CHAPTER 17

スタンドアロン Content Engine での管理ログイン認証と許可の設定

この章では、スタンドアロン Content Engine の管理ログイン認証および許可サポートの設定方法について説明します。また、設定、監視、トラブルシューティングの目的で、ローカル データベースと外部 RADIUS および TACACS+ データベースを使用して、Content Engine にアクセスする管理者からのログイン要求を処理するようにスタンドアロン Content Engine を設定する方法について説明します。

（注） スタンドアロン Content Engine を通して処理される要求されたコンテンツへのユーザ アクセスをコントロールするコンテンツ認証および許可は、Content Engine 用の管理ログイン認証および許可とは無関係です。コンテンツの認証および許可の詳細は、第 10 章「スタンドアロン Content Engine のコンテンツ認証および許可の設定」を参照してください。

この章で使用する CLI（コマンドライン インターフェイス）コマンドの構文および使用方法については、『*Cisco ACNS Software Command Reference*』Release 5.5 を参照してください。Content Distribution Manager に登録している Content Engine のログイン認証および許可の設定方法については、『*Cisco ACNS Software Configuration Guide for Centrally Managed Deployments*』Release 5.5 を参照してください。

この章の内容は、次のとおりです。

- 管理ログイン認証および許可の概要（p.17-2）
- 管理ログイン認証および許可の設定（p.17-8）
- 管理認証および許可の設定の表示（p.17-19）

管理ログイン認証および許可の概要

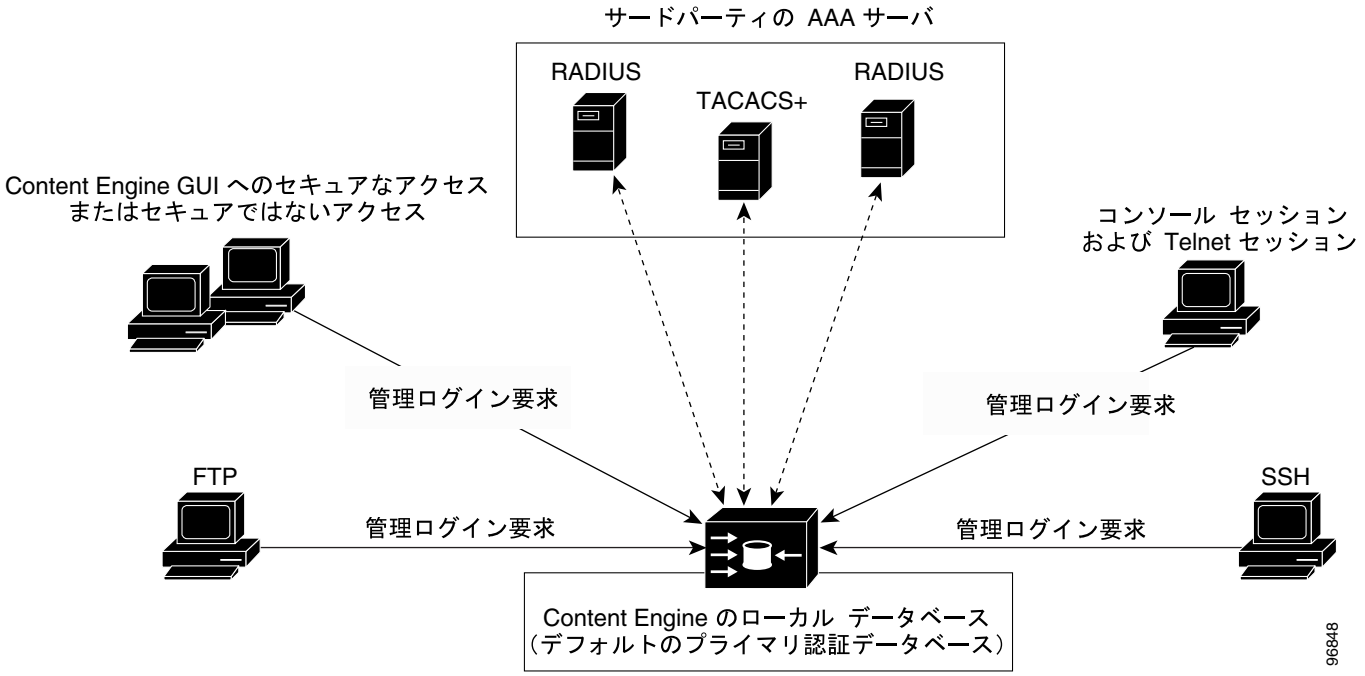
管理ログイン認証および許可を使用して、Content Engine への管理者アクセス権限を制御します。たとえば、定義済みの ACNS ソフトウェア スーパーユーザ アカウント（ルート管理者）を使用して管理者がログインすると、Content Engine は、その管理者に最大の権限レベル（レベル 15）を与えます。これにより、管理者は、ログイン セッション中にすべての Content Engine 管理タスクを実行できます。たとえば、この管理者は次のどの管理タスクも実行できます。

- Content Engine を設定する。
- Content Engine が収集した統計情報を取得する。
- Content Engine を再ロードする。

（注）　管理ログイン アカウントの管理方法については、「管理ログイン アカウントの管理」（p.5-3）を参照してください。

図 17-1 は、コンソールまたは Content Engine GUI を通して、管理者が Content Engine にどのようにしてログインできるかを示しています。これらの管理者ログイン要求を処理するために、Content Engine は指定された認証データベースをチェックし、ユーザのユーザ名とパスワードを確認し、特別な管理者がログイン セッション時に承認されるアクセス権を判別します。Content Engine は管理ログイン要求を受信すると、ローカル データベースまたは遠隔地のサードパーティ データベース（TACACS+ データベースまたは RADIUS データベース）をチェックし、パスワードでユーザ名を確認し、管理者アクセス権を判別します。

図 17-1　認証データベースとスタンドアロン Content Engine



（注）　ACNS 5.1 ソフトウェアおよびそれ以降のリリースでは、Content Engine GUI へのセキュア アクセスまたはノンセキュア アクセスがサポートされます（Content Engine GUI へのセキュアなアクセスまたはノンセキュアなアクセスのいずれか一方はサポート可能ですが、セキュアなアクセスとノンセキュアなアクセスは同時にサポートできません）。

セキュアな Content Engine GUI がデフォルトです（https://*Content_Engine_ip_address:*8003）。詳細は、「Content Engine GUI へのログイン」（p.4-56）を参照してください。

これらの認証と許可の方式を任意に組み合わせて設定し、スタンドアロン Content Engine への管理ログイン アクセスをコントロールできます。

- ローカル認証および許可 —「ローカル データベースを介したログイン認証および許可の概要」（p.17-5）を参照
- RADIUS —「RADIUS 認証および許可の概要」（p.17-6）を参照
- TACACS+ —「TACACS+ 認証と許可の概要」（p.17-6）を参照

デフォルトでは、Content Engine は、管理ログイン要求を処理する基本方式として、ローカル ログイン認証方式を使用します。ローカル認証を他の認証方式とともにイネーブルにし、優先度フラグ（プライマリ、セカンダリ、またはターシャリ）を設定していない場合、ローカル認証が常に試行されます。コンソールと Telnet 接続では、複数の異なるログイン認証方式を指定できません。

デフォルトの管理ログイン認証と許可の設定

デフォルトでは、Content Engine はローカル データベースを使用して、管理ユーザ用のログイン認証および許可権限を取得します。

（注）　**authentication** グローバル コンフィギュレーション コマンドにより、Content Engine への管理ログインおよび設定のアクセスを決定する認証方式を設定します。

表 17-1 に、管理ログイン認証と許可のデフォルト設定を示します。

表 17-1　管理ログイン認証と許可のデフォルト設定

機能	デフォルト値
管理ログイン認証	イネーブル
管理設定許可	イネーブル
認証サーバに到達できないために発生する認証サーバのフェールオーバー	ディセーブル
TACACS+ ログイン認証（コンソールおよび Telnet）	ディセーブル
TACACS+ 許可（コンソールおよび Telnet）	ディセーブル
TACACS+ 鍵	未指定
TACACS+ サーバ タイムアウト	5 秒
TACACS+ 再送信の回数	2 回
RADIUS ログイン認証（コンソールおよび Telnet）	ディセーブル
RADIUS 認証（コンソールおよび Telnet）	ディセーブル

表 17-1　管理ログイン認証と許可のデフォルト設定（続き）

機能	デフォルト値
RADIUS サーバの IP アドレス	未指定
RADIUS サーバの UDP 許可ポート	ポート 1645
RADIUS 鍵	未指定
RADIUS サーバのタイムアウト	5 秒
RADIUS 再送信の回数	2 回

これらのデフォルト値は、Content Engine CLI または GUI を使用して変更できます。「管理ログイン認証および許可の設定」（p.17-8）を参照してください。

管理ログイン認証用のフェールオーバーの概要

デフォルトでは、Content Engine がプライマリ管理認証方式に失敗したときは、必ずセカンダリ管理認証方式にフェールオーバーします。ACNS 5.0.5 ソフトウェア リリースより前の ACNS ソフトウェア リリースでは、管理ログイン認証用のデフォルトのフェールオーバー方式を変更できませんでした。

ACNS 5.0.5 ソフトウェアおよびそれ以降のリリースでは、このデフォルトのログイン認証フェールオーバー方式を変更できます。スタンドアロン Content Engine には、Content Engine GUI（**System** > **Authentication** の順に選択し、**Failover due to Server Unreachable** チェックボックスにチェックマークを付けます）または CLI（**authentication fail-over server unreachable** グローバル コンフィギュレーション コマンドを使用します）を使用して、アクセス不可のサーバが原因のフェールオーバーを有効にできます。

次の例は、認証サーバに到達できない場合にのみ実行するように管理ログイン認証用のフェールオーバーを設定する方法を示しています。この場合、Content Engine は、管理ログイン認証サーバに到達できないときに、次の認証方式を照会だけ行います。

```
ContentEngine(config)# authentication fail-over server-unreachable
ContentEngine(config)#
```

ログイン認証のフェールオーバー機能を使用するには、TACACS+ または RADIUS をプライマリ ログイン認証方式として設定し、ローカルをセカンダリ ログイン認証方式として設定する必要があります。

failover due to unreachable server オプションがイネーブルになっている場合、次の点に注意してください。

- Content Engine 上では、2 つのログイン認証方式（プライマリおよびセカンダリ認証方式）のみが許可されます。
- Content Engine が、プライマリ認証方式からセカンダリ認証方式にフェールオーバーするのは、指定された認証サーバに到達できない場合のみです。

たとえば、failover due to the unreachable server オプションがイネーブルで、RADUIS がプライマリ ログイン認証方式として、ローカルがセカンダリ ログイン認証スキームとして設定されている場合、次のようなことが発生します。

- スタンドアロン Content Engine が管理ログイン要求を受け取ると、Content Engine は RADIUS 認証サーバに照会を行います。
- RADIUS サーバに到達できる場合、スタンドアロン Content Engine はこの RADIUS データベースを使用して管理者を認証します。

- RADIUS サーバに到達できない場合、スタンドアロン Content Engine は、セカンダリ認証方式（Content Engine がローカル認証データベースに照会を行う）を試行して、管理者を認証します。

（注）　この RADIUS サーバに到達できない場合に限り、認証用にローカル データベースに問い合わせを行います。それ以外の場合（たとえば、RADIUS サーバでの認証に失敗した場合）には、認証用にローカル データベースに問い合わせません。

反対に、failover due to unreachable server オプションがディセーブルの場合、スタンドアロン Content Engine は、プライマリ認証データベースでの認証に失敗した理由に関係なく、セカンダリ認証データベースに問い合わせます。

すべての認証データベースを使用できる場合、これらすべてのデータベースに、選択された優先度順に、およびフェールオーバー理由に基づいて照会していきます。フェールオーバーの理由が指定されていない場合には、優先度の順にすべてのデータベースが照会されます。たとえば、最初にプライマリ認証データベース、次にセカンダリ認証データベース、最後にターシャリ認証データベースが照会されます。

ローカルおよびリモート データベース（TACACS+ および RADIUS）は、Content Engine CLI または GUI を使用して、有効または無効にできます。Content Engine は、すべてのデータベースが無効であるかどうかを確認し、無効の場合、システムをデフォルトの状態（認証用にローカル データベースが照会される）に設定します。このデフォルトの状態については、「デフォルトの管理ログイン認証と許可の設定」（p.17-3）を参照してください。

各種のログイン認証および許可方式については、次の各項を参照してください。

- ローカル データベースを介したログイン認証および許可の概要（p.17-5）
- RADIUS 認証および許可の概要（p.17-6）
- TACACS+ 認証と許可の概要（p.17-6）

（注）　ローカルに配置されているスタンドアロン Content Engine 上で、管理ログイン認証および許可の設定を行う方法については、「管理ログイン認証および許可の設定」（p.17-8）を参照してください。

ローカル データベースを介したログイン認証および許可の概要

ローカル認証および許可では、ローカルに設定されているログインとパスワードを使用して、管理ログイン認証を行います。これらのログインとパスワードは、各 Content Engine に対してローカルです。また、個々のユーザ名にはマップされません。

デフォルトでは、ローカル ログイン認証は最初はイネーブルになっています。他のログイン認証方式（複数可）をイネーブルにしたあとでのみ、ローカル ログイン認証をディセーブルにできます。ただし、ローカル ログイン認証がディセーブルになっているときに、他の管理ログイン認証方式をすべてディセーブルにすると、ローカル ログイン認証は自動的に再度イネーブルになります。

RADIUS 認証および許可の概要

RADIUS とは、クライアント / サーバ認証のことで、Network Access Server（NAS）が、ネットワーク装置に接続しようとするユーザの認証に使用する許可アクセス プロトコルです。NAS はクライアントとして機能し、ユーザ情報を 1 台または複数の RADIUS サーバに送信します。NAS は、1 台または複数台の RADIUS サーバから受信する応答に基づいて、ユーザへのネットワーク アクセスの許可または拒否を行っています。RADIUS は、RADIUS クライアントとサーバ間の転送に UDP を使用します。

ユーザはクライアントとサーバ上で RADIUS 鍵を設定できます。クライアント上で鍵を設定する場合、RADIUS サーバ上で設定されている鍵と同一にする必要があります。RADIUS クライアントとサーバは、この鍵を使用して、送信される RADIUS パケットをすべて暗号化します。RADIUS 鍵を設定しない場合は、パケットは暗号化されません。鍵自体がネットワーク上に送信されることはありません。

（注）　RADIUS プロトコルの機能の詳細は、RFC 2138『*Remote Authentication Dial In User Service (RADIUS)*』を参照してください。

RADIUS 認証は通常、次のような場合に実行されます。

- 管理ログイン認証 — 管理者がスタンドアロン Content Engine に最初にログインして、監視、設定、トラブルシューティングの目的で Content Engine を設定する場合。詳細は、「RADIUS による管理ログイン認証および許可のイネーブル化とディセーブル化」（p.17-17）を参照してください。
- HTTP 要求認証 — Content Engine でサービスされているコンテンツへのアクセス権限が必要なサービス要求をエンド ユーザが送信する場合。詳細は、「RADIUS 認証サービスの設定」（p.10-19）を参照してください。

RADIUS 認証は、デフォルトでは無効になります。RADIUS 認証と他の認証方式を同時にイネーブルにできます。最初に使用する認証方式を指定することもできます。RADIUS 認証設定については、「スタンドアロン Content Engine のための RADIUS 認証設定の指定」（p.17-9）を参照してください。

TACACS+ 認証と許可の概要

TACACS+ は、ネットワーク装置へのアクセスを制御します。ネットワーク装置と中央データベース間で、NAS 情報を交換してユーザまたはエンティティの身元を識別しています。TACACS+ は、TACACS（RFC 1492 で指定される UDP ベースのアクセス制御プロトコル）の拡張バージョンです。TACACS+ は、TCP を使用して、信頼性の高い配信を行い、TACACS+ サーバとネットワーク装置の TACACS+ デーモン間のトラフィックをすべて暗号化します。

TACACS+ では、固定パスワード、ワンタイム パスワード（使い捨てパスワード）、およびチャレンジ レスポンス認証などのさまざまなタイプの認証が可能です。TACACS+ 認証は通常、次のような場合に実行されます。

- 管理ログイン認証 — 管理者がスタンドアロン Content Engine に最初にログインして、監視、設定、トラブルシューティングの目的で Content Engine を設定する場合。詳細は、「TACACS+ による管理ログイン認証および許可のイネーブル化とディセーブル化」（p.17-18）を参照してください。
- HTTP 要求認証 — Content Engine でサービスされているコンテンツへのアクセス権限が必要なサービス要求をエンド ユーザが送信する場合。詳細は、「TACACS+ 認証サービスの設定」（p.10-20）を参照してください。

ユーザが、制限されたサービスを要求すると、TACACS+ は MD5 暗号化アルゴリズムを使用してユーザのパスワード情報を暗号化し、TACACS+ パケット ヘッダーを追加します。このヘッダー情報は、送信されているパケット タイプ（たとえば、認証パケット）、パケット シーケンス番号、使用される暗号化タイプ、およびパケット長の合計を識別します。次に、TACACS+ プロトコルはパケットを TACACS+ サーバに転送します。

TACACS+ サーバは、認証、許可、およびアカウンティングの機能を備えています。これらのサービスが TACACS+ 機能のすべてです。これらの機能は互いに独立しているため、TACACS+ 設定に応じてサービスの一部またはすべてを使用できます。

TACACS+ サーバがパケットを受信すると、次の操作を実行します。

- ユーザ情報を認証し、ログイン認証が正常に行われたか失敗したかをクライアントに通知する。
- 認証が続行されること、またクライアントが情報を追加する必要があることをクライアントに通知する。このチャレンジ レスポンス プロセスは、ログイン認証が正しく行われるか、失敗するまで、繰り返し実行されます。

ユーザはクライアントとサーバ上で TACACS+ 鍵を設定できます。Content Engine 上で鍵を設定する場合、TACACS+ サーバ上で設定された鍵と同一にする必要があります。TACACS+ クライアントとサーバは、この鍵を使用して、送信される TACACS+ パケットをすべて暗号化します。TACACS+ 鍵を設定しない場合は、パケットは暗号化されません。

TACACS+ 認証は、デフォルトでディセーブルになります。TACACS+ 認証とローカル認証を同時にイネーブルにできます。

TACACS+ イネーブル パスワード属性

ACNS ソフトウェアの CLI EXEC モードは、システム動作の設定、表示、および試験に使用します。これは、ユーザと権限の 2 つのアクセス レベルに分かれます。権限レベルの EXEC モードにアクセスするには、ユーザ アクセス レベルのプロンプトで **enable** EXEC コマンドと入力し、パスワードの入力するプロンプトが表示されたときに、特権 EXEC パスワード（スーパーユーザまたは admin と同じパスワード）を指定します。

TACACS+ には、管理レベルのユーザごとに異なるイネーブル パスワードを管理者が定義するためのイネーブル パスワード機能があります。管理レベルのユーザが、admin または admin と同じユーザ アカウント（特権レベル 15）ではなく、Content Engine に通常レベルのユーザ アカウント（特権レベル 0）でログインした場合は、そのユーザが権限レベル EXEC モードにアクセスするには、admin パスワードを入力する必要があります。

```
ContentEngine> enable
Password:
```

この注意事項は、ACNS ユーザがログイン認証のために TACACS+ を使用している場合にも該当します。

管理ログイン認証および許可の設定

ここでは、監視、設定、トラブルシューティングの目的で Content Engine にログインする ACNS 管理者用のログイン認証と許可を設定する方法について説明します。

（注）　スタンドアロン Content Engine を通して処理される、要求されたコンテンツへのユーザ アクセスをコントロールするコンテンツ認証および許可は、Content Engine 用の管理ログイン認証および許可とは無関係です。

コンテンツ認証および許可の詳細については、第 10 章「スタンドアロン Content Engine のコンテンツ認証および許可の設定」を参照してください。

スタンドアロン Content Engine で管理ログイン認証と許可を設定する手順は、次のとおりです。

ステップ 1　スタンドアロン Content Engine に対して設定する、管理ログイン認証要求時に使用されるログイン認証方式（たとえば、ローカル データベースをプライマリ ログイン データベースとし、RADIUS 認証サーバをセカンダリ認証サーバとする）を決定します。

ステップ 2　ログイン認証サーバの設定値を Content Engine 上で設定します（リモート認証データベース リストを使用する場合）。

たとえば、Content Engine がログイン要求の認証に使用するリモート RADIUS サーバまたは TACACS+ サーバの IP アドレスを指定します。詳しくは、次の項を参照してください。

- スタンドアロン Content Engine のための RADIUS 認証設定の指定（p.17-9）
- スタンドアロン Content Engine のための TACACS+ 認証設定の指定（p.17-11）

ステップ 3　Content Engine が管理ログイン要求の処理に使用する、ログイン認証の設定方式を指定します。

- 管理ログイン認証方式を指定します。
- 管理ログイン許可方式を指定します。
- 管理ログイン認証サーバ用のフェールオーバー 方式を指定します（任意）。

たとえば、ログイン要求を処理するのに Content Engine がどの管理認証データベースをチェックするかを指定します。詳細は、「管理ログイン認証および許可方式の指定とイネーブル化」（p.17-13）を参照してください。

注意　ローカル認証および許可をディセーブルにする場合は、事前に、RADIUS または TACACS+ 認証が正しく設定され動作していることを確認してください。RADIUS または TACACS+ が正しく設定されていない場合、あるいは RADIUS サーバまたは TACACS+ サーバがオンラインになっていない場合にローカル認証をディセーブルにすると、Content Engine にログインできないことがあります。

ローカル認証がディセーブルになっているときに、他の認証方法をすべてディセーブルにすると、ローカル認証は自動的に再度イネーブルになります。

次の項では、スタンドアロン Content Engine に認証サーバ設定値を指定する方法について説明します。

- スタンドアロン Content Engine のための RADIUS 認証設定の指定（p.17-9）
- スタンドアロン Content Engine のための TACACS+ 認証設定の指定（p.17-11）

スタンドアロン Content Engine のための RADIUS 認証設定の指定

RADIUS 認証のクライアントは、ACNS 5.x ソフトウェアを実行する Content Engine 上に存在します。これらのクライアントは、可能な場合、中央（リモート）の RADIUS サーバに認証要求を送信します。RADIUS サーバには、ログイン認証情報とネットワーク サービス アクセス情報が入っています。

RADIUS 認証をスタンドアロン Content Engine で設定するには、一連の RADIUS 認証サーバの設定値を Content Engine 上で設定する必要があります。Content Engine GUI または CLI を使用して、ローカルに配置された Content Engine に対して、一連の RADIUS 認証サーバの設定を行うこともできます。

表 17-2 で、RADIUS 認証設定について説明します。

表 17-2　スタンドアロン Content Engine のための RADIUS 認証設定

設定	説明
RADIUS サーバ	Content Engine が RADIUS 認証に使用する RADIUS サーバ。Content Engine で、指定した RADIUS サーバを使用するには、RADIUS サーバの IP アドレスまたはホスト名およびポート情報を入力します。異なるホストを 5 つまで指定できます。以前の RADIUS の配置には、ポート番号 1645 を使用していましたが、現在の公式な RADIUS 用のポート番号は 1812 です。異なるポート番号が 5 つまで使用可能です。
RADIUS 鍵	RADIUS クライアント（スタンドアロン Content Engine）と RADIUS サーバ間のすべての通信の暗号化と認証に使用される鍵。この鍵には、最大 15 文字まで指定できます。デフォルトは指定されていません。 **ヒント**　同一の RADIUS 鍵が RADIUS サーバ上でイネーブルになっていることを確認してください。
RADIUS タイムアウト時間	Content Engine がタイムアウトを宣言するまで、指定の RADIUS 認証サーバから応答を待つ時間（秒）。範囲は 1 ～ 20 秒です。デフォルト値は 5 秒です。
RADIUS 再送信回数	RADIUS タイムアウト時間を超過した場合、Content Engine が接続を RADIUS に再送信する回数。範囲は 1 ～ 3 回です。デフォルト値は 2 回です。

これらの RADIUS 認証設定値を Content Engine 上で設定後、次のタイプの RADIUS 認証を Content Engine 上でイネーブルにできます。

- 「RADIUS による管理ログイン認証および許可のイネーブル化とディセーブル化」（p.17-17）で説明している RADIUS ログイン認証および許可
- 「RADIUS 認証サービスの設定」（p.10-19）で説明している RADIUS HTTP 要求認証

Content Engine GUI を使用して、スタンドアロン Content Engine で RADIUS 認証を設定するには、**Caching > RADIUS** の順に選択します。表示される RADIUS Authentication Settings ウィンドウを使用します。**Enable RADIUS On** オプション ボタンをクリックして、この Content Engine 上で RADIUS 認証をイネーブルにします。RADIUS Authentication Settings ウィンドウを使用して、その他の RADIUS 認証の設定値を指定します。このウィンドウの詳細については、ウィンドウの **HELP** ボタンをクリックしてください。

Content Engine CLI を使用して、スタンドアロン Content Engine で RADIUS 認証を設定する手順は、次のとおりです。

ステップ 1　1 台または複数の RADIUS サーバを指定します。オプションとして、サーバで使用する送信先 UDP ポートを指定します。デフォルトのポートは 1645 です。

```
ContentEngine(config)# radius-server host ip_addr [auth-port port]
```

次の例は、RADIUS サーバを 172.16.52.3 に指定する方法を示しています。

```
ContentEngine(configure)# radius-server 172.16.52.3
```

ステップ 2　Content Engine 上で RADIUS 鍵を指定します。

```
ContentEngine(configure)# radius-server key myradiuskey
```

ステップ 3　RADIUS タイムアウト時間を指定します。

たとえば、Content Engine が、10 秒間待機しても RADIUS サーバからの応答を受信しない場合、タイムアウトを宣言します。

```
ContentEngine(config)# radius-server timeout 10
```

ステップ 4　RADIUS の再送信の回数を指定します。

たとえば、Content Engine が、RADIUS タイムアウトが発生した場合、3 回 RADIUS サーバに再送信を行うように設定します。

```
ContentEngine(config)# radius-server retransmit 3
```

（注）　RADIUS 認証設定（たとえば、RADIUS 鍵）の詳細は、表 17-2 を参照してください。**radius-server** グローバル コンフィギュレーション コマンドの詳細については、『*Cisco ACNS Software Command Reference*』Release 5.5 を参照してください。

次の例では、RADIUS クライアントを Content Engine 上で有効にし、認証用のリモート RADIUS サーバを指定します。さらに RADIUS 鍵を Content Engine 上で指定し、再送信のデフォルト値を受け入れ、domain name と mydomain.net ドメインを RADIUS 認証から除外しています。設定は、**show radius-server** と **show rule all** の EXEC コマンドを使用して表示できます。

```
ContentEngine(config)# radius-server enable
ContentEngine(config)# radius-server host 172.16.90.121
ContentEngine(config)# radius-server key myradiuskey
ContentEngine(config)# rule enable
ContentEngine(config)# rule no-auth domain mydomain.net
```

これで、この Content Engine に対して、「RADIUS による管理ログイン認証および許可のイネーブル化とディセーブル化」（p.17-17）で説明されているように、RADIUS を管理ログイン認証および許可の目的で有効にできます。

スタンドアロン Content Engine のための TACACS+ 認証設定の指定

TACACS+ 認証をスタンドアロン Content Engine に設定するには、一連の TACACS+ 認証の設定値を Content Engine 上で設定する必要があります。Content Engine CLI または GUI を使用して、スタンドアロン Content Engine に対して、この一連の TACACS+ 認証の設定を行うこともできます。

表 17-3 では、TACACS+ 認証設定について説明しています。

（注）　TACACS+ サーバが Content Engine 上に設定されていない場合、TACACS+ 認証は実行されません。

表 17-3　スタンドアロン Content Engine のための TACACS+ 認証設定

設定	説明
TACACS+ サーバ	Content Engine が TACACS+ 認証に使用する TACACS+ サーバ。プライマリ TACACS+ サーバを明示的に指定します。明示的に指定しないと、Content Engine が独自の判断を行います。プライマリ TACACS+ サーバ 1 台とバックアップ TACACS+ サーバ 2 台を設定できます。TACACS+ は、指定のサービスに基づいて、通信用として標準ポート（ポート 49）を使用します。
TACACS+ 鍵	Content Engine が TACACS+ サーバとの通信用に使用する秘密鍵。TACACS+ 鍵の最大文字数は、印刷可能 ASCII 文字で 99 文字を超えない数です（タブを含めない）。空白の鍵文字列がデフォルトです。鍵文字列の先頭のスペースはすべて無視され、中間および最後のスペースは無視されません。鍵内にスペースがある場合でも、二重引用符は不要です。二重引用符が鍵の一部であるときは、記入されます。デフォルトはありません。 **ヒント**　同一の TACACS+ 鍵が TACACS+ サーバに設定されていることを確認してください。
TACACS+ タイムアウト時間	Content Engine がタイムアウトを宣言するまで指定の TACACS+ 認証サーバから応答を待つ時間（秒）。範囲は 1 ～ 20 秒です。デフォルト値は 5 秒です。
TACACS+ 再送信回数	TACACS+ タイムアウト時間が超過した場合、Content Engine が自身の接続要求を TACACS+ に再送信する回数。範囲は 1 ～ 3 回です。デフォルト値は 2 回です。
TACACS+ パスワード認証方式	パスワード認証方式。デフォルトでは、Password Authentication Protocol（PAP）をパスワード認証に使用します。これ以外には、ASCII 平文テキストをパスワード認証に使用するオプションがあります。

Content Engine CLI を使用して、スタンドアロン Content Engine で TACACS+ 認証を設定する手順は、次のとおりです。

ステップ 1　1 台または複数の TACACS+ サーバを指定します。

```
ContentEngine(config)# tacacs server ip_addr [primary]
```

次の例は、ある特定の TACACS+ サーバをプライマリ サーバに指定する方法を示しています。

```
ContentEngine(config)# tacacs server 172.16.50.1 primary
```

次の例は、ある特定の TACACS+ サーバをバックアップ サーバに指定する方法を示しています。この場合、**primary** オプションを指定する必要はありません。

```
ContentEngine(config)# tacacs server 172.16.50.2
```

ステップ 2　TACACS+ 鍵を指定します。

```
ContentEngine(config)# tacacs key key
```

ステップ 3　TACACS+ タイムアウト時間を指定します。

たとえば、Content Engine が、15 秒間待機しても TACACS+ サーバからの応答を受信しない場合、タイムアウトを宣言するよう設定します。

```
ContentEngine(config)# tacacs timeout 15
```

ステップ 4　TACACS+ の再送信の回数を指定します。

たとえば、Content Engine が、TACACS+ タイムアウトが発生した場合、もう 1 度 TACACS+ サーバに再送信を行うように設定します。

```
ContentEngine(config)# tacacs retransmit 1
```

ステップ 5　TACACS+ パスワード認証方式を指定します。

たとえば、**ASCII** キーワードを入力することにより、ASCII 平文テキストを指定します。

```
ContentEngine(config)# tacacs password ascii
```

（注）　TACACS+ 認証設定（たとえば、TACACS+ 鍵の指定）の詳細は、表 17-3 を参照してください。**tacacs server** グローバル コンフィギュレーション コマンドの詳細については、『*Cisco ACNS Software Command Reference*』Release 5.5 を参照してください。

次の例では、spearhead というホスト名を持つ TACACS+ サーバを、プライマリ TACACS+ サーバとして設定しています。Content Engine は、TACACS+ サーバ（spearhead という名）で使用されているのと同一の鍵（human789）を使用するように設定されています。また、デフォルトのタイムアウ

ト時間、再送信回数、およびパスワード タイプが変更されています。この例はまた、Content Engine 上での現行の TACACS+ 設定を表示するための **show tacacs** EXEC コマンドの使用方法も示しています。

```
ContentEngine(config)# tacacs host spearhead primary
ContentEngine(config)# tacacs key human789
ContentEngine(config)# tacacs timeout 10
ContentEngine(config)# tacacs retransmit 5
ContentEngine(config)# tacacs password ascii
ContentEngine(config)# exit

ContentEngine# show tacacs
    Login Authentication for Console/Telnet Session: enabled (secondary)
    Configuration Authentication for Console/Telnet Session: enabled (secondary)

    TACACS+ Configuration:
    ---------------------
    TACACS+ Authentication is off
    Key         = *****
    Timeout     = 5
    Retransmit = 2
    Password type: ascii

    Server                          Status
    ----------------------------    ------
    10.107.192.148                 primary
    10.107.192.168
    10.77.140.77
```

これで、この Content Engine に対して、「TACACS+ による管理ログイン認証および許可のイネーブル化とディセーブル化」（p.17-18）で説明されているように、TACACS+ を管理ログイン認証および許可の目的で有効にできます。

管理ログイン認証および許可方式の指定とイネーブル化

ここでは、スタンドアロン Content Engine 上に各種の管理ログイン認証と許可方式（認証設定）を定義、変更する方法について説明します。

- 使用上の注意事項（p.17-14）
- ローカル　データベースを介したログイン認証および許可の再イネーブル化とディセーブル化（p.17-16）
- RADIUS による管理ログイン認証および許可のイネーブル化とディセーブル化（p.17-17）
- TACACS+ による管理ログイン認証および許可のイネーブル化とディセーブル化（p.17-18）

注意　ローカル認証および許可をディセーブルにする場合は、事前に、RADIUS または TACACS+ 認証が正しく設定され動作していることを確認してください。RADIUS または TACACS+ が正しく設定されていない場合、あるいは RADIUS サーバまたは TACACS+ サーバがオンラインになっていない場合に、ローカル認証をディセーブルにすると Content Engine にログインできないことがあります。

使用上の注意事項

認証設定の方式をスタンドアロン Content Engine に対して定義または変更する場合には、次の重要な点に注意してください。

- ユーザ アクセス管理に外部のアクセス サーバを使用するか、または内部（ローカル）の Content Engine ベースの AAA システムを使用するかの選択は、Content Engine GUI または CLI を使用して行うことができます。
- これらの複数の認証と許可の方式を組み合わせて、スタンドアロン Content Engine 上でアクセスの制御および権限の設定を行うことができます。
  - ローカル認証および許可
  - RADIUS 認証および許可
  - TACACS+ 認証および許可
- ログイン認証および許可（設定）オプションを設定するには、**authentication** グローバル コンフィギュレーション コマンドを使用します。

  authentication {**configuration** {**local** | **radius** | **tacacs**} **enable** [**primary** | **secondary** | **tertiary**] | **fail-over server-unreachable** | **login** {**local** | **radius** | **tacacs**} **enable** [**primary** | **secondary** | **tertiary**]}

  表 17-4 では、**authentication** グローバル コンフィギュレーション コマンドに関するパラメータについて説明しています。

表 17-4　認証 CLI コマンドのパラメータ

パラメータ	説明
configuration	設定認証（許可）を設定します。
local	認証用のローカル方式を選択します。
radius	認証用の RADIUS サーバを選択します。
tacacs	認証用の TACACS+ サーバを選択します。
enable	設定およびログイン認証用のデータベースを有効にします。
primary	（任意）選択した認証データベースをプライマリとして設定します。
secondary	（任意）選択した認証データベースをセカンダリとして設定します。
tertiary	（任意）選択した認証データベースをターシャリ（3 次）として設定します。
fail-over server-unreachable	現行の認証サーバが到達不能の場合にのみ、その次の認証サーバに照会します。
login	ログイン認証データベースを設定します。

- **authentication** グローバル コンフィギュレーション コマンドは、スタンドアロン Content Engine への管理ログインと設定アクセスの両方を設定します。
- **authentication login local** と **authentication configuration local** のグローバル コンフィギュレーション コマンドでは、認証と許可にローカル データベースを使用します。
  - **authentication login** コマンドには、管理者が Content Engine に対する何らかのレベルのアクセス許可を持っているかどうかを判別するための管理ログイン認証方式を指定します。
  - **authentication configuration** コマンドは、認証済みの管理者に対する権限（Content Engine へのユーザ アクセスのレベル）を判別します。
- **authentication login radius** と **authentication configuration radius** のグローバル コンフィギュレーション コマンドは、管理者アクセス レベルの判別に RADIUS リモート サーバを使用します。

- デフォルトでは、管理ログインと設定に対して、ローカル方式がイネーブルになり、TACACS+ と RADIUS の両方式がディセーブルになります。TACACS+ と RADIUS がイネーブルな場合は、ローカルの方式が自動的にイネーブルになります。TACACS+、RADIUS、ローカル方式を同時にイネーブルにできます。
  - **primary** オプションにより、管理ログインと設定の両方の試行に対して、最初の方式が指定されます。
  - **secondary** オプションにより、プライマリ方式に失敗した場合に使用する方式が指定されます。
  - **tertiary** オプションにより、最初の方式と 2 番めの方式が失敗したときに使用する方式が指定されます。

  authentication login コマンドまたは **authentication configuration** コマンドの方式がすべてプライマリに設定されている場合か、すべてがセカンダリまたはターシャリに設定されている場合は、ローカル方式が最初に試行され、次に TACACS+、その次に RADIUS の順に試行されます。

  次の例では、まず最初に、ローカル、TACACS+、および RADIUS の認証と許可を有効にしています。次に、TACACS+ を最初に使用する方式に設定し、ローカルを TACACS+ 方式が失敗したときのセカンダリの方式に設定し、最後に RADIUS をローカルと TACACS+ の両方が失敗したときのターシャリの方式に設定しています。

```
ContentEngine(config)# authentication login tacacs enable primary
ContentEngine(config)# authentication login local enable secondary
ContentEngine(config)# authentication login radius enable tertiary
ContentEngine(config)# authentication configuration tacacs enable primary
ContentEngine(config)# authentication configuration local enable secondary
ContentEngine(config)# authentication configuration radius enable tertiary
```

（注）　**tacacs** グローバル コンフィギュレーション コマンドと TACACS+ サーバでは、TACACS+ 認証および許可の方式を使用するように設定する必要があります。TACACS+ サーバの設定に関する詳細は、「スタンドアロン Content Engine のための TACACS+ 認証設定の指定」（p.17-11）を参照してください。

radius-server グローバル コンフィギュレーション コマンドと RADIUS サーバでは、RADIUS 認証と許可の方式を使用するように設定する必要があります。RADIUS サーバの設定に関する詳細は、「スタンドアロン Content Engine のための RADIUS 認証設定の指定」（p.17-9）を参照してください。

- 認証設定は次の場合に適用されます。
  - コンソールおよび Telnet 接続の試行
  - Secure FTP（SFTP）、SSH（SSH Version 1 および Version 2）、Websense サーバ アクセス
- Content Engine（RADIUS と TACACS+ クライアント）上で RADIUS 鍵または TACACS+ 鍵を設定する場合は、必ず RADIUS サーバまたは TACACS+ サーバで同一の鍵を設定してください。
- 複数の RADIUS サーバまたは TACACS+ サーバを設定する場合は、最初に設定されているサーバがプライマリ サーバになり、このサーバに最初に認証要求が送信されます。セカンダリ サーバおよびターシャリ（3 次）サーバを認証および許可用に指定することもできます。
  - **primary**、**secondary**、または **tertiary** キーワードを **authentication** グローバル コンフィギュレーション コマンドで使用して、サーバをプライマリ、セカンダリ、ターシャリとして指定できます。
  - Content Engine GUI からも、サーバをプライマリ、セカンダリ、またはターシャリとして指定できます。**System** > **Authentication** の順に選択し、次に該当するサーバの隣にあるドロップダウンリストから、**Primary**、**Secondary**、または **Tertiary** を選択します。
- デフォルトでは、Content Engine はローカル データベースを使用して管理ログイン要求を認証し、許可します。Content Engine は、すべての認証データベースが無効になっているかどうかを確認し、無効の場合はシステムをデフォルトの状態に設定します。このデフォルト状態の詳

細については、「デフォルトの管理ログイン認証と許可の設定」（p.17-3）を参照してください。

ローカル データベースを介したログイン認証および許可の再イネーブル化とディセーブル化

デフォルトでは、Content Engine は、ローカル データベースを使用して管理ログイン要求を認証し、許可するように設定されています。この認証と許可方式は、ローカル方式と呼ばれます。Content Engine GUI または CLI を使用して、この認証および許可方式をスタンドアロン Content Engine 上でディセーブル、または再びイネーブルにできます。

注意　ローカル認証および許可をディセーブルにする場合は、事前に、RADIUS または TACACS+ 認証が正しく設定され動作していることを確認してください。RADIUS または TACACS+ が正しく設定されていない場合、あるいは RADIUS サーバまたは TACACS+ サーバがオンラインになっていない場合に、ローカル管理認証をディセーブルにすると Content Engine にログインできないことがあります。

Content Engine でこの認証をディセーブルにしていて、Content Engine GUI から再びイネーブルにする場合には、**System > Authentication** の順に選択します。Authentication Configuration ウィンドウが表示されたら、Local の横にある **Enable** チェックボックスにチェックマークを付けて、ローカル ログイン認証を有効にします。デフォルトでは、ローカル データベースが管理ログイン認証用のプライマリ データベースになります。デフォルトを変更するには、もう 1 つのオプション（たとえば、**Secondary** または **Tertiary**）を **Local** の横にあるドロップダウンリストから選択します。**Update** をクリックします。Authentication Configuration ウィンドウでの操作方法については、このウィンドウの **HELP** ボタンをクリックしてください。

Content Engine CLI を使用して、スタンドアロン Content Engine でローカル方式を再びイネーブルにするには、次のようにします。

ステップ 1　ローカル ログイン認証を再びイネーブルにします。

```
ContentEngine(config)# authentication login local enable
```

ステップ 2　管理ユーザのローカル許可を再びイネーブルにします（セッション中にユーザの特権を制御します）。

```
ContentEngine(config)# authentication configuration local enable
```

管理ユーザには、通常レベルの管理アクセス（制限付き権限レベル 0）、またはスーパーユーザ管理アクセス（特権レベル 15）の 2 つのレベルの特権を与えることができます。管理ユーザの特権レベルの詳細については、「管理ログイン アカウントの管理」（p.5-3）を参照してください。

（注）　スタンドアロン Content Engine 上でローカル管理認証および許可をディセーブルにするには、**authentication** グローバル コンフィギュレーション コマンドの **no** 形式を使用します（たとえば、ローカル管理認証をディセーブルにするのには、**no authentication login local enable** コマンドを使用します）。

RADIUS による管理ログイン認証および許可のイネーブル化とディセーブル化

RADIUS を使用して管理ログイン要求を認証し、許可するようにスタンドアロン Content Engine を設定するときには、以下の重要な点に注意してください。

- デフォルトでは、スタンドアロン Content Engine 上の RADIUS 認証および許可はディセーブルになっています。
- Content Engine で RADIUS 認証をイネーブルにする前に、Content Engine が使用する 1 つまたは複数の RADIUS サーバを指定する必要があります。RADIUS サーバの指定方法については、「スタンドアロン Content Engine のための RADIUS 認証設定の指定」（p.17-9）を参照してください。
- RADIUS 認証と他の認証方式を同時にイネーブルにできます。最初に使用する認証方式を指定するには、**primary** キーワードを使用します。ローカル認証がディセーブルになっているときに、他の認証方法をすべてディセーブルにすると、ローカル認証は自動的に再度イネーブルになります。
- Content Engine GUI または CLI を使用して、スタンドアロン Content Engine 上の RADIUS 認証と許可をイネーブルにできます。

Content Engine GUI から、**System > Authentication** の順に選択します。表示される Authentication Configuration ウィンドウを使用します。Authentication Configuration ウィンドウの使用方法については、このウィンドウの **HELP** ボタンをクリックしてください。

Content Engine CLI を使用して、スタンドアロン Content Engine で RADIUS 認証と許可をイネーブルにする手順は、次のとおりです。

ステップ 1　通常ログイン モードの RADIUS 認証をイネーブルにします。

```
ContentEngine(config)# authentication login radius enable [primary] [secondary]
[tertiary]
```

たとえば、Content Engine に 強制的に RADIUS 認証を最初に試行（TACACS+ 認証を使用する前に試行）させるには、次のコマンドを入力します。

```
ContentEngine(config)# authentication login radius enable primary
```

ステップ 2　RADIUS 許可をイネーブルにします。

```
ContentEngine(config)# authentication configuration radius enable [primary]
[secondary] [tertiary]
```

たとえば、Content Engine に 強制的に RADIUS 許可を最初に試行（TACACS+ 許可を使用する前に試行）させるには、次のコマンドを入力します。

```
ContentEngine(config)# authentication configuration radius enable primary
```

（注）　スタンドアロン Content Engine 上で RADIUS 認証と許可をディセーブルにするには、**no** 形式の **authentication** グローバル コンフィギュレーション コマンドを使用します（たとえば、RADIUS 認証を無効にするには、**no authentication login radius enable** コマンドを使用します）。

TACACS+ による管理ログイン認証および許可のイネーブル化とディセーブル化

TACACS+ を使用して管理ログイン要求を認証し、許可するようにスタンドアロン Content Engine を設定するときには、次の重要な点に注意してください。

- デフォルトでは、スタンドアロン Content Engine 上の TACACS+ 認証および許可はディセーブルになっています。
- **authentication login tacacs** コマンドと **authentication configuration tacacs** コマンドは、管理ログイン認証と許可で TACACS+ リモート サーバを使用し、管理アクセス レベルを特定します。
- Content Engine で TACACS+ 認証をイネーブルにする前に、Content Engine が使用する 1 つまたは複数の TACACS+ サーバを指定する必要があります。TACACS+ サーバの指定方法については、「スタンドアロン Content Engine のための TACACS+ 認証設定の指定」（p.17-11）を参照してください。
- RADIUS と TACACS+ の両方を使用している場合、**primary** キーワードを使用して Content Engine 上で強制的に TACACS+ 認証を最初に実行できます。
- Content Engine GUI または CLI を使用して、スタンドアロン Content Engine 上の TACACS+ 認証と許可をイネーブルにできます。

Content Engine GUI から TACACS+ 認証と許可をイネーブルにするには、**System > Authentication** の順に選択して、表示される Authentication Configuration ウィンドウを使用します。Authentication Configuration ウィンドウの使用方法については、ウィンドウの **HELP** ボタンをクリックしてください。

Content Engine CLI を使用して、スタンドアロン Content Engine で TACACS+ 認証と許可をイネーブルにする手順は、次のとおりです。

ステップ 1　通常ログイン モードの TACACS+ 認証をイネーブルにします。

```
ContentEngine(config)# authentication login tacacs enable [primary]
[secondary] [tertiary]
```

たとえば、Content Engine に 強制的に TACACS+ 許可を最初に試行（RADIUS 許可を使用する前に試行）させるには、次のコマンドを入力します。

```
ContentEngine(config)# authentication login tacacs enable primary
```

ステップ 2　TACACS+ 許可をイネーブルにします。

```
ContentEngine(config)# authentication configuration tacacs enable [primary]
[secondary] [tertiary]
```

たとえば、Content Engine に強制的に TACACS+ 許可を最初に試行（RADIUS 許可を使用する前に試行）させるには、次のコマンドを入力します。

```
ContentEngine(config)# authentication configuration tacacs enable primary
```

（注）　スタンドアロン Content Engine 上で TACACS+ 認証と許可をディセーブルにするには、**authentication** グローバル コンフィギュレーション コマンドの **no** 形式を使用します（たとえば、TACACS+ 認証をディセーブルにするには、**no authentication login tacacs enable** コマンドを使用します）。

管理認証および許可の設定の表示

スタンドアロン Content Engine で現在の管理ログイン認証および許可の設定を表示するには、**show authentication user** EXEC コマンドを入力します。次の出力例が示すように、管理ログイン要求を使用するように Content Engine が設定されている認証方式（たとえば、ローカル、RADIUS、TACACS+）が表示されます。

```
ContentEngine# show authentication user
Authentication scheme fail-over reason: server unreachable

Login Authentication:         Console/Telnet Session
----------------------------- ----------------------
local                         enabled (primary)
radius                        disabled
tacacs                        disabled

Configuration Authentication: Console/Telnet Session
----------------------------- ----------------------
local                         enabled (primary)
radius                        disabled
tacacs                        disabled
```