



## 管理ログインの認証および許可の設定

この章では、WAFS File Engine と Wide Area Application Engine (WAE) の管理ログインの認証および許可を設定する方法について説明します。また、設定、モニタリング、またはトラブルシューティングを目的として、File Engine または WAE へのアクセスを必要としている管理者からのログイン要求を、ローカル データベースと外部 RADIUS、TACACS+、および Windows ドメイン データベースを使用して処理するように File Engine または WAE を設定する方法について説明します。

この章には、次の項があります。

- [管理ログインの認証および許可について、7-2 ページ](#)
- [管理ログインの認証および許可の設定、7-9 ページ](#)
- [認証および許可情報の表示、7-21 ページ](#)



ヒント

プリント サービスのログインの認証および許可は、WAE の管理ログインの認証および許可とは無関係です。プリント サービスの認証および許可の詳細については、[第 8 章「WAFS プリント サービスの設定」](#)を参照してください。



(注)

Cisco WAFS 3.0 ソフトウェアは、FE-511 File Engine と、WAE-611 および WAE-7326 Wide Area Application Engine で動作します。簡潔にするため、説明文の中や使用例のコマンド プロンプトの部分では、単に WAE と記述していますが、特に注釈がない限り、3 つのプラットフォームすべてに当てはまります。

この章で取り上げる CLI コマンドの完全な構文と使用方法の詳細については、『*Cisco WAFS 3.0 Command Reference*』を参照してください。

## 管理ログインの認証および許可について

管理ログインの認証および許可は、WAE への管理者のアクセス権を制御するために使用されます。管理者が、事前に定義された WAFS 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 WAE にログインした場合は、WAE はその管理者に最高レベル (レベル 15) の特権を付与します。これにより、管理者は、そのログイン セッションの間、すべての WAE 管理タスクを実行できます。

たとえば、管理者は、次の管理タスクを実行できます。

- WAE の設定
- WAE が収集した統計情報の取得
- WAE のリロード

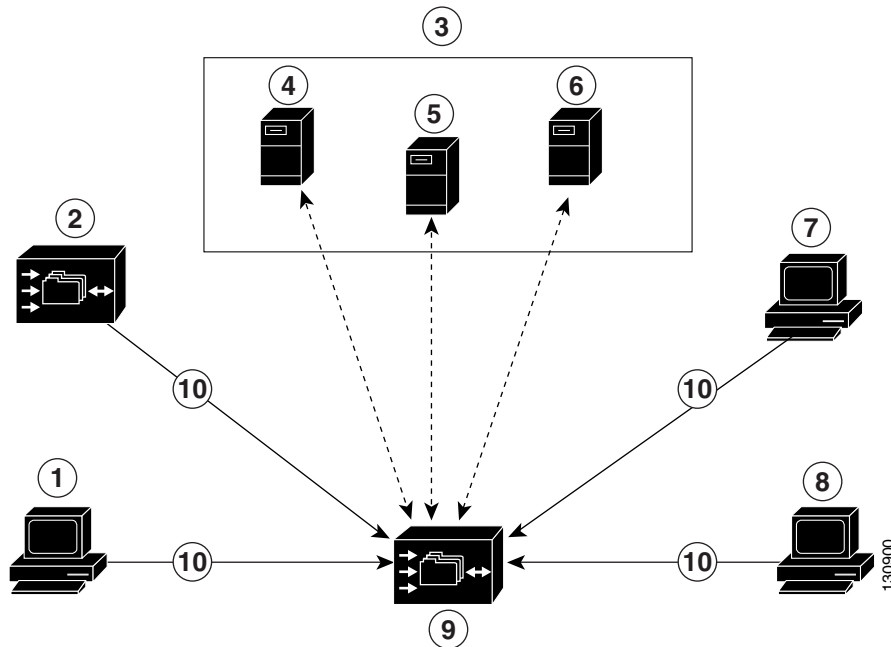


(注)

管理ログイン アカウントの管理方法の詳細については、[3-5 ページの「管理ログイン アカウントの管理」](#)を参照してください。

図 7-1 は、管理者が、コンソール ポートまたは WAFS Manager GUI を介して WAE にどのようにログインできるかを示しています。これらの管理ログイン要求を処理するために、WAE 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、現在のログイン セッションの間にこの特定の管理者に付与するアクセス権を決定します。WAE は、管理ログイン要求を受信した場合、ローカル データベースまたはリモート サードパーティ データベース (TACACS+、RADIUS、または Windows ドメイン データベース) をチェックし、ユーザ名とパスワードを確認し、管理者のアクセス特権を決定できます。

図 7-1 認証データベースと File Engine または WAE



1	FTP/SFTP クライアント	6	Windows ドメイン サーバ
2	WAFS Central Manager または FE Manager GUI	7	コンソールまたは Telnet クライアント
3	サードパーティ AAA サーバ	8	SSH クライアント
4	RADIUS サーバ	9	ローカル データベースおよびデフォルトのプライマリ認証データベースを含む File Engine または WAE
5	TACACS+ サーバ	10	管理ログイン要求

WAE への管理ログイン アクセスを制御するために、ローカル、RADIUS、TACACS+、Windows ドメインといった認証および許可方式を任意に組み合わせて設定できます。デフォルトでは、WAE は、プライマリ方式として、ローカル ログイン認証方式を使用し、管理ログイン要求を処理します。ローカル認証とともに、その他の複数の認証方式もイネーブルになっており、プライオリティフラグ（プライマリ、セカンダリ、またはターシャリ）が設定されていない場合は、常に、ローカル認証は最初に試されます。コンソール接続と Telnet 接続には異なるログイン認証方式を指定することはできません。

WAFS 認証および許可方式の詳細については、次の項を参照してください。

- 7-4 ページの「管理ログインの認証および許可のデフォルト設定」
- 7-4 ページの「管理ログイン認証のフェールオーバーについて」
- 7-6 ページの「ローカル データベースを使用したログイン認証および許可について」
- 7-6 ページの「RADIUS 認証および許可について」
- 7-6 ページの「TACACS+ 認証および許可について」
- 7-8 ページの「Windows ドメイン認証について」



(注) WAE での管理ログインの認証および許可を設定する方法の詳細については、7-9 ページの「管理ログインの認証および許可の設定」を参照してください。

## 管理ログインの認証および許可のデフォルト設定

デフォルトでは、WAE はローカル データベースを使用して、管理ユーザのログイン認証および許可特権を取得します。



(注) **authentication** グローバル コンフィギュレーション コマンドは、WAE への管理ログインとコンフィギュレーション アクセスを制御する認証方式を設定します。

表 7-1 は、管理ログインの認証および許可のデフォルト設定を示しています。

表 7-1 管理ログインの認証および許可のデフォルト設定

機能	デフォルト値
管理ログインの認証	Enabled
管理設定の許可	Enabled
認証サーバが到達不能な場合の認証サーバのフェールオーバー	Disabled
TACACS+ ログイン認証 (コンソールおよび Telnet)	Disabled
TACACS+ 許可 (コンソールおよび Telnet)	Disabled
TACACS+ キー	指定なし
TACACS+ サーバのタイムアウト	5 秒
TACACS+ 再送信の試行回数	2 回
RADIUS ログイン認証 (コンソールおよび Telnet)	Disabled
RADIUS 許可 (コンソールおよび Telnet)	Disabled
RADIUS サーバの IP アドレス	指定なし
RADIUS サーバの UDP 許可ポート	ポート 1645
RADIUS キー	指定なし
RADIUS サーバのタイムアウト	5 秒
RADIUS 再送信の試行回数	2 回
Windows ドメイン ログイン認証	Disabled
Windows ドメイン許可	Disabled

7-9 ページの「管理ログインの認証および許可の設定」で説明するように、これらのデフォルト値は、WAFS CLI を使用して変更できます。

## 管理ログイン認証のフェールオーバーについて

デフォルトでは、WAE は、プライマリ方式の管理ログイン認証が失敗した場合に、セカンダリ方式の管理ログイン認証にフェールオーバーします。デフォルトのログイン認証フェールオーバー方式は、**authentication fail-over server-unreachable** グローバル コンフィギュレーション CLI コマンドを使用して変更できます。

次の例では、認証サーバが到達不能な場合にだけ、管理ログイン認証のフェールオーバーを実行するように設定しています。この場合、WAE は、管理ログイン認証サーバが到達不能なときの、次の認証方式を照会するだけです。

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



(注) ログイン認証フェールオーバー機能を使用するには、TACACS+、RADIUS、または Windows ドメインをプライマリ認証方式として、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。

到達不能なサーバに起因するフェールオーバー オプションが **イネーブル**の場合は、次のガイドラインにしたがってください。

- WAE に設定できるログイン認証方式は2つ（プライマリおよびセカンダリ方式）だけです。
- WAE は、指定した認証サーバが到達不能な場合にだけ、プライマリ認証方式からセカンダリ認証方式へフェールオーバーします。

たとえば、到達不能なサーバに起因するフェールオーバー オプションがイネーブルで、RADIUS がプライマリ ログイン認証方式、ローカルがセカンダリ ログイン認証方式として設定されている場合は、次のように処理されます。

1. WAE は、管理ログイン要求を受信すると、RADIUS 認証サーバを照合します。
2. 次のどちらかが実行されます。
  - a. RADIUS サーバが到達可能な場合、WAE はこの RADIUS データベースを使用して管理者を認証します。
  - b. RADIUS サーバが到達不能な場合、WAE はセカンダリ認証方式を使用して（つまり、ローカル認証データベースを照合して）、管理者の認証を試みます。



(注) 認証のためにローカル データベースとやり取りするのは、RADIUS サーバが到達不能な場合だけです。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は）、認証のためにローカル データベースとやり取りすることはありません。

逆に、到達不能なサーバに起因するフェールオーバー オプションが **ディセーブル**の場合は、WAE は、プライマリ認証データベースで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とやり取りします。

すべての認証データベースの使用がイネーブルになっている場合は、フェールオーバーの理由に基づき、選択されたプライオリティの順番で、すべてのデータベースが照合されます。フェールオーバーの理由が指定されていない場合は、すべてのデータベースがプライオリティ順に照合されます。たとえば、最初にプライマリ認証データベースが照合され、次にセカンダリ認証データベースが照合され、最後にターシャリ データベースが照合されます。

ローカル データベースとリモート データベース (TACACS+、RADIUS、および Windows ドメイン) は、WAFS CLI を使用してイネーブルまたはディセーブルにすることができます。WAE は、すべてのデータベースがディセーブルであるかどうかを確認し、そうである場合は、システムをデフォルトの状態（認証のためローカル データベースが照合される）に設定します。このデフォルトの状態の詳細については、7-4 ページの「[管理ログインの認証および許可のデフォルト設定](#)」を参照してください。

## ローカル データベースを使用したログイン認証および許可について

ローカル認証および許可は、ローカルで設定されたログインとパスワードを使用して、管理ログインの試行を認証します。ログインとパスワードは、各 WAE にとってローカルであり、個々のユーザ名にはマッピングされません。

デフォルトでは、最初にローカル ログイン認証がイネーブルになります。ローカル ログイン認証をディセーブルにできるのは、その他の複数の管理ログイン認証方式をイネーブルにした後だけです。ただし、ローカル ログイン認証をディセーブルにすると、その他のすべての管理ログイン認証方式がディセーブルになった場合に、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 認証および許可について

RADIUS は、network access server (NAS; ネットワーク アクセス サーバ)が、ネットワーク デバイスに接続しようとしているユーザを認証するために使用するクライアント / サーバ認証および許可 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 台以上の RADIUS サーバへ渡します。NAS は、1 台以上の RADIUS サーバから受信した応答に基づいて、ユーザにネットワーク アクセスを許可または拒否します。RADIUS は、RADIUS クライアントとサーバ間の転送に、User Datagram Protocol (UDP; ユーザ データグラム プロトコル)を使用します。

クライアントとサーバには、RADIUS キーを設定できます。クライアントにキーを設定する場合は、RADIUS サーバに設定されているキーと同じキーを設定する必要があります。RADIUS クライアントとサーバは、キーを使用して、送信されたすべての RADIUS パケットを暗号化します。RADIUS キーを設定しないと、パケットは暗号化されません。キー自体が、ネットワーク経由で送信されることは決してありません。



(注) RADIUS プロトコルの動作方法の詳細については、RFC 2138、『Remote Authentication Dial In User Service (RADIUS)』を参照してください。

RADIUS 認証は、通常、管理者が、モニタリング、コンフィギュレーション、またはトラブルシューティングを目的として WAE を設定するために最初にログインしたときに実行されます。詳細については、7-17 ページの「RADIUS を使用した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」を参照してください。

RADIUS 認証は、デフォルトでは、ディセーブルになっています。RADIUS 認証とその他の認証方式は同時にイネーブルにすることができます。また、最初の使用する方式を指定することもできます。RADIUS 認証の設定方法の詳細については、7-10 ページの「RADIUS サーバ認証の設定値の指定」を参照してください。

## TACACS+ 認証および許可について

TACACS+ は、ネットワーク デバイスと中央集中型データベースとの間で network access server (NAS; ネットワーク アクセス サーバ)情報を交換し、ユーザまたはエンティティの ID を判断することで、ネットワーク デバイスへのアクセスを制御します。TACACS+ は、TACACS の拡張版であり、RFC 1492 で規定されている UDP ベースのアクセス コントロール プロトコルです。TACACS+ は、TCP を使用して、TACACS+ サーバとネットワーク デバイス上の TACACS+ デモンとの間のすべてのトラフィックの信頼できる配信と暗号化を保証します。

TACACS+ は、固定パスワード、ワンタイムパスワード、チャレンジ - レスポンス認証などの多数のタイプの認証と連携して動作します。TACACS+ 認証は、通常、管理者が、モニタリング、コンフィギュレーション、またはトラブルシューティングを目的として WAE を設定するために最初にログインしたときに実行されます。7-18 ページの「TACACS+ を使用した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」を参照してください。

ユーザが限定されたサービスを要求した場合、TACACS+ は MD5 暗号化アルゴリズムを使用してユーザパスワード情報を暗号化し、TACACS+ パケットヘッダーに追加します。このヘッダー情報は、送信されたパケットのタイプ（たとえば、認証パケット）、パケットのシーケンス番号、使用されている暗号化タイプ、パケット長の合計を示しています。その後、TACACS+ プロトコルはパケットを TACACS+ サーバへ転送します。

TACACS+ サーバは、Authentication, Authorization, and Accounting (AAA; 認証、許可、アカウントリング) 機能を提供できます。このサービスは、すべて TACACS+ の一部ですが、互いに独立しているため、特定の TACACS+ コンフィギュレーションでは、3 つのサービスすべてを使用することもできれば、その中のいずれかを使用することもできます。

TACACS+ サーバは、パケットを受信すると、次のように処理します。

- ユーザ情報を認証し、ログイン認証が成功したか失敗したかどうかを、クライアントに通知します。
- 認証を続行することと、クライアントが追加情報を提供する必要があることを、クライアントに通知します。このチャレンジ - レスポンス プロセスは、ログイン認証が成功するか失敗するまで、何度も繰り返し実行できます。

クライアントとサーバには、TACACS+ キーを設定できます。WAE にキーを設定する場合は、TACACS+ サーバに設定されているキーと同じキーを設定する必要があります。TACACS+ クライアントとサーバは、キーを使用して、送信されたすべての TACACS+ パケットを暗号化します。TACACS+ キーを設定しないと、パケットは暗号化されません。

TACACS+ 認証は、デフォルトでは、ディセーブルになっています。TACACS+ 認証とローカル認証は同時にイネーブルにすることができます。

## TACACS+ イネーブルパスワードの属性

システム動作を設定、表示、およびテストするには、WAFS ソフトウェアの CLI EXEC モードを使用します。ユーザと特権の 2 つのアクセスモードに分かれています。特権レベルの 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 コマンドを入力し、パスワードの入力が求められたら特権 EXEC パスワード（スーパーユーザまたは管理者相当のパスワード）を指定します。

TACACS+ には、管理者が、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定義できる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、管理者（admin）または管理者相当のユーザアカウント（特権レベル 15）ではなく、通常レベルのユーザアカウント（特権レベル 0）で WAE にログインした場合、そのユーザは、特権レベル EXEC モードにアクセスするために admin パスワードを入力する必要があります。

```
WAE> enable
Password:
```

この手順は、これらの WAFS ユーザがログイン認証に TACACS+ を使用している場合にも当てはまります。

## Windows ドメイン認証について

WAFS は、ネットワーク ログインに関して、次の Windows ドメイン チャレンジ/レスポンス認証方式をサポートしています。

- NT LAN Manager (NTLM)バージョン 1 Active Directory を使用する Windows 98、Windows NT などのレガシー システム、および Windows 2000、Windows XP、Windows 2003 などの最近の Windows システムを含む、すべての Windows システムで使用されます。

WAFS プリント サービスに対応した Edge FE にアクセスする各種クライアントとの互換性を最大限引き出すために、NTLM バージョン 1 を使用することをお勧めします。それが使用できないか、許されない (バージョン 1 は安全性が低い) 場合は、NTLM バージョン 2 を使用してください。

- NTLM バージョン 2 Active Directory を使用する Windows 98、Windows NT 4.0 (サービス パック 4 以上)、Windows XP、Windows 2000、Windows 2003 といった Windows システムで使用されます。

## 管理ログインの認証および許可の設定

ここでは、モニタリング、設定、またはトラブルシューティングを目的に File Engine または WAE にログインする必要がある WAFS 管理者のログイン認証および許可を設定する方法について説明します。ここで説明する内容は、次のとおりです。

- [基本的な設定手順、7-9 ページ](#)
- [RADIUS サーバ認証の設定値の指定、7-10 ページ](#)
- [TACACS+ サーバ認証の設定値の指定、7-11 ページ](#)
- [Windows ドメイン サーバ認証の設定値の指定、7-14 ページ](#)
- [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、7-15 ページ](#)

### 基本的な設定手順

WAE の管理ログインの認証および許可を設定する一般的な手順は、次のとおりです。

**ステップ 1** 管理ログイン要求の認証時に WAE に使用させるログイン認証方式として、どの方式を設定するかを決定します（たとえば、ローカル データベースをプライマリ ログイン データベースとして、RADIUS サーバをセカンダリ認証データベースとして使用します）。

**ステップ 2** WAE のログイン認証サーバの設定値を設定します（リモート認証データベースを使用する場合）。

たとえば、WAE がログイン要求を認証するために使用する、リモート RADIUS サーバ、TACACS+ サーバ、または Windows ドメイン サーバの IP アドレスを指定します。次の項を参照してください。

- [RADIUS サーバ認証の設定値の指定、7-10 ページ](#)
- [TACACS+ サーバ認証の設定値の指定、7-11 ページ](#)
- [Windows ドメイン サーバ認証の設定値の指定、7-14 ページ](#)

**ステップ 3** WAE が管理ログイン要求を処理するために使用する、ログイン認証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のフェールオーバー方式を指定します（オプション）。

たとえば、WAE が管理ログイン要求を処理するとき、どの認証データベースをチェックする必要があるかを指定します。[7-15 ページの「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」](#)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前に、RADIUS、TACACS+、または Windows ドメイン認証が設定され、正常に動作していることを確認します。ローカル認証がディセーブルで、RADIUS、TACACS+、または Windows ドメイン設定値が正しく設定されていない場合、もしくは RADIUS、TACACS+、または Windows ドメイン サーバがオンラインでない場合は、WAE 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の場合に、その他のすべての認証方式がディセーブルになると、ローカル認証は自動的に再度イネーブルになります。


## RADIUS サーバ認証の設定値の指定

RADIUS 認証クライアントは、WAFS 3.x ソフトウェアを稼働する File Engine または WAE に常駐します。イネーブルの場合、これらのクライアントは認証要求を中央（リモート）の RADIUS サーバへ送信します。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 アクセス情報が含まれています。

WAE に RADIUS 認証を設定するには、一連の RADIUS 認証サーバの設定値を WAE に設定する必要があります。この RADIUS 認証サーバの一連の設定値は、CLI を使用して WAE に設定できます。

表 7-2 は、RADIUS 認証の設定値とその説明をまとめたものです。

表 7-2 WAE の RADIUS 認証の設定値

設定値	説明
RADIUS サーバ	WAE が RADIUS 認証に使用する RADIUS サーバ。WAE の特定の RADIUS サーバの使用をイネーブルにするには、RADIUS サーバの IP アドレスまたはホスト名と、ポート情報を入力します。最大 5 台の異なるホストを設定できます。RADIUS の早期の展開ではポート番号 1645 が使用されていましたが、現在の RADIUS の正式なポート番号は 1812 です。最大 5 個の異なるポートを設定できます。
RADIUS キー	RADIUS クライアント（WAE）と RADIUS サーバとの間で、すべての通信の暗号化と認証に使用されるキー。キーの最大文字数は 15 です。デフォルト値はありません。 
RADIUS タイムアウト インターバル	WAE が、タイムアウトを宣言する前に、指定された RADIUS 認証サーバからの応答を待機する秒数。指定できる範囲は、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 インターバルを過ぎた場合に、WAE がその接続を RADIUS サーバへ再送信する回数。指定できる範囲は、1 ~ 3 回です。デフォルト値は 2 回です。



ヒント 必ず、RADIUS サーバ上でも同じ RADIUS キーをイネーブルにしてください。

CLI を使用して RADIUS 認証の設定値を WAE に設定する手順は、次のとおりです。

- ステップ 1** 1 台以上の RADIUS サーバを指定します。オプションで、サーバ上で使用する宛先 UDP ポートを指定します。デフォルト値は 1645 です。

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

この例は、192.168.52.3 にある RADIUS サーバを指定する方法を示しています。

```
WAE(config)# radius-server 192.168.52.3
```

- ステップ 2** WAE に RADIUS キーを指定します。

```
WAE(config)# radius-server key myradiuskey
```

ステップ 3 RADIUS タイムアウト インターバルを指定します。たとえば、RADIUS サーバからの応答を受信しなかった場合に、10 秒間待機してからタイムアウトを宣言するように WAE を設定します。

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

ステップ 4 RADIUS 再送信回数を指定します。たとえば、RADIUS タイムアウトが起こった場合に、RADIUS サーバへ 3 回再送信するように WAE を設定します。

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



(注) RADIUS 認証の設定値（たとえば、RADIUS キー）の詳細については、表 7-2 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 WAFS 3.0 Command Reference を参照してください。

---

これで、7-17 ページの「RADIUS を使用した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」で説明したとおり、RADIUS をこの WAE の管理ログイン認証および許可方式としてイネーブルにすることができました。

## TACACS+ サーバ認証の設定値の指定


TACACS+ 認証を File Engine または WAE に設定するには、一連の TACACS+ 認証の設定値を設定する必要があります。この TACACS+ 認証の一連の設定値は、CLI を使用して WAE に設定できます。

表 7-3 は、TACACS+ 認証の設定値とその説明をまとめたものです。



(注) TACACS+ 認証は、TACACS+ サーバが WAE に設定されていないかぎり、実行されません。

表 7-3 WAE の TACACS+ 認証設定値

設定値	説明
TACACS+ サーバ	WAE が TACACS+ 認証に使用する TACACS+ サーバ。プライマリ TACACS+ サーバは明示的に指定します。そうしないと、WAE が自分で決定してしまいます。1 台のプライマリ TACACS+ サーバと 2 台のバックアップ TACACS+ サーバを設定できます。TACACS+ は、指定されたサービスに基づき、通信用に標準ポート(ポート 49)を使用します。
TACACS+ キー	WAE が TACACS+ サーバとの通信に使用する秘密鍵。TACACS+ キーの最大文字数は、出力可能な ASCII 文字で 99 文字までです(タブを除く)。デフォルトは、空のキー ストリングです。先行するスペースは、すべて無視されます。キー ストリング内のスペースと、キーの終わりのスペースは無視されません。キー内にスペースがある場合でも、引用符がキーの一部でないかぎり、二重引用符は必要ありません。デフォルト値はありません。 
	ヒント 必ず、TACACS+ サーバにも同じ TACACS+ キーを指定してください。
TACACS+ タイムアウト インターバル	WAE が、タイムアウトを宣言する前に、指定された TACACS+ 認証サーバからの応答を待機する秒数。指定できる範囲は、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 インターバルを過ぎた場合に、WAE がその接続を TACACS+ サーバへ再送信する回数。指定できる範囲は、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	パスワード認証のメカニズム。デフォルトでは、Password Authentication Protocol (PAP; パスワード認証プロトコル) がパスワード認証用のメカニズムです。その他のオプションとして、ASCII クリア テキストをパスワード認証メカニズムとして使用することができます。

CLI を使用して TACACS+ 認証の設定値を WAE に設定する手順は、次のとおりです。

ステップ 1 1 台以上の TACACS+ サーバを指定します。

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

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

```
WAE(config)# tacacs server 192.168.50.1 primary
```

次の例は、特定の TACACS+ サーバをバックアップサーバとして指定する方法を示しています。この場合、**primary** オプションを指定せずにコマンドを実行します。

```
WAE(config)# tacacs server 192.168.50.2
```

ステップ 2 TACACS+ キーを指定します。

```
WAE(config)# tacacs key key
```

ステップ 3 TACACS+ タイムアウト インターバルを指定します。たとえば、TACACS+ サーバからの応答を受信しなかった場合に、15 秒間待機してからタイムアウトを宣言するように WAE を設定します。

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

ステップ 4 TACACS+ 再送信回数を指定します。たとえば、TACACS+ タイムアウトが起こった場合に、TACACS+ サーバへ 1 回だけ再送信するように WAE を設定します。

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

ステップ 5 TACACS+ パスワード認証のメカニズムを指定します。たとえば、ASCII クリア テキストをメカニズムとして使用するには、ASCII キーワードを入力します。

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



(注) TACACS+ 認証の設定値（たとえば、TACACS+ キーの指定方法）の詳細については、表 7-3 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 WAFS 3.0 Command Reference』を参照してください。

次の例では、ホスト名が spearhead の TACACS+ サーバをプライマリ TACACS+ サーバとして設定しています。WAE は、TACACS+ サーバ（サーバ名 spearhead）で使用されるキーと同じキー（human789）を使用するように設定され、さらに、デフォルトのタイムアウト インターバル、再送信回数、パスワード タイプは変更されています。また、この例は、show tacacs EXEC コマンドを使用して、WAE 上の現在の TACACS+ 設定を表示する方法も示しています。

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

```
WAE# 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      = 10
```

```
Retransmit   = 5
```

```
Password type: ascii
```

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

これで、7-18 ページの「TACACS+ を使用した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」で説明したとおり、TACACS+ をこの WAE の管理ログイン認証および許可方式としてイネーブルにすることができました。

## Windows ドメイン サーバ認証の設定値の指定

Windows ドメイン認証を File Engine または WAE に設定するには、一連の Windows ドメイン認証の設定値を設定する必要があります(表 7-4 を参照)。この一連の認証設定値は、CLI を使用して WAE に設定できます。



(注) Windows ドメイン認証は、WAE に Windows ドメイン サーバが設定されていないかぎり、実行されません。

表 7-4 WAE の Windows ドメイン サーバ認証の設定値

設定値	説明
NetBIOS 名	WAE の NetBIOS 名。WAE が認証サービスに対する自身のアベイラビリティを通知するときに提供される名前。
パスワード サーバ	クライアント パスワードの検証に使用されるパスワード サーバのホスト名または IP アドレス。
WINS サーバ	Windows Internet Naming Service (WINS) サーバのホスト名または IP アドレス。
ワークグループ	WAE が常駐するワークグループ (または、ドメイン) の名前。

CLI を使用して Windows ドメイン認証の設定値を WAE に設定する手順は、次のとおりです。

**ステップ 1** `windows-domain` グローバル コンフィギュレーション コマンドを使用して、WINS サーバを指定します。次の例では、IP アドレス 10.10.24.1 にある Windows ドメイン サーバを指定しています。

```
WAE(config)# windows-domain wins-server 10.10.24.1
```

**ステップ 2** パスワード サーバを指定します。次の例では、IP アドレス 10.10.100.4 にあるパスワード サーバを指定しています。

```
WAE(config)# windows-domain password-server 10.10.100.4
```

**ステップ 3** WAE の NetBIOS 名を指定します。次の例では、`myFileEngine` を使用しています。

```
WAE(config)# windows-domain netbios-name myFileEngine
```

**ステップ 4** WAE が常駐するドメインを指定します。次の例では、`cisco` ドメインを使用しています。

```
WAE(config)# windows-domain workgroup cisco
```

これで、7-18 ページの「TACACS+ を使用した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」で説明したとおり、Windows ドメインをこの WAE の管理ログイン認証および許可方式としてイネーブルにすることができました。

## 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、さまざまな管理ログイン認証および許可方式（認証設定）を WAE に定義したり、それを変更したりする方法について説明します。ここで説明する内容は、次のとおりです。

- 使用上のガイドライン
- ローカル データベースを使用した管理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
- RADIUS を使用した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+ を使用した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
- Windows ドメイン サーバを使用した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



### 注意

ローカル認証および許可をディセーブルにする前に、RADIUS、TACACS+、または Windows ドメイン認証が設定され、正常に動作していることを確認します。ローカル認証がディセーブルで、RADIUS、TACACS+、または Windows ドメイン認証が正しく設定されていない場合、もしくは RADIUS、TACACS+、または Windows ドメイン サーバがオンラインでない場合は、WAE にログインできないことがあります。

## 使用上のガイドライン

WAE の認証設定方式を定義または変更する際は、次のガイドラインにしたがってください。

- CLI を使用して、ユーザ アクセス管理に、外部アクセスサーバを使用するか、または内部（ローカル）WAE ベースの AAA システムを使用するかを選択できます。
- WAE 上でアクセスを制御し特権を設定するために、次の認証および許可方式を任意に組み合わせて設定できます。
  - 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
  - Windows ドメイン認証
- **authentication** グローバル コンフィギュレーション コマンドは、管理ログイン認証および許可（設定）オプションを設定します。

```
authentication {configuration {local | radius | tacacs} enable [primary | secondary | tertiary] |  
fail-over server-unreachable | login {local | radius | tacacs | windows-domain} enable [primary  
| secondary | tertiary] | print-services windows-domain enable}
```

- **authentication** グローバル コンフィギュレーション コマンドは、WAE への管理ログインとコンフィギュレーション アクセスの両方を設定します。
- **authentication login local** および **authentication configuration local** グローバル コンフィギュレーション コマンドは、認証および許可のためにローカル データベースを使用します。
  - **authentication login** コマンドは、管理者が WAE に対してどのレベルのアクセス権を持っているかを判断するために使用する管理ログイン認証方式を指定します。
  - **authentication configuration** コマンドは、認証された管理者の特権（WAE に対するユーザ アクセス レベル）を決定します。
- **authentication login radius** および **authentication configuration radius** グローバル コンフィギュレーション コマンドは、リモート RADIUS サーバを使用して、管理アクセス レベルを決定します。

- **authentication login tacacs** および **authentication configuration tacacs** グローバル コンフィギュレーション コマンドは、リモート TACACS+ サーバを使用して、管理アクセス レベルを決定します。
- **authentication login windows-domain** グローバル コンフィギュレーション コマンドは、リモート Windows ドメイン サーバを使用して、管理アクセス レベルを決定します。
- デフォルトでは、ローカル方式がイネーブルになっており、TACACS+、RADIUS、Windows ドメインはすべて、管理ログインおよび設定に対してはディセーブルになっています。TACACS+、RADIUS、および Window ドメイン方式がディセーブルのときは常に、ローカル方式が自動的にイネーブルになります。TACACS+、RADIUS、Windows ドメイン、およびローカル方式は、同時にイネーブルにすることができます。
  - **primary** オプションは、管理ログインと設定の両方に対して、最初に試行される方式を指定します。
  - **secondary** オプションは、プライマリ方式が失敗した場合に使用する方式を指定します。
  - **tertiary** オプションは、プライマリ方式とセカンダリ方式が失敗した場合に使用する方式を指定します。

**authentication login** または **authentication configuration** コマンドで、すべての方式がプライマリとして設定された場合、またはすべての方式がセカンダリもしくはターシャリとして設定された場合は、最初にローカル方式が試行され、次に RADIUS、TACACS+、Windows ドメインの順で試行されます。

次の例では、ローカル、TACACS+、および RADIUS の認証と許可をイネーブルにし、TACACS+ を最初に使用する方式として、ローカルを TACACS+ 方式が失敗した場合のセカンダリ方式として、さらに RADIUS をローカルと TACACS+ の両方が失敗した場合のターシャリ方式として設定しています。

```
WAE(config)# authentication login tacacs enable primary
WAE(config)# authentication login local enable secondary
WAE(config)# authentication login radius enable tertiary
WAE(config)# authentication configuration tacacs enable primary
WAE(config)# authentication configuration local enable secondary
WAE(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+ サーバは、TACACS+ 認証および許可方式を使用するように設定する必要があります。TACACS+ サーバの設定方法の詳細については、7-11 ページの「[TACACS+ サーバ認証の設定値の指定](#)」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 サーバは、RADIUS 認証および許可方式を使用するように設定する必要があります。RADIUS サーバの設定方法の詳細については、7-10 ページの「[RADIUS サーバ認証の設定値の指定](#)」を参照してください。

- 認証の設定は、次のものに適用されます。
  - コンソールおよび Telnet の接続試行
  - Secure FTP (SFTP; セキュア FTP) および SSH (SSH バージョン 1 およびバージョン 2)
  - プリントサーバアクセス
- RADIUS または TACACS+ キーを WAE (RADIUS および TACACS+ クライアント) に設定する場合は、必ず、RADIUS または TACACS+ サーバにも同一のキーを設定してください。
- 複数の RADIUS または TACACS+ サーバを設定する場合、最初に設定したサーバがプライマリサーバとなり、認証要求は最初にこのサーバに送信されます。また、認証および許可を目的とする、セカンダリサーバとターシャリサーバを指定することもできます。**authentication** グローバル コンフィギュレーション コマンドで **primary**、**secondary**、または **tertiary** キーワードを使用して、それぞれの重要度を設定します。

- デフォルトでは、WAE 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、アクセス権を許可します。WAE は、すべての認証データベースがディセーブルであるかどうかを確認し、そうである場合は、システムをデフォルトの状態に設定します。このデフォルトの状態の詳細については、7-4 ページの「管理ログインの認証および許可のデフォルト設定」を参照してください。

## ローカル データベースを使用した管理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、WAE 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アクセス権を許可するように設定されます。この認証および許可方式は、ローカル方式と呼ばれます。WAE 上のこの認証および許可方式は、CLI を使用してディセーブルにしたり、再度イネーブルにしたりすることができます。



注意

ローカル認証および許可をディセーブルにする前に、RADIUS または TACACS+ 認証が設定され、正常に動作していることを確認します。ローカル管理認証がディセーブルで、RADIUS または TACACS+ が正しく設定されていない場合、もしくは RADIUS または TACACS+ サーバがオンラインでない場合は、WAE にログインできないことがあります。

WAE 上のローカル方式がディセーブルで、それを再度イネーブルにする手順は、次のとおりです。

ステップ 1 ローカル ログイン認証を再度イネーブルにします。

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

ステップ 2 管理ユーザのローカル許可（セッション中の特権を制御する）を再度イネーブルにします。

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

管理ユーザには、通常レベル管理アクセス（限定された特権レベル 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 つの特権レベルを付与できます。管理ユーザの特権レベルの詳細については、3-5 ページの「管理ログイン アカウントの管理」を参照してください。



(注)

WAE 上の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には、**no authentication login local enable** コマンドを使用します）。

## RADIUS を使用した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

WAE が RADIUS を使用して管理ログイン要求を認証しアクセス権を許可するように設定されている場合は、次のガイドラインにしたがってください。

- デフォルトでは、WAE 上の RADIUS 認証および許可はディセーブルです。
- WAE 上で RADIUS 認証をイネーブルにする前に、WAE が使用する RADIUS サーバを少なくとも 1 台は指定する必要があります。RADIUS サーバの指定方法の詳細については、7-10 ページの「RADIUS サーバ認証の設定値の指定」を参照してください。

- RADIUS 認証とその他の認証方式は同時にイネーブルにすることができます。 **primary** キーワードを使用して、最初にどの方式を使用するかを指定できます。ローカル認証がディセーブルの場合に、その他のすべての認証方式がディセーブルになると、ローカル認証は自動的に再度イネーブルになります。
  - CLI を使用して、WAE 上の RADIUS 認証および許可をイネーブルにすることができます。
- CLI を使用して WAE 上の RADIUS 認証および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。

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

たとえば、強制的に WAE が最初に RADIUS 認証を試行 (TACACS+ 認証を使用する前に試行) するように指定するには、次のコマンドを入力します。

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

#### ステップ 2 RADIUS 許可をイネーブルにします。

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

たとえば、強制的に WAE が最初に RADIUS 許可を試行 (TACACS+ 許可を使用する前に試行) するように指定するには、次のコマンドを入力します。

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



(注) WAE 上の RADIUS 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、RADIUS 認証をディセーブルにするには、**no authentication login radius enable** コマンドを使用します)。

### TACACS+ を使用した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

WAE が TACACS+ を使用して管理ログイン要求を認証しアクセス権を許可するように設定されている場合は、次のガイドラインにしたがってください。

- デフォルトでは、WAE 上の TACACS+ 認証および許可はディセーブルです。
  - **authentication login tacacs** および **authentication configuration tacacs** コマンドは、管理ログイン認証および許可にリモート TACACS+ サーバを使用して、管理アクセス レベルを決定します。
  - WAE 上で TACACS+ 認証をイネーブルにする前に、WAE が使用する TACACS+ サーバを少なくとも 1 台は指定する必要があります。TACACS+ サーバの指定方法の詳細については、[7-11 ページの「TACACS+ サーバ認証の設定値の指定」](#)を参照してください。
  - RADIUS と TACACS+ の両方を指定する場合は、**primary** キーワードを使用して、WAE が最初に TACACS+ 認証を試行するように強制的に指定できます。
  - CLI を使用して、WAE 上の TACACS+ 認証および許可をイネーブルにすることができます。
- CLI を使用して WAE 上の TACACS+ 認証および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。

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

たとえば、強制的に WAE が最初に TACACS+ 認証を試行 (RADIUS 認証を使用する前に試行) するように指定するには、次のコマンドを入力します。

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

ステップ 2 TACACS+ 許可をイネーブルにします。

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

たとえば、強制的に WAE が最初に TACACS+ 許可を試行 (RADIUS 許可を使用する前に試行) するように指定するには、次のコマンドを入力します。

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



(注)

WAE 上の TACACS+ 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、TACACS+ 認証をディセーブルにするには、**no authentication login tacacs enable** 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)。

## Windows ドメイン サーバを使用した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

WAE が Windows ドメイン サーバを使用して管理ログイン要求を認証しアクセス権を許可するように設定されている場合は、次のガイドラインにしたがってください。

- デフォルトでは、WAE 上の Windows ドメイン認証はディセーブルです。
- **authentication login windows-domain** コマンドは、管理ログイン認証にリモート Windows ドメイン サーバを使用します。ログイン認証は、ローカル、RADIUS、または TACACS+ データベースを使用して処理されます。
- WAE 上で Windows ドメイン認証をイネーブルにする前に、WAE が使用する Windows ドメイン サーバを少なくとも 1 台は指定する必要があります。Windows ドメイン サーバの指定方法の詳細については、7-14 ページの「[Windows ドメイン サーバ認証の設定値の指定](#)」を参照してください。
- RADIUS と TACACS+ の両方を指定する場合は、**primary** キーワードを使用して、WAE が最初に TACACS+ 認証を試行するように強制的に指定できます。
- CLI を使用して、WAE 上の Windows ドメイン ログイン認証および許可をイネーブルにすることができます。

CLI を使用して WAE 上の Windows ドメイン ログイン認証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 Windows ドメイン認証をイネーブルにします。

```
WAE(config)# authentication login windows-domain enable [primary] [secondary]
[tertiary]
```

たとえば、強制的に WAE が最初に Windows ドメイン認証を試行（別の認証方式を使用する前に試行）するように指定するには、次のコマンドを入力します。

```
WAE(config)# authentication login windows-domain enable primary
```

ステップ 2 オプションで、セカンダリまたはターシャリ認証サーバ（ローカル、RADIUS、または TACACS+）を設定します。次の例では、ローカル データベースを、Windows ドメイン認証が失敗した場合のセカンダリ認証として使用しています。順番を指定するかどうかに関わらず、ユーザを認証するために、設定されているすべての認証タイプが試行されます。

```
WAE(config)# authentication login local enable secondary
```

ステップ 3 許可をイネーブルにします。次の例では、ローカル データベースが使用されています。

```
WAE(config)# authentication configuration local enable primary
```



(注) WAE 上の Windows ドメイン認証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、**no authentication login windows-domain enable** と入力します）。

Windows ドメイン サーバが到達不能だったために Windows 認証に失敗した場合の唯一の認証オプションとしてローカル データベースを設定する手順は、次のとおりです。

ステップ 1 Windows ドメイン認証をイネーブルにします。

```
WAE(config)# authentication login windows-domain enable primary
```

ステップ 2 ローカル データベースを使用した許可をイネーブルにします。

```
WAE(config)# authentication configuration local enable primary
```

ステップ 3 到達不能なサーバに起因するフェールオーバーをイネーブルにします。

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

## 認証および許可情報の表示

WAE 上の認証および許可について現在の設定と統計情報を表示できます。

### 現在の管理認証および許可の設定の表示

WAE 上の現在の管理ログイン認証および許可（認証設定）を表示するには、**show authentication user EXEC** コマンドを使用します。出力例は、管理ログイン要求の認証と許可に使用するように WAE に設定されている認証方式（たとえば、ローカル、RADIUS、または TACACS+）を示しています。

```
WAE# show authentication user

Login Authentication:      Console/Telnet/Ftp/SSH Session
-----
local                     enabled (primary)
Windows domain           enabled (primary)
Radius                   disabled
Tacacs+                  disabled

Configuration Authentication: Console/Telnet/Ftp/SSH Session
-----
local                     enabled (primary)
Radius                   disabled
Tacacs+                  disabled
```

### 認証および許可の統計情報の表示

RADIUS、TACACS+、または Windows ドメイン サーバを使用して、認証および許可要求の数と、これらの要求の中で成功した数と失敗した数を追跡できます。各方式に対して **show statistics EXEC** コマンドを実行すると、履歴を表示できます。

次の例は、Windows ドメイン方式の場合の出力を示しています。

```
WAE# show statistics windows-domain
Windows Domain Statistics
-----
Authentication:
  Number of access requests:          12
  Number of access deny responses:    3
  Number of access allow responses:   9

Authorization:
  Number of authorization requests:    0
  Number of authorization failure responses: 0
  Number of authorization success responses: 0

Accounting:
  Number of accounting requests:       0
  Number of accounting failure responses: 0
  Number of accounting success responses: 0
```

