ロールおよびアカウントについて \(16-2 ページ\)](#)
- [システム管理者およびアカウントの設定 \(16-3 ページ\)](#)
- [ロールについて \(16-3 ページ\)](#)
- [管理者アカウントの作成、複製、編集、および削除 \(16-8 ページ\)](#)
- [事前定義済みのロールの表示 \(16-14 ページ\)](#)
- [管理者の認証設定 \(16-15 ページ\)](#)
- [セッションアイドルタイムアウトの設定 \(16-17 ページ\)](#)
- [管理者のアクセス設定 \(16-18 ページ\)](#)
- [管理アクセス コントロールの使用 \(16-19 ページ\)](#)
- [RADIUS ID および RSA SecurID サーバに対する管理者の認証 \(16-24 ページ\)](#)
- [管理者パスワードのリセット \(16-30 ページ\)](#)
- [管理者パスワードの変更 \(16-30 ページ\)](#)

管理者ロールおよびアカウントについて

ACS 5.8 に初めてログインすると、事前定義済みの管理者ユーザ名 (*ACSAdmin*) の入力を要求するプロンプトが表示され、事前定義済みのパスワード名 (*default*) を変更することを要求されます。Cisco Secure ACS リリース 5.8 の *acsadmin* アカウントは、*SuperAdmin* ロールのほかの管理者アカウントと同様です。*SuperAdmin* ロールの別のリカバリ管理者アカウントがある場合、デフォルトの *acsadmin* アカウントは無効になっているか、削除されています。アカウントの無効化の条件は、パスワードの有効期間、アカウントの無効化、および失敗した認証試行回数の超過などのアカウント無効化の条件は、デフォルトの *acsadmin* アカウントにも適用されません。

パスワードを変更したあと、システムの設定を開始できます。事前定義済みの管理者には、すべての ACS リソースに対するスーパー管理者権限 (*Create*、*Read*、*Update*、*Delete*、および *eXecute (CRUDX)*) があります。

きめ細かなアクセス コントロールが必要ない場合は、SuperAdmin ロールが最も便利です。このロールは、事前定義済みの ACSAdmin アカウントに割り当てられています。

きめ細かなアクセス コントロールを行うには、次の手順を実行します。

-
- ステップ 1** 管理者を定義します。システム管理者およびアカウントの設定 (16-3 ページ) を参照してください。
- ステップ 2** 管理者にロールを関連付けます。ロールについて (16-3 ページ) を参照してください。
- これらの手順が完了すると、定義された管理者はシステムにログインして操作を開始できます。
-

認証について

認証要求は、すべての管理セッションに対して最初に行われる処理です。認証に失敗すると、管理セッションが終了します。認証に成功した場合、管理セッションは管理者がログアウトするかセッションがタイムアウトするまで続きます。

ACS 5.8 では、ユーザ資格情報 (ユーザ名とパスワード) を使用してすべてのログイン操作を認証します。その後、ACS では、管理者とロールの定義を使用して、適切な権限を取得し、後続の認可要求に対応します。

ACS ユーザ インターフェイスには、必要な管理者特権を持っている機能とオプションだけが表示されます。



(注) システムの変更が反映されるように、しばらく待ってから再度ログインしてください。

関連項目

- 管理者ロールおよびアカウントについて (16-2 ページ)
- システム管理者およびアカウントの設定 (16-3 ページ)

システム管理者およびアカウントの設定

ここでは、次の内容について説明します。

- ロールについて (16-3 ページ)
- 管理者アカウントとロールの関連付け (16-7 ページ)
- 管理者アカウントの作成、複製、編集、および削除 (16-8 ページ)
- ロール プロパティの表示 (16-14 ページ)

ロールについて

ロールは一般的な管理者タスクで構成され、それぞれのタスクに権限のセットが関連付けられています。各管理者には複数の事前定義済みのロールを指定でき、1つのロールを複数の管理者に適用できます。これにより、1人の管理者に複数のタスクを設定したり、1つのタスクに複数の管理者を設定したりできます。

ロールを割り当てるには、[Administrator Accounts] ページを使用します。一般的に、最初に正確にロールを定義しておくことを推奨します。詳細は [管理者アカウントの作成、複製、編集、および削除 \(16-8 ページ\)](#) を参照してください。

ロールの割り当て

内部管理者アカウントにロールを割り当てることができます。ACS 5.8 には、内部管理者にロールを割り当てるために、以下の 2 通りの方法が用意されています。

- 静的ロール割り当て：ロールは、内部管理者アカウントに手動で割り当てられます。
- 動的ロール割り当て：ロールは、AAC 認可ポリシーの規則に基づいて割り当てられます。

静的ロールの割り当て

ACS 5.8 では、内部管理者アカウントに管理者ロールを静的に割り当てることができます。これは内部管理者アカウントにのみ適用されます。この静的オプションを選択した場合は、それぞれの内部管理者アカウントには管理者ロールを手動で選択する必要があります。管理者がアカウントにアクセスしようとした場合に、その管理者が静的ロール割り当てとともに管理者内部 ID ストアに設定されていると、ID ポリシーだけが認証で実行されます。認可ポリシーはスキップされます。ID ポリシーが正常に実行された後で、管理者には管理者アカウント用に選択されたロールが割り当てられます。

動的ロールの割り当て

ACS 5.8 では、内部管理者アカウントに管理者ロールを静的に割り当てることができます。

管理者アカウントが外部または内部 ID ストアに設定され、かつ動的ロール割り当てがある場合、ACS は、認可ポリシーを評価し、その結果として、管理者ロールのリストを取得して動的に使用するか、[Deny Access] を使用します。SuperAdmin が管理者に動的ロールを割り当て、認証ポリシーを設定しない場合、その管理者アカウントの認証はデフォルト値「deny access」を使用します。その結果、この管理者アカウントの認可は拒否されます。ただし、管理者に静的ロールを割り当てると、認可ポリシーは、その管理者の認可にまったく影響しません。

選択したロールに基づいて、ACS は認証を行い、管理者のアクセス制限と認証を管理します。Deny Access が評価の結果である場合、ACS は管理者へのアクセスを拒否し、カスタマー ログに失敗の理由を記録します。



(注)

ACS Web ユーザーインターフェイスには、自分が特権を持っている機能だけが表示されます。たとえば、ロールが Network Device Admin の場合、[System Administration] ドロウは表示されません。これは、そのドロウ内の機能に対する権限がないためです。

権限

権限は、特定の管理タスクに適用されるアクセス権です。権限の構成要素は次のとおりです。

- リソース：管理者がアクセスできる ACS コンポーネント（ネットワーク リソース、ポリシー要素など）のリスト。
- 特権：特権には、Create、Read、Update、Delete、および eExecute (CRUDX) があります。特定のリソースに適用できない特権もあります。たとえば、ユーザー リソースは実行できません。

特権のない管理者にリソースを割り当てても、その管理者はリソースにアクセスできません。また、権限は独立しています。Create、Update、および Delete 特権がリソースに適用されている場合、Read 特権は使用できません。

オブジェクトに権限が定義されていない場合、管理者はこのオブジェクトにアクセスできず、読み取ることもできません。



(注) 権限は変更できません。

事前定義済みのロール

ACS 5.8 には、Provisioning Admin と Operations Admin という 2 つの新規既定管理者ロールが導入されています。これらの 2 つの新規ロールを使用して、新規の管理者アカウントを作成できます。管理者アカウントの作成時、この 2 つの管理者ロールを同時に使用することはできませんし、その他の管理者ロールと共に使用することもできません。

表 16-1 に、ACS の事前定義済みのロールを示します。

表 16-1 事前定義済みのロールの説明

ロール	権限
ChangeAdminPassword	このロールは、他の管理者アカウントを管理する ACS 管理者用です。このロールが割り当てられた管理者は、他の管理者のパスワードを変更できます。
ChangeUserPassword	このロールは、内部ユーザアカウントを管理する ACS 管理者用です。このロールが割り当てられた管理者は、内部ユーザのパスワードを変更できます。
NetworkDeviceAdmin	このロールは、デバイスの追加、更新、削除など、ACS ネットワーク デバイス リポジトリの管理だけを実行する必要がある ACS 管理者用です。このロールには、次の権限があります。 <ul style="list-style-type: none"> 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 [Network Resources] ドロウ内のすべての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
OperationsAdmin	このロールは、既存のいくつかの管理者アカウントに追加のリソースと特権を組み合わせたロールです。 OperationsAdmin のリソースと権限を参照するには、次のようにします。 <ol style="list-style-type: none"> ACS Web インターフェイスから [System Administration] > [Administrators] > [Roles] を選択します。 [OperationsAdmin] の近くにあるラジオボタンをクリックします。 [View] をクリックします。 ACS は OperationsAdmin に関連するリソースと権限を表示します。 ACS の他の管理者と同様、外部データベースに対して OperationsAdmin を認証できます。 (注) 管理者アカウントを作成する時に、他の管理者ロールと OperationsAdmin ロールを組み合わせることはできません。 (注) 他の管理者と同様に、ProvisioningAdmin にロール、リソース、特権を割り当てることができます。しかし、OperationsAdmin をリカバリ管理者アカウントとして割り当てることはできません。

表 16-1 事前定義済みのロールの説明 (続き)

ロール	権限
PolicyAdmin	<p>このロールは、ACS アクセス サービスとアクセス ポリシー規則、およびポリシー規則によって参照されるポリシー要素を作成および管理する ACS ポリシー管理者用です。このロールには、次の権限があります。</p> <ul style="list-style-type: none"> • ポリシーで使用されているすべての要素（認可プロファイル、NDG、IDG、条件など）に対する読み取りおよび書き込み権限 • サービス ポリシーに対する読み取りおよび書き込み権限
ProvisioningAdmin	<p>このロールは、既存のいくつかの管理者アカウントに追加のリソースと特権を組み合わせたロールです。</p> <p>ProvisioningAdmin のリソースと権限を参照するには、次のようにします。</p> <ol style="list-style-type: none"> 1. ACS Web インターフェイスから [System Administration] > [Administrators] > [Roles] を選択します。 2. [ProvisioningAdmin] の近くにあるラジオボタンをクリックします。 3. [View] をクリックします。 <p>ACS は ProvisioningAdmin に関連するリソースと権限を表示します。</p> <p>ACS の他の管理者と同様、外部データベースに対して ProvisioningAdmin を認証できます。</p> <p>(注) 管理者アカウントを作成する時に、他の管理者ロールと ProvisioningAdmin ロールを組み合わせることはできません。</p> <p>(注) 他の管理者と同様に、ProvisioningAdmin にロール、リソース、特権を割り当てることができます。しかし、ProvisioningAdmin をリカバリ管理者アカウントとして割り当てることはできません。</p>
ReadOnlyAdmin	<p>このロールは、ACS ユーザ インターフェイスのすべての部分に対する読み取り専用アクセスを必要とする ACS 管理者用です。</p> <p>このロールには、すべてのリソースに対する読み取り専用アクセス権があります。</p>
ReportAdmin	<p>このロールは、ACS Monitoring and Report Viewer にアクセスしてレポートまたはモニタリング データだけを生成および表示する必要がある管理者用です。</p> <p>このロールには、ログに対する読み取り専用アクセス権があります。</p>
SecurityAdmin	<p>このロールは、ACS 管理者アカウントの作成、更新、または削除、管理ロールの割り当て、および ACS パスワード ポリシーの変更を行うために必要です。このロールには、次の権限があります。</p> <ul style="list-style-type: none"> • 内部プロトコル ユーザおよび管理者パスワード ポリシーに対する読み取りおよび書き込み権限 • 管理者アカウント設定に対する読み取りおよび書き込み権限 • 管理者アクセス設定に対する読み取りおよび書き込み権限
SuperAdmin	<p>Super Admin ロールには、すべての ACS 管理機能に対する完全なアクセス権があります。きめ細かなアクセス コントロールが必要ない場合は、このロールが最も便利です。このロールは、事前定義済みの ACSAdmin アカウントに割り当てられています。</p> <p>このロールには、すべてのリソースに対する Create、Read、Update、Delete、および eXecute (CRUDX) 権限があります。</p>

表 16-1 事前定義済みのロールの説明 (続き)

ロール	権限
SystemAdmin	このロールは、ACS システムの設定と操作を行う管理者用です。このロールには、次の権限があります。 <ul style="list-style-type: none"> アカウント定義を除くすべてのシステム管理アクティビティに対する読み取りおよび書き込み権限 ACS インスタンスに対する読み取りおよび書き込み権限
UserAdmin	このロールは、内部ユーザや内部ホストなど、内部 ACS ID ストア内のエントリを追加、更新、または削除する管理者用です。このロールには、次の権限があります。 <ul style="list-style-type: none"> ユーザとホストに対する読み取りおよび書き込み権限 IDG に対する読み取り権限



(注) 最初のログイン時には、特定の管理者に Super Admin だけが割り当てられています。

関連項目

- 管理者アカウントとロールの関連付け (16-7 ページ)
- 管理者アカウントの作成、複製、編集、および削除 (16-8 ページ)

ロールの関連付けの変更

ACS のすべてのロールは、事前に定義される設計になっており、変更できません。ACS では、ロールの関連付けだけを変更できます。ロールの関連付けを変更する特権は、システム全体の認可ステータスに悪影響を及ぼす可能性があるため、ACS の Super Admin ロールと SecurityAdmin ロールにだけ割り当てられています。

ロールの関連付けの変更は、影響を受ける管理者がログアウトし、再度ログインしたあとで初めて有効になります。新たにログインするとき、ACS によってロールの関連付けの変更が読み取られ、適用されます。



(注) ロールの関連付けの変更はグローバルに影響するため、ACS の Super Admin ロールと SecurityAdmin ロールを割り当てる場合は注意が必要です。

管理者アカウントとロールの関連付け

管理者アカウントの定義は、名前、ステータス、説明、電子メールアドレス、パスワード、およびロールの割り当てで構成されています。



(注) ユーザごとに固有の管理者を作成することを推奨します。これにより、操作が監査ログに明確に記録されます。

管理者は、内部データベースおよび外部データベースに対して認証されます。

既存のアカウントを編集および削除できます。ただし、最後のスーパー管理者を削除またはディisableにしようとする、Web インターフェイスにエラー メッセージが表示されます。

ID や証明書は、適切な管理者だけが設定できます。[System Administration] ドロワで設定された ID は [Users and Identity Stores] ドロワで使用できますが、変更はできません。

新しい管理者を作成した場合は、パスワードタイプに ID ストアのタイプを選択できます。新しい管理者はこのパスワードタイプに基づいて認証されます。パスワードタイプにできるのは、内部管理者、AD、LDAP です。すべての既存の管理者のデフォルト値は **AdminsIDStore** です。パスワードタイプには、管理者アカウントと ID ストアとの間に関連付けを作成するために定義された新しい関連付けがあります。内部管理者の認証中に、管理者が内部データベースに存在する場合は、パスワードタイプフィールドの値が読み込まれ属性リストに入力されます。この属性値が **AdminsIDStore** に等しくなければ、認証はパスワードタイプフィールドで設定した値に基づいて LDAP または AD の ID ストアにルーティングされます。AD および LDAP に対して管理者を認証するために ACS は PAP 認証を使用します。

リカバリ管理者アカウント

ACS 5.8 ではシステム管理者がリカバリ アカウントとして少なくとも 1 つの管理者アカウントを保持する必要があります。アカウントがリカバリ アカウントとして設定されていると、ACS はその特定の管理者を認証するために管理者 ID ポリシーおよび認可ポリシーをバイパスします。このリカバリ管理者アカウントは管理者内部 ID ストアに対して認証されます。リカバリアカウントを使用して ACS にアクセスしようとする、内部管理者ユーザに対して認証され、ロールは静的に割り当てられます。複数のリカバリ アカウントを持つことができます。デフォルトでは、**Super Admin** アカウントはリカバアカウントとして設定されます。新しい管理者アカウントを作成すると、ACS によってそのアカウントはリカバリ アカウントとして設定されませんが、アカウント設定でリカバリ アカウントとして設定する必要があります。リカバリ管理者は、ACS のパスワードハッシングを有効にすることはできません。

リカバリ アカウントとして管理者アカウントを設定するには、次の操作を実行する必要があります。

- 管理者アカウントに静的ロールを割り当てます。
- 管理者アカウントに **Super Admin** ロールを割り当てます。
- パスワードタイプを使用して管理者アカウントに外部 ID ストアを設定しないでください。
- パスワードハッシングを有効にしないでください。

関連項目

- [ロールについて \(16-3 ページ\)](#)
- [管理者アカウントの作成、複製、編集、および削除 \(16-8 ページ\)](#)

管理者アカウントの作成、複製、編集、および削除

管理者アカウントを作成、複製、編集、または削除するには、次の手順を実行します。

ステップ 1 [System Administration] > [Administrators] > [Accounts] を選択します。

表 16-2 で説明されている設定済み管理者のリストを含む [Administrators] ページが表示されます。

表 16-2 [Accounts] ページ

オプション	説明
Status	この管理者の現在のステータス。 <ul style="list-style-type: none"> Enabled : この管理者はアクティブです。 Disabled : この管理者はアクティブではありません。 無効の管理者アカウントを使用して ACS にログインすることはできません。
Name	管理者の名前。
Role(s)	管理者に割り当てられているロール。
Description	この管理者の説明。

ステップ 2 次のいずれかを実行します。

- [Create] をクリックします。
- 複製するアカウントのチェックボックスをオンにし、[Duplicate] をクリックします。
- 変更するアカウントをクリックします。または、名前のチェックボックスをオンにして [Edit] をクリックします。
- パスワードを変更するアカウントのチェックボックスをオンにし、[Change Password] をクリックします。詳細については、別の管理者のパスワードのリセット (16-31 ページ) を参照してください。



(注) [Duplicate] ページでは、少なくとも [Admin Name] を変更する必要があります。

- 削除するアカウントのチェックボックスを1つ以上オンにして、[Delete] をクリックします。

ACS では、ACS データベース内に SuperAdmin ロールを持つリカバリ管理者アカウントが選択した管理者アカウント以外に1つ以上ある場合にのみ、選択した管理者アカウントが削除されます。



(注) [Prevent this page from creating additional dialogs] チェックボックスをオンしている場合、Firefox では、ACS Web インターフェイスから最後のリカバリ管理者アカウントを削除しようとしても、警告メッセージは表示されません。

ステップ 3 表 16-3 の説明に従って、[Administrator Accounts Properties] ページのフィールドに入力します。

表 16-3 [Administrator Accounts Properties] ページ

オプション	説明
General	
Administrator Name	この管理者に設定されている名前。規則を複製する場合は、必ず固有の名前を入力してください。
Status	[Status] ドロップダウンメニューから、アカウントをイネーブルにするかディセーブルにするかを選択します。このオプションは、[Account never disabled] チェックボックスをオンにした場合はディセーブルになっています。

表 16-3 [Administrator Accounts Properties] ページ (続き)

オプション	説明
Description	この管理者の説明。
Email Address	管理者の電子メールアドレス。ACS View によって、この電子メールアドレスに警告が送信されます。ACS はこの E メールアドレスを使用して、内部管理者のパスワードの期限が切れる n 日前に、パスワードの期限が切れることについて社内管理者へ通知します。
Recovery Account	あるアカウントをリカバリ アカウントとして設定するためには、このオプションにチェックを入れます。このオプションを使用する時、管理者を認証するために、ACS は管理者 ID ポリシーおよび認証ポリシーを経由します。詳細については、 リカバリ管理者アカウント (16-8 ページ) を参照してください。 (注) ACS は、リカバリ管理者アカウントのパスワードハッシングを有効にさせません。リカバリ アカウントとして管理者アカウントを設定すると、ACS は次のメッセージを表示します。 Please note that for a valid recovery account, you must enable the account, disable password hash, set assignment type to static, assign the SuperAdmin role, and set password type to the Internal Administrators Store.
Account never disabled	アカウントを無効にしない場合にオンにします。アカウントは、次の場合も無効にはなりません。 <ul style="list-style-type: none"> パスワードが失効した場合 アカウントが非アクティブになった場合 指定されたログイン試行回数を超えた場合
Enable Password Hash	このチェックボックスをオンにして、Cisco SSL ハッシュ アルゴリズムの PBKDF2 を使用したパスワードハッシングを有効にし、管理者パスワードのセキュリティを強化します。デフォルトでは、このオプションは無効になっています。このオプションは、内部管理者にのみ適用されます。途中でこのオプションを無効にした場合、無効にした直後に [Change Password] オプションを使用してパスワードを再設定する必要があります。詳細については、 内部管理者のパスワードハッシングの有効化および無効化 (16-12 ページ) を参照してください。 (注) このオプションが正常に動作するためには、ACS ランタイムプロセスが起動し正しく動作している必要があります
Authentication Information	
Password Type	デフォルトのパスワードタイプであり、設定済みの外部 ID ストア名および社内管理者を表示します (AD、LDAP のみ)。リストから任意の ID ストアを選択することができます。 管理者の認証中に、外部 ID ストアが管理者へ設定されている場合、社内 ID ストアは設定済みの外部 ID ストアに対して認証要求を転送します。 外部 ID ストアが選択されている場合、管理者のパスワードは設定できません。パスワード編集ボックスは無効です。 パスワードタイプにおいて外部 ID ストアとして ID シーケンスを使用することはできません。 [System Administration] > [Administrators] > [Accounts] ページにある [Change Password] ボタンを使用してパスワードタイプを変更することができます。
Password	認証パスワード。
Confirm Password	認証パスワードの確認。

表 16-3 [Administrator Accounts Properties] ページ (続き)

オプション	説明
Change password on next login	次のログイン時にユーザに新しいパスワードの入力を求めるにはチェックを入れます。 (注) 管理者アカウントで次回ログイン時のパスワード変更のオプションが有効になっている場合、管理者は分散導入に ACS インスタンスを追加することはできません。
ロール割り当て	
Available Roles	設定されているすべてのロールのリスト。この管理者に割り当てるロールを選択し、[>] をクリックします。この管理者にすべてのロールを割り当てるには、[>>] をクリックします。
Assigned Roles	この管理者に適用されるロール。

ステップ 4 [Submit] をクリックします。

新しいアカウントが保存されます。作成または複製した新しいアカウントを含む [Administrators] ページが表示されます。



(注) Active Directory で [User must change password at next logon] オプションが有効な場合、AD として設定されたパスワードタイプを持つ管理者アカウントに対する ACS は認証に失敗します。



(注) 静的ロールが割り当てられた SuperAdmin は他の管理者に対して SuperAdmin ロールの作成、割当て、削除が可能です。動的ロールが割り当てられた SuperAdmin は他の管理者に対して SuperAdmin ロールの作成、割当て、削除をすることができません。

関連項目

- [ロールについて \(16-3 ページ\)](#)
- [管理者アカウントとロールの関連付け \(16-7 ページ\)](#)
- [事前定義済みのロールの表示 \(16-14 ページ\)](#)
- [管理者の認証設定 \(16-15 ページ\)](#)
- [管理者アカウントのエクスポート \(16-11 ページ\)](#)

管理者アカウントのエクスポート

ACS 5.8 では、[Administrator Accounts] ページで使用可能なエクスポート オプションを使用して、.csv ファイルに admin アカウントをエクスポートできます。このオプションを選択すると、管理者アカウントのページで作成され、リストされているすべての管理者アカウントが .csv ファイルにエクスポートされます。このファイルをローカル ドライブに保存しておくと監査に使用できます。また、暗号化パスワード オプションを使用してエクスポートされたファイルを暗号化できます。エクスポートされたファイルを復号化するにはこのパスワードが必要です。ただし、ACS に再度エクスポートされた管理者アカウントの詳細はインポートできません。動的な管理者アカウントについては、エクスポートされたファイルのカラム ロールは空です。管理者に複数のロールを割り当てている場合は、ロールとロールの間にセミコロンが使用されています。また、ACS CLI から管理者アカウントをエクスポートできますが、Rest PI を使用して管理者アカウントをエクスポートすることはできません。



(注)

管理者アカウントをエクスポートするためには、SuperAdmin ロール、SystemAdmin ロール、または UserAdmin ロールを持つ管理者アカウントが必要です。

管理者アカウントを ACS Web インターフェイスからエクスポートするには、次の手順を実行します。

- ステップ 1** [System Administration] > [Administrators] > [Accounts] を選択します。
表 16-2 で説明されている設定済み管理者のリストを含む [Administrators] ページが表示されます。
- ステップ 2** [Export] をクリックします。
[Export properties] ダイアログボックスが表示されます。
- ステップ 3** [Password] フィールドのチェックボックスをオンにし、エクスポートされたファイルを暗号化
する場合は暗号化パスワードを入力します。
- ステップ 4** [Start Export] をクリックします。
[Export Progress] ダイアログボックスが開き、エクスポート操作の進行状況が表示されます。
このダイアログボックスには、ユーザがエクスポート操作中にエラーを特定できるよう、エクスポートのログが表示されます。



(注)

ACS CLI から管理者アカウントをエクスポートするには、**export-data administrator** `<repository>` `<export_filename>` `<result_filename>` `<encryption_type>` コマンドを ACS コンフィギュレーションモードで実行します。

関連項目

- [ロールについて \(16-3 ページ\)](#)
- [管理者アカウントとロールの関連付け \(16-7 ページ\)](#)
- [事前定義済みのロールの表示 \(16-14 ページ\)](#)
- [管理者の認証設定 \(16-15 ページ\)](#)

内部管理者のパスワードハッシングの有効化および無効化

内部管理者パスワードのセキュリティを向上させるためにパスワードハッシングを有効にすることが可能です。ACS Web インターフェイスの [ACS Administrator Account] ページから、[Enable Password Hash] オプションを有効にできます。

内部管理者パスワードのセキュリティを強化するために、ACS 5.8 は新機能「パスワードハッシングの有効化」を導入しています。このオプションを有効にする場合、管理者パスワードは Cisco SSL ハッシュアルゴリズムの PBKDF2 を使用してハッシュに変換され、内部データベースに保存されます。この機能はパスワードベースの認証に対してのみ適用できます。このオプションが正常に動作するためには、ACS ランタイムプロセスが起動し正しく動作している必要があります。

内部管理者アカウントの作成時、[Enable Password Hashing] オプションが有効になっている場合、ACS はパスワードをハッシュに変換し内部データベースに保存します。管理者がログインパスワードを使用して ACS にアクセスしようとした時、ACS は PBKDF2 ハッシュアルゴリズム

ムを使用してパスワードをハッシュに変換し、そのハッシュ エントリーと内部データベースに保存されているエントリーを比較します。ACS は、パスワードのハッシュ値とデータベースのハッシュ値が一致した時のみ、管理者にログインさせます。ACS は、分散導入でのパスワードハッシュの有効化をサポートしています。リカバリ管理者の場合、パスワードハッシングを有効にすることはできません。

分散導入では、パスワード ハッシング オプションが有効である管理者アカウントを使用して ACS インスタンスを二次インスタンスとして追加するには、ACS インスタンス間の信頼された通信を有効にする必要があります。信頼された通信の詳細については、[分散展開での信頼通信 \(17-33 ページ\)](#) を参照してください。

内部管理者のパスワード ハッシングを有効にするには、次のようにします。

-
- ステップ 1** [System Administration] > [Administrators] > [Accounts] を選択します。
[Internal Administrators] ページが表示され、利用可能な内部管理者のリストが表示されます。
- ステップ 2** 次のいずれかの操作を行います。
- [Create] をクリックします。
 - パスワードハッシングを有効にしたい管理者アカウントの隣にあるチェックボックスにチェックを入れて [Edit] をクリックします。
- ステップ 3** [Enable Password Hash] チェックボックスをオンにします。
- ステップ 4** [Submit] をクリックします。
選択された内部管理者のパスワード ハッシング オプションが有効になります。
-



(注) リカバリ管理者アカウントのパスワード ハッシングを有効にし [Submit] をクリックすると、ACS は次のエラーを表示します。「For a recovery account password hash must be disabled.」

内部管理者のパスワード ハッシングを無効にするには、次のようにします。

-
- ステップ 1** [System Administration] > [Administrators] > [Accounts] を選択します。
[Internal Administrators] ページが表示され、利用可能な内部管理者のリストが表示されます。
- ステップ 2** パスワードハッシングを無効にする管理者アカウントの隣にあるチェックボックスをオンにし、[Edit] をクリックします。
- ステップ 3** [Enable Dynamic Authorization] チェックボックスをオフにします。
- ステップ 4** [Submit] をクリックします。
選択した内部管理者のパスワード ハッシング オプションは無効になります。
-



(注) [Enable Password Hash] オプションを無効にすると、ユーザ パスワードを直ちに変更する必要があります。

- ステップ 5** パスワード ハッシング オプションを無効にする管理者アカウントの隣にあるチェックボックスをオンにし、[Change Password] をクリックします。
- ステップ 6** [Password] フィールドに新しいパスワードを入力します。

ステップ 7 [Confirm Password] フィールドにパスワードを再度入力します。

ステップ 8 [Submit] をクリックします。

関連項目

- [ロールについて \(16-3 ページ\)](#)
- [管理者アカウントとロールの関連付け \(16-7 ページ\)](#)
- [事前定義済みのロールの表示 \(16-14 ページ\)](#)
- [管理者の認証設定 \(16-15 ページ\)](#)

事前定義済みのロールの表示

ACS の事前定義済みのロールについては、[表 16-1](#)を参照してください。

事前定義済みのロールを表示するには、次の手順を実行します。

[System Administration] > [Administrators] > [Roles] を選択します。

事前定義済みのロールのリストを含む [Roles] ページが表示されます。[表 16-4](#) に、[Roles] ページのフィールドを示します。

表 16-4 [Roles] ページ

フィールド	説明
Name	設定されているすべてのロールのリスト。事前定義済みのロールのリストについては、 事前定義済みのロール (16-5 ページ) を参照してください。
Description	各ロールの説明。

ロールプロパティの表示

このページは、各ロールのプロパティを表示する場合に使用します。

[System Administration] > [Administrators] > [Roles] を選択し、ロールをクリックするか、またはロールのオプション ボタンを選択して [View] をクリックします。

[表 16-5](#)で説明されている [Roles Properties] ページが表示されます。

表 16-5 [Roles Properties] ページ

フィールド	説明
Name	ロールの名前。ロールを複製する場合は、最小設定として固有の名前を入力する必要があります。その他のフィールドはすべて任意です。ロールは作成または編集できません。事前定義済みのロールのリストについては、 表 16-4 を参照してください。
Description	ロールの説明。詳細については、 事前定義済みのロール (16-5 ページ) を参照してください。
Permissions List	

表 16-5 [Roles Properties] ページ (続き)

フィールド	説明
Resource	使用可能なリソースのリスト。
Privileges	各リソースに割り当てることができる特権。特権が適用されない場合、特権のチェックボックスは選択できません (使用できません)。 行の色は、特定の特権が使用可能かどうかとは関係ありません。[Privileges] カラムの明示的なテキストによって決まります。

関連項目

- [ロールについて \(16-3 ページ\)](#)
- [管理者アカウントとロールの関連付け \(16-7 ページ\)](#)
- [管理者の認証設定 \(16-15 ページ\)](#)

管理者の認証設定

認証設定は、管理者に強力なパスワードの使用や定期的なパスワードの変更などを強制することによって、セキュリティを強化する規則のセットです。パスワードポリシーの変更は、すべての ACS システム管理者アカウントに適用されます。

パスワードポリシーを設定するには、次の手順を実行します。

- ステップ 1** [System Administration] > [Administrators] > [Settings] > [Authentication] を選択します。
[Password Complexity] タブと [Advanced] タブを含む [Password Policies] ページが表示されます。
- ステップ 2** [Password Complexity] タブで、管理者パスワードの設定に使用する各チェックボックスをオンにします。

表 16-6 に、[Password Complexity] タブのフィールドを示します。

表 16-6 [Password Complexity] タブ

オプション	説明
Applies to all ACS system administrator accounts	
Minimum length	必要な最小長。有効なオプションは 4 ~ 127 です。
Password may not contain the username or its characters in reversed order	パスワードにユーザ名または逆順のユーザ名を含めることができないことを指定する場合にオンにします。たとえば、ユーザ名が john の場合、パスワードを john または nhoj にすることはできません。
Password may not contain 'cisco' or its characters in reversed order	パスワードに cisco という単語またはその逆順の文字列 (つまり ocsic) を含めることができないことを指定する場合にオンにします。
Password may not contain "" or its characters in reversed order	パスワードに、入力した文字列またはその逆順の文字列を含めることができないことを指定する場合にオンにします。たとえば、文字列 polly を指定した場合、パスワードを polly または yllop にすることはできません。
Password may not contain repeated characters four or more times consecutively	パスワードで文字を 4 回以上連続して繰り返すことができないことを指定する場合にオンにします。たとえば、パスワードとして apppple を使用できません。これは、文字 p が 4 回連続して使用されているためです。

表 16-6 [Password Complexity] タブ (続き)

オプション	説明
Password must contain at least one character of each of the selected types	
Lowercase alphabetic characters	パスワードには、アルファベットの小文字が少なくとも 1 文字含まれている必要があります。
Upper case alphabetic characters	パスワードには、アルファベットの大文字が少なくとも 1 文字含まれている必要があります。
Numeric characters	パスワードには、数字が少なくとも 1 文字含まれている必要があります。
Non alphanumeric characters	パスワードには、英数字以外の文字が少なくとも 1 文字含まれている必要があります。

ステップ 3 [Advanced] タブで、管理者の認証プロセスに設定する基準の値を入力します。

表 16-7 に、[Advanced] タブのフィールドを示します。

表 16-7 [Advanced] タブ

オプション	説明
Password History	
Password must be different from the previous n versions	比較対象となる、この管理者の旧パスワードの数を指定します。このオプションを指定すると、管理者は最近使用したパスワードを設定できなくなります。有効なオプションは 1 ~ 99 です。
Password Lifetime : 管理者は定期的にパスワードを変更する必要があります	
Require a password change after n days	パスワードを n 日後に変更する必要があることを指定します。有効なオプションは 1 ~ 365 です。このオプションを設定すると、 n 日後にパスワードを変更する必要があります。
Disable administrator account after n days if password is not changed	パスワードが変更されていない場合に、管理者アカウントを n 日後にディセーブルにする必要があることを指定します。有効なオプションは 1 ~ 365 です。 ACS では、[Display reminder after n days] オプションを設定しないでこのオプションを設定することはできません。
Send Email for password expiry before n days	パスワードを変更しない場合 n 日後にパスワードが期限切れになることを、内部管理者に電子メールで通知することを指定します。有効なオプションは 1 ~ 365 です。デフォルト値は 5 日間です。このオプションを設定すると、パスワードの有効期限が切れる n 日前に内部管理者アカウントに電子メールでの通知が送信されます。 ACS では、パスワードを変更しないで n 日が経過すると管理者アカウントを無効にするオプションを設定しないと、このオプションを設定できません。
Display reminder after n days	パスワード変更の通知を n 日後に表示します。有効なオプションは 1 ~ 365 です。このオプションを設定すると、通知だけが表示されます。新しいパスワードは要求されません。

表 16-7 [Advanced] タブ

オプション	説明
Account Inactivity : ユーザアカウントが無効になっていることを確認します。	
Require a password change after <i>n</i> days of inactivity	アカウントが非アクティブになってから <i>n</i> 日後にパスワードを変更する必要があることを指定します。有効なオプションは 1 ~ 365 です。このオプションを設定すると、 <i>n</i> 日後にパスワードを変更する必要があります。 ACS では、[Display reminder after <i>n</i> days] オプションを設定しないでこのオプションを設定することはできません。
Disable administrator account after <i>n</i> days of inactivity	管理者アカウントが非アクティブになってから <i>n</i> 日後にそのアカウントをディセーブルにする必要があることを指定します。有効なオプションは 1 ~ 365 です。 ACS では、[Display reminder after <i>n</i> days] オプションを設定しないでこのオプションを設定することはできません。
Incorrect Password Attempts	
Disable account after <i>n</i> successive failed attempts	最大ログイン試行回数を指定します。この回数を超えると、アカウントはディセーブルになります。有効なオプションは 1 ~ 10 です。



(注)

ACS は、最後のログイン、最後のパスワード変更、またはログイン試行回数に基づいてアカウントを自動的に無効またはディセーブルにします。CLI および PI ユーザアカウントはブロックされ、ACS Web インターフェイスからパスワードを変更できるという内容の通知を受信します。アカウントがディセーブルになっている場合は、アカウントをイネーブルにするよう、別の管理者に依頼します。

ステップ 4 [Submit] をクリックします。

管理者パスワードに定義された基準が設定されます。これらの基準は、以降のログインだけに適用されます。

関連項目

- [ロールについて \(16-3 ページ\)](#)
- [管理者アカウントとロールの関連付け \(16-7 ページ\)](#)
- [事前定義済みのロールの表示 \(16-14 ページ\)](#)

セッションアイドルタイムアウトの設定

デフォルトでは、GUI セッションには 30 分のタイムアウト時間が割り当てられます。タイムアウト時間は、5 ~ 90 分の範囲で指定できます。セッションタイムアウト オプションは [Active Directory] ページおよび [Distributed System Management] ページには適用されません。AD ページが自動的に更新され、アプリケーションで定義した更新間隔に基づいて AD の接続ステータスが確認されます。[Distributed System Management] ページは、設定した間隔で自動的に更新されます。ACS Web インターフェイスの [Distributed System Management] ページから更新間隔を設定できます。

タイムアウト時間を設定するには、次の手順を実行します。

-
- ステップ 1 [System Administration] > [Administrators] > [Settings] > [Session] を選択します。
 - ステップ 2 [GUI Session] ページが表示されます。
 - ステップ 3 [Session Idle Timeout] の値を分単位で入力します。有効な値は 5 ～ 90 分です。
 - ステップ 4 [Submit] をクリックします。
-



(注) CLI クライアントインターフェイスには、6 時間のデフォルトのセッションタイムアウト値が設定されています。CLI クライアントインターフェイスではセッションタイムアウト時間を設定できません。

管理者のアクセス設定

ACS 5.8 では、リモートクライアントの IP アドレスに基づいて ACS への管理アクセスを制限できます。次のいずれかの方法で IP アドレスをフィルタリングできます。

- [すべての IP アドレスに接続を許可する \(16-18 ページ\)](#)
- [IP アドレスの選択リストからのリモート管理を許可する \(16-18 ページ\)](#)
- [IP アドレスの選択リストからのリモート管理を拒否する \(16-19 ページ\)](#)

すべての IP アドレスに接続を許可する

[Allow all IP addresses to connect] オプションを選択すると、すべての接続を許可できます。これがデフォルトのオプションです。

IP アドレスの選択リストからのリモート管理を許可する

管理者に ACS へのリモートアクセスを許可するには、次の手順を実行します。

-
- ステップ 1 [System Administration] > [Administrators] > [Settings] > [Access] を選択します。
[IP Addresses Filtering] ページが表示されます。
 - ステップ 2 [Allow only listed IP addresses to connect] オプション ボタンをクリックします。
[IP Range(s)] 領域が表示されます。
 - ステップ 3 [IP Range(s)] 領域で [Create] をクリックします。
新しいウィンドウが表示されます。ACS へのリモートアクセスを許可するマシンの IPv4 または IPv6 アドレスを入力します。IP アドレス範囲全体のサブネットマスクを入力します。ACS は、入力されたアドレスが IPv4 または IPv6 でサポートされる形式であるかどうかを確認します。
 - ステップ 4 [OK] をクリックします。
[IP Range(s)] 領域に IP アドレスが読み込まれます。ステップ 3 を繰り返して、リモートアクセスを許可する他の IP アドレスまたは範囲を追加します。
 - ステップ 5 [Submit] をクリックします。
-

IP アドレスの選択リストからのリモート管理を拒否する

管理者による ACS へのリモート アクセスを拒否するには、次の手順を実行します。

-
- ステップ 1 [System Administration] > [Administrators] > [Settings] > [Access] を選択します。
[IP Addresses Filtering] ページが表示されます。
- ステップ 2 [Reject connections from listed IP addresses] オプション ボタンをクリックします。
[IP Range(s)] 領域が表示されます。
- ステップ 3 [IP Range(s)] 領域で [Create] をクリックします。
新しいウィンドウが表示されます。
- ステップ 4 ACS へのリモート アクセスを許可しないマシンの IP アドレスを入力します。IP アドレス範囲全体のサブネット マスクを入力します。
- ステップ 5 [OK] をクリックします。
[IP Range(s)] 領域に IP アドレスが読み込まれます。ステップ 3 を繰り返して、拒否する他の IP アドレスまたは範囲を追加します。
- ステップ 6 [Submit] をクリックします。
-



(注)

すべての IP アドレスからの接続を拒否できます。この設定は、ACS Web インターフェイスではリセットできません。ただし、次の CLI コマンドを使用できます。

```
access-setting accept-all
```

このコマンドの詳細については、『[CLI Reference Guide for Cisco Secure Access Control System 5.8](#)』を参照してください。

管理アクセスコントロールの使用

ACS 5.8 では、管理アクセス コントロール (AAC) サービスという新しいサービス タイプが導入されています。AAC サービスは、ACS 管理者の認証と認可を扱います。

拡張 AAC Web インターフェイスは次のとおりです。

- ポリシーベースの認証および認可
- 外部データベースに対する認証は次で実行可能です。
 - 内部 ID ストア管理者の管理者アカウントのパスワードタイプ。
 - 外部データベースと照合する ID ポリシー (認証ポリシー) の設定。

この AAC サービスは、インストール時に自動的に作成されます。新しい AAC サービスの削除または追加はできません。AAC はサービス セレクション ポリシーでは使用できず、管理者ログイン時に自動的に選択されます。

AAC サービスでは、管理者ログインのための一連のポリシーを識別します。AAC サービス内で提供されるポリシーは次のとおりです。

- 管理者 ID ポリシーは管理者の認証に使用される ID データベースを決定し、以降の認可ポリシーで使用される可能性のある管理者の属性の取得も行います。

- 管理者認可ポリシーは、ACS のセッションの管理者のロールを決定します。割り当てられたロールによって、管理者の権限が決定されます。各ロールに権限の事前定義リストがあります。それはロール ページで見ることができます。

AAC サービスがこれら 2 つのポリシーを順番に処理します。管理者 ID ポリシーおよび管理者認可ポリシーの両方を設定する必要があります。両方のポリシーのデフォルトは次のとおりです。

ID ポリシー：デフォルトは、[Internal Identity Store] です。

認可ポリシー：デフォルトは [Deny Access] です。

AAC サービスは PAP 認証タイプだけをサポートします。Super Admin のみが管理者アクセスコントロールを設定することを許可されます。

ACS アプリケーションを ACS 5.8 にアップグレードする場合は、AAC は次の変更を実施します。

- 単一 AAC サービスは、アップグレード時に自動的に作成されます。
- AAC サービスの ID ポリシーは、[Administrators Internal Identity Store] に設定されます。
- すべての既存の管理者は静的ロール割り当てで検証されます。
- Super Admin ロールを持つすべての管理者はリカバリ アカウントとして自動的に設定されます。

5.8 に ACS アプリケーションをアップグレードした後で、管理者アカウントを更新しないと、アップグレードされた管理者アカウントは管理者内部 ID ストアに対して認証され、静的割り当てによりロールを取得します。アップグレード時にバックアップを復元すると、ACS 5.8 はスキーマ ファイルとデータのアップグレードを処理します。



(注)

外部 ID ストアで作成された管理者アカウントは、ACS CLI の CARS モードにアクセスできません。しかし、ACS CLI の ACS コンフィギュレーション モードにはアクセスできます。

ここでは、次の内容について説明します。

- [管理者 ID ポリシー \(16-20 ページ\)](#)
- [管理者認可ポリシー \(16-27 ページ\)](#)

管理者 ID ポリシー

管理アクセスコントロールの ID ポリシーでは、ACS で認証と属性の取得に使用する ID ソースを定義します。グループおよび属性は、外部データベースからのみ取得できます。ACS は、取得した属性をその後の認可ポリシーでのみ使用できます。

AAC サービスは次の 2 種類の ID ポリシーをサポートします。その内容は次のとおりです。

- 単一結果選択
- ルール ベース結果選択

Super Admin は、このポリシーを設定および変更できます。すべての要求の認証に同じ ID ソースを適用する単純なポリシー、またはルール ベースの ID ポリシーを設定できます。

単純なポリシーでサポートされる識別方法は次のとおりです。

- アクセス拒否：ユーザへのアクセスは拒否され、認証は実行されません。
- ID ストア：単一の ID ストア。

次の ID ストアのいずれかを選択できます。

- 内部管理者 ID ストア
- Active Directory ID ストア

- LDAP ID ストア
- RSA SecurID ストア
- RADIUS ID ストア

[Deny Access] が結果として選択されている場合、管理者のアクセスは拒否されます。

ルールベースのポリシーでは、各規則に 1 つ以上の条件、および認証に使用される ID ソースである結果が含まれます。

サポートされる条件は次のとおりです。

- システム ユーザ名
- システムの日付と時刻
- 管理者クライアント IP アドレス

AAC サービスの ID ポリシーは結果として ID ストア順序をサポートしません。ID ポリシー内の規則は、作成、複製、編集、および削除できます。また、イネーブルおよびディセーブルにすることもできます。



注意

単純なポリシー ページとルールベースのポリシー ページを切り替えると、以前に保存したポリシー設定は失われます。

単純な ID ポリシーを設定するには、次の手順を実行します。

ステップ 1 [System Administration] > [Administrative Access Control] > [Identity] を選択します。

デフォルトでは、表 16-8 で説明されているフィールドを含む [Simple Identity Policy] ページが表示されます。

表 16-8 [Simple Identity Policy] ページ

オプション	説明
Policy type	設定するポリシーのタイプを定義します。 <ul style="list-style-type: none"> • [Simple] : 結果がすべての要求に適用されることを指定します。 • [Rule-based] : 要求に応じて異なる結果が適用されるように規則を設定します。 ポリシー タイプを切り替えると、以前に保存したポリシー設定は失われます。
Identity Source	すべての要求に適用する ID ソース。デフォルトは [Deny Access] です。パスワードベースの認証の場合、単一の ID ストアまたは ID ストア順序を選択します。

ステップ 2 認証用の ID ソースを選択するか、または [Deny Access] を選択します。



ステップ 3 [Save Changes] を選択して、ポリシーを保存します。

規則ベースの ID ポリシーの表示

[System Administration] > [Administrative Access Control] > [Identity] を選択します。

デフォルトでは、表 16-8 で説明されているフィールドを含む [Simple Identity Policy] ページが表示されます。設定されている場合は、表 16-9 で説明されているフィールドを含む [Rule-Based Identity Policy] ページが表示されます。

表 16-9 [Rule-Based Identity Policy] ページ

オプション	説明
Policy type	<p>設定するポリシーのタイプを定義します。</p> <ul style="list-style-type: none"> [Simple] : 結果がすべての要求に適用されることを指定します。 [Rule-based] : 要求に応じて異なる結果が適用されるように規則を設定します。 <p> 注意 ポリシータイプを切り替えると、以前に保存したポリシー設定は失われます。</p>
Status	<p>規則の現在のステータス。規則のステータスは、次のとおりです。</p> <ul style="list-style-type: none"> Enabled : 規則はアクティブです。 Disabled : ACS によって規則の結果は適用されません。 Monitor : 規則はアクティブですが、ACS によって規則の結果は適用されません。ヒットカウントなどの結果はログに書き込まれます。ログエントリには、規則がモニタだけであることを示す情報が含まれます。モニタ オプションは、新規の規則の結果を確認する場合に特に役立ちます。
Name	ルール名。
Conditions	ポリシーの範囲を決定する条件。このカラムでは、現在のすべての条件がサブカラムに表示されます。
Results	規則の評価結果として認証に使用される ID ソース。
Hit Count	規則が一致した回数。このカラムを更新およびリセットするには、[Hit Count] ボタンをクリックします。
Default Rule	<p>次の場合に、ACS によってデフォルト規則が適用されます。</p> <ul style="list-style-type: none"> イネーブルな規則が一致しない。 他の規則が定義されていない。 <p>デフォルト規則を編集するには、リンクをクリックします。デフォルト規則の結果だけを編集できます。デフォルト規則は削除、ディセーブル、または複製できません。</p>
[Customize] ボタン	<p>ポリシー規則で使用する条件のタイプを選択する [Customize] ページを開きます。追加する条件ごとに、[Policy] ページに新しい [Conditions] カラムが表示されます。</p> <p> 注意 規則を定義したあとで条件タイプを削除した場合、その条件タイプについて設定した条件は失われます。</p>
[Hit Count] ボタン	[Policy] ページの [Hit Count] 表示をリセットおよび更新できるウィンドウが開きます。 Hit カウントの表示 (10-10 ページ) を参照してください。

ルールベースのポリシーを設定するには、次の項を参照してください。

- [ポリシー規則の作成 \(10-38 ページ\)](#)
- [規則の複製 \(10-40 ページ\)](#)
- [ポリシー規則の編集 \(10-40 ページ\)](#)
- [ポリシー規則の削除 \(10-41 ページ\)](#)

ID ポリシー規則のプロパティ設定

ID ポリシー規則を作成、複製、または編集して、管理者の認証に使用する ID データベースを決定したり、管理者の属性を取得したりできます。属性の検索は、外部データベースを使用する場合だけ可能です。

このページを表示するには、次の手順を実行します。

ステップ 1 [System Administration] > [Administrative Access Control] > [Identity] を選択し、次のいずれかをおこないます。

- **[Create]** をクリックします。
- 規則チェックボックスをオンにし、**[Duplicate]** をクリックします。
- 規則名をクリックするか規則チェックボックスをオンにし、**[Edit]** をクリックします。
- [表 16-10](#) 説明に従って、**[Identity Rule Properties]** ページのフィールドに入力します。

表 16-10 **[Identity Rule Properties]** ページ

オプション	説明
General	
Rule Name	ルールの名前。規則を複製する場合は、最小設定として固有の名前を入力する必要があります。その他のフィールドはすべて任意です。
Rule Status	規則のステータスは、次のとおりです。 <ul style="list-style-type: none"> • Enabled : 規則はアクティブです。 • Disabled : ACS によって規則の結果は適用されません。 • Monitor : 規則はアクティブですが、ACS によって規則の結果は適用されません。ヒットカウントなどの結果はログに書き込まれます。ログ エントリには、規則がモニタだけであることを示す情報が含まれます。モニタ オプションは、新規の規則の結果を確認する場合に特に役立ちます。
Conditions	
conditions	規則に対して設定できる条件。デフォルトでは、複合条件が表示されます。 [Policy] ページで [Customize] ボタンを使用して、表示される条件を変更できます。 各条件のデフォルト値は、 [ANY] です。条件の値を変更するには、条件チェックボックスをオンにし、値を指定します。 [Compound Condition] をオンにすると、条件フレームに式ビルダーが表示されます。詳細については、 複合条件の設定 (10-41 ページ) を参照してください。
Results	
Identity Source	要求に適用する ID ソース。デフォルトは管理者内部 ID ストアです。パスワードベースの認証の場合、単一の ID ストアまたは ID ストア順序を選択します。

RADIUS ID および RSA SecurID サーバに対する管理者の認証

ACS 5.8 は、RADIUS ID および RSA SecurID サーバに対する管理者の認証をサポートします。この機能は ACS CLI の ACS Web インターフェイスおよび ACS 設定モードの両方で使用できます。この機能は、RADIUS ID または RSA SecurID サーバが生成するワンタイムパスワード (OTP) を使用して、管理者の認証のセキュリティを向上させます。ACS には、外部 ID ソースに対して管理者を認証するための次の 2 つのユースケースがあります。

- 管理者アカウントが ACS にあります。パスワードタイプが外部 ID ソースとして設定されます。パスワードタイプは、[System Administration] > [Administrators] > [Accounts] で外部 ID ソースとして設定します。したがって、管理者アカウントのパスワード認証は、指定された外部 ID ソースから取得する必要があります。
- 管理者アカウントは外部 ID ソースです。そのため、ACS は外部 ID ソースを使用して管理者アカウントとパスワードの両方を確認し、外部 ID ソースに対して管理者を認証します。

ここでは、次の内容について説明します。

- [RADIUS ID サーバに対する管理者の認証 \(16-24 ページ\)](#)
- [RSA SecurID サーバに対する管理者の認証 \(16-25 ページ\)](#)

RADIUS ID サーバに対する管理者の認証

管理者を RADIUS ID サーバに対して認証するには、次のようにします。

-
- ステップ 1** ACS に RADIUS ID サーバを追加します。詳細については、「[RADIUS ID サーバの作成、複製、および編集 \(8-91 ページ\)](#)」を参照してください。
 - ステップ 2** RADIUS ID サーバに ACS と管理者アカウントを追加します。これらの操作の実行方法については、RADIUS ID サーバのドキュメントを参照してください。
 - ステップ 3** ACS Web インターフェイスで、[System Administration] > [Administrative Access Control] > [Identity] を選択します。
 - ステップ 4** [Single result selection] オプション ボタンをクリックします。
 - ステップ 5** [RADIUS Identity] サーバを [Identity Source] として選択し、[Save Changes] をクリックします。
 - ステップ 6** ACS Web インターフェイスからログアウトします。
 - ステップ 7** ACS Web インターフェイスを起動し、RADIUS ID サーバに対して管理者アカウントの認証を初めて行わせます。
 - ステップ 8** [Username] フィールドにユーザ名を入力し、[Password] フィールドに RADIUS ID サーバに設定されたパスワードを入力して、[Login] をクリックします。

RADIUS ID サーバの設定に基づき、ACS は管理者に認証前にさまざまなメッセージを表示することがあります。

ACS は管理者が RADIUS ID サーバに設定されたパスワードを使用して Web インターフェイスにログインできるようにします。



(注) ACS CLI から RADIUS ID サーバに対して ACS 管理者を認証するには、前述の ACS CLI の **acs-config** モードと同じ手順を使用します。

関連項目

- [RSA SecurID サーバに対する管理者の認証 \(16-25 ページ\)](#)

RSA SecurID サーバに対する管理者の認証

外部 ID ソースとしての RSA SecurID サーバに対して管理者を認証するには、次のようにします。

ACS 管理者認証用に外部 ID ソースとして RSA SecurID サーバを設定する

- ステップ 1 ACS に RSA SecurID サーバを追加します。詳細については、[RSA SecurID エージェントの設定 \(8-82 ページ\)](#) を参照してください。
- ステップ 2 RSA SecurID サーバに ACS と管理者アカウントを追加します。詳細については、『[RSA Authentication Manager Administrator's Guide](#)』を参照してください。
- ステップ 3 ACS Web インターフェイスで、[System Administration] > [Administrative Access Control] > [Identity] を選択します。
- ステップ 4 [Single result selection] オプション ボタンをクリックします。
- ステップ 5 [RSA SecurID] サーバを [Identity Source] として選択し、[Save Changes] をクリックします。これで、管理者認証用に外部 ID ソースとして RSA SecurID サーバを設定しました。

RSA SecurID サーバを使用して ACS 管理者を初めて認証する

- ステップ 1 ACS Web インターフェイスを起動します。
- ステップ 2 ユーザ名を [Username] フィールドに入力します。
- ステップ 3 トークン コードを RSA SecurID デバイスを使用して生成し、そのトークン コードを ACS の Web インターフェイスの [Password] フィールドに入力し、[Login] をクリックします。

RSA SecurID サーバ設定に基づいて、ACS はシステムで生成された PIN を使用して次のメッセージが表示されることがあります。

```
PIN: <XXXXXXXX> Please remember your new PIN then press Return to continue.
```



(注) 上記のメッセージに表示される PIN をコピーし、システムに保存します。この PIN を使用して、ACS Web インターフェイスにログインするための後続のトークン コードを生成する必要があります。

- ステップ 4 [Login] をクリックします。
ACS は、管理者が Web インターフェイスにログインできるようにします。RSA SecurID サーバに対する最初の管理者認証が成功します。

RSA SecurID サーバを使用して管理者アカウントを最初に認証する際、次のようになります。

- ACS がチャレンジメッセージを表示したときに [Cancel] をクリックした場合、認証手順を最初から行う必要があります。
- ACS がシステムで生成される PIN を表示した後 [Cancel] をクリックした場合、最初の認証はキャンセルされ、システムにより生成された PIN をその後の認証の実行に使用できます。

後続の管理者認証に RSA SecurID サーバを使用する際、誤ったパスコードを入力した場合、ACS は正しいパスワードの入力を求めます。正しいパスワードを入力し [Login] をクリックした場合、ACS はセキュリティを確保するために次のトークンコードの入力を求めます。

RSA SecurID サーバを使用した後続の ACS 管理者認証の実行。

-
- ステップ 1 ACS Web インターフェイスを起動します。
- ステップ 2 ユーザ名を [Username] フィールドに入力します。
- ステップ 3 ACS が表示したシステム生成 PIN を RSA SecurID デバイスに入力し、矢印アイコンをクリックします。
- RSA SecurID デバイスは、パスコードを表示します。
- ステップ 4 RSA SecurID デバイスからパスコードをコピーして、ACS Web インターフェイスのパスワードフィールドに同じものを入力し、[Login] をクリックします。

ACS は、管理者が Web インターフェイスにログインできるようにします。RSA SecurID サーバに対する後続の管理者認証が成功します。

管理者認証のログは、[Monitoring and Reports] > [Reports] > [ACS Reports] > [ACS Instance] > [ACS Administrator Logins] ページにあります。



- (注) ACS CLI から RSA SecurID サーバに対して ACS 管理者を認証するには、前述の ACS CLI の **acs-config** モードと同じ手順を使用します。ACS CLI から RSA SecurID サーバに対して管理者を認証する際、1 つの CLI 認証に対して 2 つのログ エントリがあります。1 つのエントリは ACS Web インターフェイスに関するもので、もう 1 つは CLI に関するものです。両方のエントリで、ループバック アドレス (127.0.0.1) として IP アドレスが表示されます。ACS Web インターフェイスのログ エントリは、認証要約と詳細な手順を表示します。一方、CLI エントリは認証の概要だけをリストし、詳細な手順はリストしません。
-



- (注) 次のリンクから RSA SecurID ソフトウェア トークンをダウンロードできます。
<http://www.emc.com/security/rsa-securid/rsa-securid-software-authenticators/ms-windows.htm>
-

関連項目

- RADIUS ID サーバに対する管理者の認証 (16-24 ページ)

管理者認可ポリシー

管理アクセス コントロールの認可ポリシーはログイン時に管理者に動的にロールを割り当てるために使用されます。管理者のロールは、ポリシーで定義された規則に従って設定されます。ポリシーに定義されている規則に従って、条件には、外部データベースで認証されるときにグループおよび属性を含めることができます。ACS は、取得した属性をその後のポリシーで使用できます。

認可ポリシー ベースのロール割り当ては内部および外部管理者アカウントの両方に適用されます。外部管理者アカウントにロールを割り当てるのに使用可能なこれが唯一の方法です。

管理者認可ポリシーでは、各規則に 1 つ以上の条件があり、認証と結果に使用されます。

サポートされる条件は次のとおりです。

- システム ユーザ名
- システムの日付と時刻
- 管理者クライアント IP アドレス
- AD ディクショナリまたは LDAP ディレクトリ（外部グループおよび属性）

通常は、RADIUS ID サーバから返される属性に基づいて許可ポリシーを設定する可能性も追加したことになります。

管理者 ID ポリシーおよびパスワード タイプ機能により、管理者は Active Directory または LDAP の ID ストアなどの外部 ID ストアの要求を認証し、管理者グループおよび属性を取得することができます。管理者認可ポリシー規則は、次の取得したグループと属性に基づいて設定できます。

管理者に割り当てられる一連の管理者ロールで管理者認可ポリシーの結果を設定できます。

サポートされる認可ポリシーの結果は次のとおりです。

- [Administrator Role Result] : 1 つ以上の管理者ロール
- [Deny Access] : 認証失敗

認可ポリシー内の規則は、作成、複製、編集、および削除できます。また、規則はイネーブルおよびディセーブルにすることもできます。

管理者認可ポリシーの設定

管理者認可ポリシーは、ACS 管理者のロールを決定します。

AAC アクセス サービスのプロパティ ページの説明については、[アクセスサービスの一般プロパティの設定 \(10-13 ページ\)](#) を参照してください。


このページは、次のことを実行する場合に使用します。

- 規則を表示します。
- 規則を削除します。
- 規則を作成、複製、編集、およびカスタマイズできるページを開きます。

[System Administration] > [Administrative Access Control] > [Authorization] > [Standard Policy] を選択します。

表 16-11 で説明されている [Administrator Administration Authorization Policy] ページが表示されます。

表 16-11 [Administrator Authorization Policy] ページ

オプション	説明
Status	規則のステータスは、次のとおりです。 <ul style="list-style-type: none"> • Enabled : 規則はアクティブです。 • Disabled : ACS によって規則の結果は適用されません。 • Monitor : 規則はアクティブですが、ACS によって規則の結果は適用されません。ヒットカウントなどの結果はログに書き込まれます。ログ エントリには、規則がモニタだけであることを示す情報が含まれます。モニタ オプションは、新規の規則の結果を確認する場合に特に役立ちます。
Name	ルールの名前。
Conditions	規則の範囲を定義する条件。規則で使用する条件のタイプを変更するには、[Customize] ボタンをクリックします。使用する条件をあらかじめ定義しておく必要があります。
Results	対応する規則が一致したときに適用される管理者ロールを表示します。 規則の結果をカスタマイズできます。規則は、管理者ロールを適用できます。表示されるカラムには、カスタマイゼーション設定が反映されます。
Hit Count	規則が一致した回数。このカラムを更新およびリセットするには、[Hit Count] ボタンをクリックします。
Default Rule	次の場合に、ACS によってデフォルト規則が適用されます。 <ul style="list-style-type: none"> • イネーブルな規則が一致しない。 • 他の規則が定義されていない。 デフォルト規則を編集するには、リンクをクリックします。デフォルト規則の結果だけを編集できます。デフォルト規則は削除、ディセーブル、または複製できません。
[Customize] ボタン	ポリシー規則で使用する条件および結果のタイプを選択する [Customize] ページを開きます。 [Conditions] および [Results] カラムには、カスタマイゼーション設定が反映されます。  注意 規則を定義したあとで条件タイプを削除した場合、その条件タイプについて設定した条件は失われます。
[Hit Count] ボタン	[Policy] ページの [Hit Count] 表示をリセットおよび更新できるウィンドウが開きます。 Hit カウンタの表示 (10-10 ページ) を参照してください。

管理者認可規則のプロパティの設定

このページは、AAC アクセス サービスの管理者ロールを決定する規則を作成、複製、および編集する場合に使用します。

[System Administration] > [Administrative Access Control] > [Authorization] > [Standard Policy] を選択し、[Create]、[Edit]、[Duplicate] のいずれかをクリックします。

表 16-12 で説明されている [Administrator Authorization Rule Properties] ページが表示されます。

表 16-12 [Administrators Authorization Rule Properties] ページ

オプション	説明
General	
Name	ルールの名前。規則を複製する場合は、最小設定として固有の名前を入力する必要があります。その他のフィールドはすべて任意です。
Status	規則のステータスは、次のとおりです。 <ul style="list-style-type: none"> • Enabled : 規則はアクティブです。 • Disabled : ACS によって規則の結果は適用されません。 • Monitor : 規則はアクティブですが、ACS によって規則の結果は適用されません。ヒットカウントなどの結果はログに書き込まれます。ログ エントリには、規則がモニタだけであることを示す情報が含まれます。モニタ オプションは、新規の規則の結果を表示して確認する場合に特に役立ちます。
Conditions	
conditions	これらは、規則に対して設定できる条件です。デフォルトでは、複合条件が表示されます。 [Policy] ページで [Customize] ボタンを使用して、表示される条件を変更できます。 各条件のデフォルト値は、[ANY] です。条件の値を変更するには、条件チェックボックスをオンにし、値を指定します。 [Compound Condition] をオンにすると、条件フレームに式ビルダーが表示されます。詳細については、 複合条件の設定 (10-41 ページ) を参照してください。
Results	
Roles	規則に適用されるロール。

管理者のログインプロセス

管理者が ACS Web インターフェイスにログインすると、ACS 5.8 では、次のように認証を実行します。

管理者アカウントが管理者内部 ID ストアのリカバリ アカウントとして設定されていると、ACS は、ID ポリシーおよび認可ポリシーをバイパスし、管理者内部 ID ストアに対して管理者を認証し、ロールを静的に割り当てます。管理者アカウントがリカバリ アカウントでない場合、ACS はポリシーベースの認証に進みます。

ポリシーベースの認証の一環として、ACS では、ID ポリシーおよび認可ポリシーの設定で AAC サービスを取得します。ACS は、ID ポリシーを評価し、その結果として ID ストアを取得します。ID ポリシーの結果が管理者内部 ID ストアである場合、ACS はパスワードを評価し、結果として ID ストアを取得します。

ACS は、管理者アカウントが外部 ID ストアに設定されている場合に、選択されている ID ストアに対して管理者を認証し、ユーザ グループとユーザ属性を取得します。

管理者アカウントが内部 ID ストアに設定されているときに、静的ロール割り当てがある場合は、ACS は管理者ロールのリストを抽出します。

管理者アカウントが、外部または内部 ID ストアに設定されているときに、動的ロール割り当てがある場合は、ACS は、認可ポリシーを評価して、管理者ロールのリストを取得し、それを動的に使用するか、結果として [Deny Access] を取得します。

選択したロールに基づいて、ACS は認証を行い、管理者のアクセス制限と認証を管理します。Deny Access が評価の結果である場合、ACS は管理者へのアクセスを拒否し、カスタマー ログに失敗の理由を記録します。



(注) Super Admin ロールのある管理者には、他の管理者のロールと権限を変更する権利があります。



(注) AD または LDAP サーバの管理者パスワードが期限切れまたはリセットの場合、ACS は Web インターフェイスへの管理者アクセスを拒否します。

管理者パスワードのリセット

管理者アクセスの設定中、すべての管理者アカウントがロックアウトされ、管理者が企業内のいずれの IP アドレスからも ACS にアクセスできなくなる場合があります。この場合、ACS Config CLI から管理者パスワードをリセットする必要があります。すべての管理者パスワードをリセットするには、次のコマンドを使用する必要があります。

access-setting accept-all

本コマンドについての詳しい情報は、『[CLI Reference Guide for Cisco Secure Access Control System 5.8](#)』を参照してください。



(注) ACS Web インターフェイスでは管理者パスワードをリセットできません。

管理者パスワードの変更

ACS 5.8 には、新しい Change Admin Password というロールが導入されました。このロールが割り当てられた管理者は、別の管理者のパスワードを変更できます。管理者のアカウントがディセーブルになっている場合、Change Admin Password ロールが割り当てられている他の管理者は、ACS Web インターフェイスからディセーブルになっているアカウントをリセットできません。ここでは、次の内容について説明します。

- [自分の管理者パスワードの変更 \(16-30 ページ\)](#)
- [別の管理者のパスワードのリセット \(16-31 ページ\)](#)

自分の管理者パスワードの変更



(注) すべての管理者は、自分のパスワードを変更できます。この操作を実行するのに特別なロールは必要ありません。

パスワードを変更するには、次の手順を実行します。

ステップ 1 [My Workspace] > [My Account] を選択します。

[My Account] ページが表示されます。有効な値については、[\[My Account\] ページ \(5-2 ページ\)](#)を参照してください。

- ステップ 2 [Password field] セクションに、現在の管理者パスワードを入力します。
- ステップ 3 [New Password] フィールドに、新しい管理者パスワードを入力します。
- ステップ 4 [Confirm Password] フィールドに、新しい管理者パスワードを再入力します。
- ステップ 5 [Submit] をクリックします。
管理者パスワードが作成されます。
-

acs reset-password コマンドを使用して ACS 管理者アカウントのパスワードをリセットすることもできます。本コマンドについての詳しい情報は、『[CLI Reference Guide for Cisco Secure Access Control System 5.8](#)』を参照してください。

別の管理者のパスワードのリセット

Super Admin ロールまたは ChangeAdminPassword ロールを持つ内部 Web 管理者は他の管理者のパスワードをリセットまたは変更できます。別の管理者のパスワードをリセットするには、次の手順を実行します。

- ステップ 1 [System Administration] > [Administrators] > [Accounts] を選択します。
管理者アカウントのリストを含む [Accounts] ページが表示されます。
- ステップ 2 パスワードを変更する管理者アカウントのチェックボックスをオンにし、[Change Password] をクリックします。
[Authentication Information] ページが表示され、管理者のパスワードが最後に変更された日付が示されます。
- ステップ 3 [Password] フィールドに、新しい管理者パスワードを入力します。
- ステップ 4 [Confirm Password] フィールドに、新しい管理者パスワードを再入力します。
- ステップ 5 他の管理者が最初のログイン時にパスワードを変更できるように、[Change password on next login] チェックボックスをオンにします。
- ステップ 6 [Submit] をクリックします。
管理者パスワードがリセットされます。
-

関連項目

- [管理者の認証設定 \(16-15 ページ\)](#)
- [ロールについて \(16-3 ページ\)](#)
- [管理者アカウントとロールの関連付け \(16-7 ページ\)](#)
- [事前定義済みのロールの表示 \(16-14 ページ\)](#)

