CHAPTER 6

管理ログインの認証、許可、およびアカウンティングの設定

この章では、Wide Area Application Service（WAAS）デバイス用の管理ログインの Authentication, Authorization, and Accounting（AAA; 認証、許可、アカウンティング）を設定する方法について説明します。

この章の構成は、次のとおりです。

WAAS Central Manager GUI を使用して、WAAS デバイス用の 2 種類の管理者ユーザ アカウント（デバイスに基づく CLI アカウントと役割に基づくアカウント）を集中的に作成し、管理します。詳細については、第 7 章「管理者ユーザ アカウントおよびグループの作成と管理」を参照してください。

（注） この章では、ネットワークに存在する WAAS Central Manager と Wide Area Application Engine（WAE）を総称する用語として「WAAS デバイス」を使用します。「WAE」は、WAE アプライアンスおよび WAE ネットワーク モジュール（NME-WAE デバイス ファミリ）を示します。

管理ログインの認証および許可について

WAAS ネットワークでは、管理的ログイン認証と許可を使用して、設定、監視、またはトラブルシューティング用に WAAS デバイスにアクセスしたい管理者からのログイン要求を制御します。

ログイン認証とは、WAAS デバイスが、デバイスにログインしようとしている管理者が有効なユーザ名とパスワード持っているかどうかを確認するプロセスです。ログインしようとする管理者は、デバイスに登録されたユーザ アカウントを持つ必要があります。ユーザ アカウント情報は、ユーザの管理ログインと設定特権を許可する役割を果たします。ユーザ アカウント情報は AAA データベースに保存され、AAA データベースが存在する特定の認証サーバにアクセスするように WAAS デバイスを設定する必要があります。ユーザがデバイスにログインしようとすると、デバイスは、その人物のユーザ名、パスワード、および特権レベルをデータベースに保存されたユーザ アカウント情報と比較します。

WAAS ソフトウェアは、外部アクセス サーバ（たとえば、RADIUS または TACACS+ サーバ）を持つユーザと AAA 機能を持つローカル アクセス データベースが必要なユーザ用の次の AAA サポートを提供します。

- 認証（またはログイン認証）は、ユーザが誰であるかを決定する処理です。ユーザ名とパスワードを検査します。
- 許可（または設定）は、ユーザが許可されていることを決定する処理です。一般に、認証の後で許可が実行されます。ユーザがログインするには、認証と許可の両方が必要です。
- アカウンティングは、システムアカウンティングを目的に管理ユーザのアクティビティを追跡する機能です。WAAS ソフトウェアでは、TACACS+ による AAA アカウンティングがサポートされています。詳細については、「WAAS デバイス用の AAA アカウンティングの設定」（p.6-35）を参照してください。

（注）　管理者は、コンソール ポートまたは WAAS Central Manager GUI を通じて WAAS Central Manager デバイスにログインできます。管理者は、コンソール ポートまたは WAE Device Manager GUI を通じて、Core WAE または Edge WAE として機能する WAAS デバイスにログインできます。

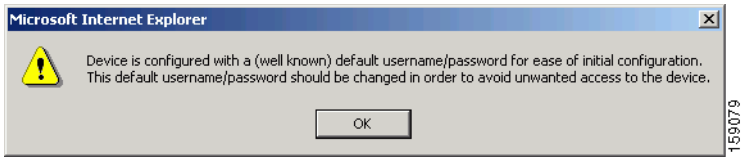
認証と許可が設定される前にシステム管理者が WAAS デバイスにログインするとき、管理者は、定義済みの superuser アカウントを使用して WAAS デバイスにアクセスできます（定義済みのユーザ名は admin、定義済みのパスワードは default です）。この定義済みの superuser アカウントを使用して WAAS デバイスにログインするとき、WAAS システム内のすべての WAAS サービスと要素へのアクセスが許可されます。

（注）　WAAS デバイスごとに、ユーザ名が admin の 1 つの管理者アカウントが必要です。定義済みの superuser アカウントのユーザ名は、変更できません。定義済みの superuser アカウントは、ユーザ名 admin を持つ必要があります。

WAAS デバイスを初期設定したあとで、各 WAAS デバイスで定義済みの superuser アカウント用のパスワードをただちに変更することを強く推奨します（定義済みのユーザ名は admin、パスワードは default、特権レベルは superuser、特権レベル 15 です）。

WAAS Central Manager デバイスでこの superuser アカウント用の定義済みのパスワードが変更されていない場合は、アカウントを使用して WAAS Central Manager GUI にログインするたびに、次のダイアログボックスが表示されます（図 6-1 を参照）。

図 6-1　superuser アカウント用の定義済みのパスワードを変更する必要があることを示すメッセージ



この superuser アカウント用の定義済みのパスワードが変更されていない場合、アカウントを使用して WAAS デバイスの WAAS CLI にログインするたびに、コンソールに次のメッセージも表示されます。

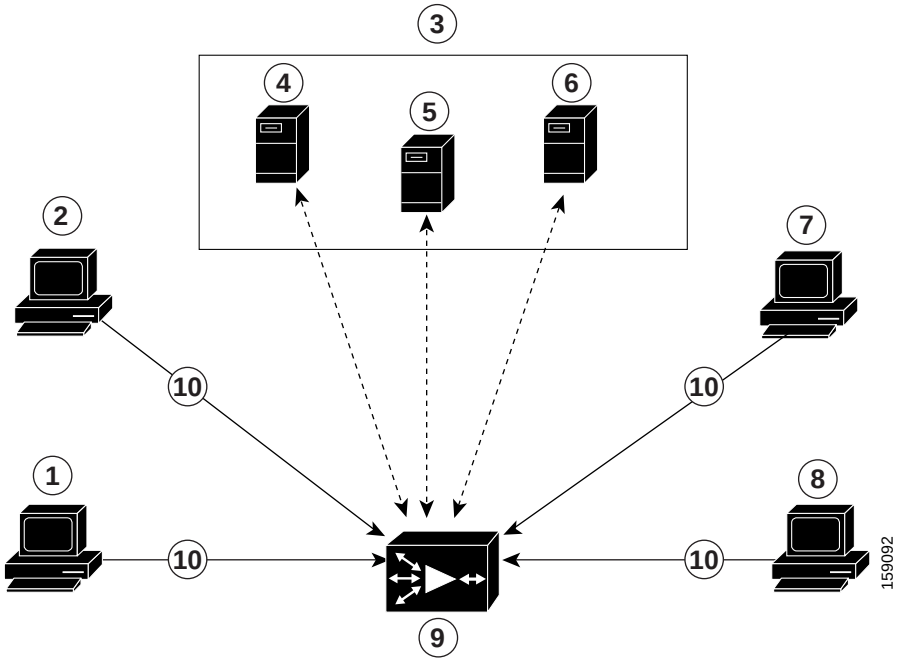
```
Device is configured with a (well known) default username/password
for ease of initial configuration. This default username/password
should be changed in order to avoid unwanted access to the device.

System Initialization Finished.
waas-cm#
```

WAAS Central Manager GUI を使用して定義済みの superuser アカウント用のパスワードを変更する手順については、「自身のアカウントのパスワードの変更」（p.7-8）を参照してください。

図 6-2 に、管理者が、コンソール ポートまたは WAAS GUI（WAAS Central Manager GUI または WAE Device Manager GUI）を通じて WAE にログインする方法を示します。WAAS デバイスが管理ログイン要求を受信すると、WAE は、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 6-2　認証データベースと WAE



1	FTP/SFTP クライアント	6	Windows ドメイン サーバ
2	WAAS Central Manager GUI または WAE Device 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 データベースとデフォルトの一次認証データベースを搭載する WAE
5	TACACS+ サーバ	10	管理ログイン要求

ユーザ アカウント情報は AAA データベースに保存され、AAA データベースが存在する特定の認証サーバにアクセスするように WAAS デバイスを設定する必要があります。WAAS デバイスへのログイン アクセスを制御するために、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
- TACACS+
- Windows ドメイン認証

（注） 外部認証サーバを使用して認証を設定する場合は、第 7 章「管理者ユーザ アカウントおよびグループの作成と管理」の説明に従って WAAS Central Manager でユーザ アカウントを作成する必要があります。ユーザ アカウントをローカル ユーザ アカウントにしないでください。つまり、アカウント作成時に [Local User] チェック ボックスを選択しないでください。

デフォルトの AAA 設定の詳細については、「管理ログインの認証および許可のデフォルト設定」（p.6-5）を参照してください。AAA 設定の詳細については、「管理ログインの認証および許可の設定」（p.6-7）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、WAAS デバイスはローカル 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。

表 6-1 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 6-1　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+ ログイン許可（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 ログイン許可（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 ログイン許可	Disabled
Windows ドメイン パスワード サーバ	指定なし
Windows ドメイン領域（Kerberos 認証を使用するとき、認証に使用される Kerberos 領域） （注）　Kerberos 認証を有効にすると、デフォルトの**領域**は DOMAIN.COM になり、セキュリティは Active Directory サービス（ADS）になります。	空（から）の文字列
Windows ドメイン用の Windows Internet Naming Service（WINS）サーバのホスト名または IP アドレス	指定なし
Window ドメインの管理グループ	定義済みの管理グループはありません。
Windows ドメインの NetBIOS 名	指定なし
Kerberos 認証	Disabled
Kerberos サーバのホスト名または IP アドレス（指定した Kerberos 領域用の Key Distribution Center [KDC; 鍵発行局] を運用するホスト）	指定なし
Kerberos サーバのポート番号（KDC サーバ上のポート番号）	ポート 88
Kerberos ローカル領域（WAAS 用のデフォルト領域）	Kerberos 領域空（から）の文字列
Kerberos 領域（ホスト名または DNS ドメイン名を Kerberos 領域にマップする）	空（から）の文字列

（注）　WAAS デバイス（RADIUS および TACACS+ クライアント）で RADIUS または TACACS+ キーを設定する場合は、必ず、外部の RADIUS または TACACS+ サーバにも同一のキーを設定してください。

「管理ログインの認証および許可の設定」（p.6-7）の説明に従って、WAAS Central Manager GUI を使用してこれらのデフォルトを変更します。

WAAS ソフトウェアには、Windows ドメイン認証を設定できる複数の Windows ドメイン ユーティリティが付属しています。WAAS CLI からこれらのユーティリティにアクセスするには、**windows-domain diagnostics** EXEC コマンドを使用できます。

WAAS Central Manager GUI からこれらのユーティリティを起動する、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインから、**[My WAN] > [Manage Devices]** を選択します。

ステップ 2　定義済みの順序でユーティリティを実行したいデバイスの横にある **[Edit]** アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、**[Admin] > [Authentication] > [Windows Domain]** を選択します。

ステップ 4　表示されるウィンドウで、ウィンドウの一番下にある **[Show Authentication Status]** ボタンをクリックします。

管理ログインの認証および許可の設定

WAAS デバイスまたはデバイス グループ（WAE のグループ）用の管理ログイン認証および許可を集中的に設定するには、次の手順に従ってください。

ステップ 1　管理ログイン要求の認証時に WAAS デバイス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 1 次ログイン データベースとして、RADIUS サーバを 2 次認証データベースとして使用します）。

ステップ 2　「WAAS デバイス用のログイン アクセス コントロール設定の構成」（p.6-8）の説明に従って、WAAS デバイス用のログイン アクセス コントロール設定を構成します。

ステップ 3　WAAS デバイスで管理ログイン認証サーバ設定を構成します（リモート認証データベースを使用する場合）。たとえば、次の項の説明に従って、WAAS デバイスが管理ログイン要求を認証するために使用する必要がある、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。

- RADIUS サーバ認証設定の構成（p.6-14）
- TACACS+ サーバ認証設定の構成（p.6-17）
- Windows ドメイン サーバ認証設定の構成（p.6-19）

ステップ 4　次のログイン認証設定方式の中から、WAAS デバイスが管理ログイン要求を処理するために使用する必要がある 1 つまたはすべての方式を指定します。

- 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（任意）。

たとえば、WAAS デバイスが管理ログイン要求を処理するときに、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。「WAAS デバイス用の管理ログイン認証および許可方式の有効化」（p.6-29）を参照してください。

注意　ローカル認証および許可を無効にする前に、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。ローカル認証が無効で、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、WAAS デバイスにログインできないことがあります。

WAAS Central Manager GUI または WAAS CLI を使用して、ローカルおよびリモート データベース（TACACS+、RADIUS、および Windows ドメイン）を有効または無効にすることができます。WAAS デバイスは、すべてのデータベースが無効になってい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（表 6-1 を参照してください）。管理認証と許可用に 1 つまたは複数の外部のサードパーティ データベース（TACACS+、RADIUS、または Windows ドメイン認証）を使用するように WAAS デバイスを設定した場合は、WAAS デバイスでもローカル認証方式と許可方式が有効であり、最後のオプションとしてローカル方式が指定されていることを確認します。そうでない場合、WAAS デバイスは、指定した外部のサードパーティ データベースに到達できない場合、デフォルトでローカル認証方式と許可方式へ進みません。

デフォルトでは、最初にローカル ログイン認証が有効になります。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 WAAS デバイス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。ローカル認証が無効の場合に、その他のすべての認証方式が無効になると、ローカル認証は自動的に再度有効になります。

ローカル ログイン認証を無効にできるのは、その他の複数の管理ログイン認証方式を有効にした後だけです。ただし、ローカル ログイン認証を無効にすると、その他のすべての管理ログイン認証方式が無効になった場合に、ローカル ログイン認証は自動的に再度有効になります。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。

管理ログインの認証方式と許可方式を同じ順序で設定することを強く推奨します。たとえば、管理ログイン認証と許可の両方の 1 次ログイン方式として RADIUS を使用し、2 次ログイン方式として TACACS+ を使用し、第 3 の方式として Windows を使用し、第 4 の方式としてローカル方式を使用するように、WAAS デバイスを設定します。

（注）　TACACS+ サーバは別の方式で認証されたユーザを許可しません。たとえば、Windows をプライマリ認証方式として設定し、TACACS+ をプライマリ許可方式として設定すると、TACACS+ 許可は失敗します。

ログイン認証方式と許可方式の優先順位リストの最後の方式として、ローカル方式を指定することを強く推奨します。この方法に従うことで、指定した外部のサードパーティ サーバ（TACACS+、RADIUS、または Windows ドメイン サーバ）に到達可能できない場合でも、WAAS 管理者は、ローカル認証方式と許可方式を使用して WAAS デバイスにログインできます。

このセクションでは、管理ログインを一元的に設定する方法について説明します。内容は、次のとおりです。

- WAAS デバイス用のログイン アクセス コントロール設定の構成（p.6-8）
- WAAS デバイス用のリモート認証サーバ設定の構成（p.6-14）
- WAAS デバイス用の管理ログイン認証および許可方式の有効化（p.6-29）

WAAS デバイス用のログイン アクセス コントロール設定の構成

このセクションでは、WAAS デバイスまたはデバイス グループ用の remote login（rlogin; リモートログイン）とアクセス コントロール設定を集中的に構成する方法について説明します。内容は、次のとおりです。

- WAAS デバイス用のセキュア シェル設定の構成（p.6-9）
- WAAS デバイス用の Telnet サービスの無効化と再有効化（p.6-11）
- WAAS デバイスに対する Message of the Day 設定（p.6-12）
- WAAS デバイス用の実行タイムアウト設定の構成（p.6-13）
- WAAS デバイス用の回線コンソール キャリア検出の設定（p.6-13）

WAAS デバイス用のセキュア シェル設定の構成

Secure Shell（SSH; セキュア シェル）は、サーバとクライアント プログラムから構成されます。Telnet のように、クライアント プログラムを使用して、SSH サーバが動作するマシンにリモートにログインできますが、Telnet と異なり、クライアントとサーバ間で伝達されるメッセージは暗号化されます。SSH の機能には、user authentication（uauth; ユーザ認証）、メッセージの暗号化、およびメッセージの認証があります。

（注）　WAAS デバイスの SSH 機能はデフォルトで無効に設定されています。

WAAS Central Manager GUI の SSH 管理ウィンドウを使用すると、設定、監視、またはトラブルシューティングのために特定の WAAS デバイスまたはデバイス グループにログインするときの暗号鍵の長さ、ログイン許容時間、およびパスワードの最大試行回数を指定できます。

WAAS デバイスまたはデバイス グループで SSH 機能を集中的に有効にするには、次の手順に従ってください。

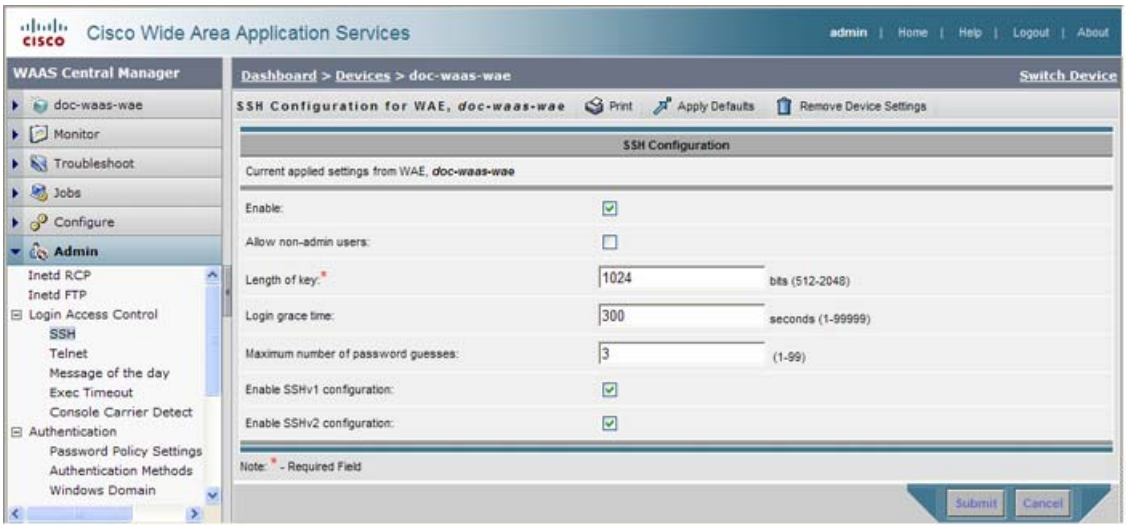
ステップ 1　WAAS Central Manager GUI ナビゲーション ペインから、**[My WAN] > [Manage Devices]**（または **[Manage Device Groups]**）を選択します。

ステップ 2　SSH を有効にしたいデバイス（またはデバイス グループ）の横にある **[Edit]** アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、**[Admin] > [Login Access Control] > [SSH]** を選択します。

[SSH Configuration] ウィンドウが表示されます（図 6-3 を参照）。

図 6-3　[SSH Configuration] ウィンドウ



ステップ 4　**[Enable]** チェック ボックスを選択して、SSH 機能を有効にします。SSH は、安全で暗号化されたチャネルを通じて、選択した WAAS デバイス（またはデバイス グループ）へのログイン アクセスを可能にします。

ステップ 5　**[Allow non-admin users]** チェック ボックスを選択して、非管理ユーザが SSH 経由で、選択したデバイス（またはデバイス グループ）にアクセスできるようにします。このオプションはデフォルトで無効になっています。

（注）　非管理ユーザとは、superuser ではない管理者です。スーパーユーザ以外の管理者はすべて、ログイン アカウントの特権レベルが 0 であるため、アクセスは WAAS デバイスのみに制限されています。スーパーユーザ管理者は、ログイン アカウントが最高の特権レベル、つまり特権レベル 15 であるため、WAAS デバイスへのフルアクセス権を持っています。

ステップ 6　[Length of key] フィールドで、SSH 暗号鍵を作成するために必要なビット数を指定します。デフォルトは、1024 です。

SSH を有効にするときは、必ず、クライアント プログラムがサーバの ID を確認するために使用する秘密鍵とホストの公開鍵の両方を生成してください。SSH クライアントを使用して WAAS デバイスにログインすると、デバイスで動作する SSH デーモンの公開鍵が、ホーム ディレクトリのクライアント マシン known_hosts ファイルに記録されます。その後に WAAS 管理者が [Length of key] フィールドにビット数を指定してホストの暗号鍵を再生成する場合、SSH クライアント プログラムを実行して WAAS デバイスにログインする前に、known_hosts ファイルから WAAS デバイスに関連する古い公開鍵項目を削除する必要があります。古い項目を削除したあとで SSH クライアント プログラムを使用すると、known_hosts ファイルが WAAS デバイス用の新しい SSH 公開鍵で更新されます。

ステップ 7　[Login grace time] フィールドで、クライアントとサーバ間のネゴシエーション（認証）フェーズ中に SSH セッションがタイムアウトする前にアクティブである時間（秒）を指定します。デフォルトは 300 秒です。

ステップ 8　[Maximum number of password guesses] フィールドで、1 接続当たりに許可する最大パスワード試行回数を指定します。デフォルトは、3 です。

[Maximum number of password guesses] フィールドの値は、SSH サーバ側から許可するパスワード試行回数を指定しますが、SSH ログイン セッションの実際のパスワード試行回数は、SSH サーバと SSH クライアントが許可するパスワード試行回数の合計で決定されます。一部の SSH クライアントは、SSH サーバがもっと多くの試行回数を許可する場合でも、許容される最大パスワード試行回数を 3 回（場合によっては 1 回）に制限します。許可するパスワード試行回数に *n* を指定すると、特定の SSH クライアントはこの数字を *n* + 1 として解釈します。たとえば、特定のデバイスの試行回数を 2 に設定すると、SSH クライアントからの SSH セッションは、3 回のパスワード試行を許可します。

ステップ 9　クライアントが SSH プロトコルのバージョン 1 またはバージョン 2 のどちらを使用しての接続を許可するかを指定します。

- バージョン 1 を指定するには、**[Enable SSHv1]** チェック ボックスを選択します。
- バージョン 2 を指定するには、**[Enable SSHv2]** チェック ボックスを選択します。

（注）　SSH バージョン 1 とバージョン 2 を同時に有効にすることができます。あるいは、片方のバージョンだけを有効にすることができます。**[Enable]** チェック ボックスの選択を解除して SSH 機能を無効にしない場合、両方の SSH バージョンを無効にすることはできません（ステップ 4 を参照）。

ステップ 10 **[Submit]** をクリックして、設定を保存します。

デフォルトまたはデバイス グループ設定を適用したあとでまだ保存されていない変更があると、[Current Settings] 行に、「Click Submit to Save」メッセージが赤い色で表示されます。また、**[Reset]** ボタンをクリックすると、以前の設定に戻すことができます。[Reset] ボタンは、デフォルトまたはグループ設定を適用して現在のデバイス設定を変更し、まだ変更を送信していない場合だけ表示されます。

変更した設定を保存せずにこのウィンドウを終了しようとすると、変更を送信するように警告するダイアログボックスが表示されます。このダイアログボックスは、Internet Explorer ブラウザを使用している場合のみ表示されます。

CLI から SSH 設定を構成するには、**sshd** および **ssh-key-generate** グローバル設定コマンドを使用できます。

WAAS デバイス用の Telnet サービスの無効化と再有効化

デフォルトでは、Telnet サービスは、WAAS デバイスで有効になっています。Telnet セッションでなく、コンソール接続を使用して、WAAS デバイス上のデバイス ネットワーク設定を定義する必要があります。ただし、コンソール接続を使用してデバイス ネットワーク設定を定義したあとでは、Telnet セッションを使用して以後の設定作業を行うことができます。

デバイスに Telnet するために [Device Dashboard] ウィンドウで [Telnet] ボタンを使用するには、Telnet サービスを有効にする必要があります。

WAAS デバイスまたはデバイス グループで Telnet サービスを集中的に無効にするには、次の手順に従ってください。

ステップ 1 WAAS Central Manager GUI ナビゲーション ペインから、**[My WAN] > [Manage Devices]**（または **[Manage Device Groups]**）を選択します。

ステップ 2 Telnet を無効したいデバイス（またはデバイス グループ）の横にある **[Edit]** アイコンをクリックします。

ステップ 3 ナビゲーション ペインで、**[Admin] > [Login Access Control] > [Telnet]** を選択します。[Telnet Settings] ウィンドウが表示されます。

ステップ 4 選択したデバイス（またはデバイス　グループ）用のリモート端末接続用の端末エミュレーション プロトコルを無効にするには、**[Telnet Enable]** チェック ボックスの選択を解除します。

ステップ 5 **[Submit]** をクリックして、設定を保存します。

デフォルトまたはデバイス グループ設定を適用したあとでまだ保存されていない変更があると、[Current Settings] 行の横に、「Click Submit to Save」メッセージが赤い色で表示されます。また、**[Reset]** ボタンをクリックすると、以前の設定に戻すことができます。**[Reset]** ボタンは、デフォルトまたはグループ設定を適用して現在のデバイス設定を変更し、まだ変更を送信していない場合だけ表示されます。

変更した設定を保存せずにこのウィンドウを終了しようとすると、変更を送信するように警告するダイアログボックスが表示されます。このダイアログボックスは、Internet Explorer ブラウザを使用している場合のみ表示されます。

あとでデバイス（またはデバイス グループ）で Telnet サービスを集中的に再有効化するには、[Telnet Settings] ウィンドウで **[Telnet Enable]** チェック ボックスを選択し、**[Submit]** をクリックします。

CLI から Telnet を無効にするには、**no telnet enable** グローバル設定コマンドを使用できます。また、Telnet を有効にするには、**telnet enable** グローバル設定コマンドを使用できます。

WAAS デバイスに対する Message of the Day 設定

Message of the Day（MOTD）機能では、WAAS ネットワークの一部であるデバイスへのログイン時にユーザに情報を提供します。設定できるメッセージは、次の 3 種類です。

- MOTD バナー
- EXEC プロセス作成バナー
- ログイン バナー

（注） SSH バージョン 1 クライアントを実行中でデバイスにログインしている場合、MOTD とログイン バナーは表示されません。デバイスへのログイン時にバナーを表示するには、SSH バージョン 2 を使用する必要があります。

MOTD 設定を行うには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインから、**[My WAN] > [Manage Devices]** を選択します。[Devices] ウィンドウが表示されます。

ステップ 2　Message of The Day を設定する WAAS デバイスの横にある **[Edit]** アイコンをクリックします。選択したデバイス用の [Device Dashboard] ウィンドウが表示されます。

ステップ 3　ナビゲーション ペインで、**[Admin] > [Login Access Control] > [Message of the day]** を選択します。選択したデバイス用の [MOTD Configuration] ウィンドウが表示されます。

ステップ 4　MOTD 設定を有効にするには、**[Enable]** チェック ボックスを選択します。Message of the Day（MOTD）バナー、EXEC プロセス作成バナー、ログイン バナーのフィールドが有効になります。

ステップ 5　Message of the Day（MOTD）バナーのフィールドで、デバイスにユーザがログインしたあとに MOTD バナーとして表示する文字列を入力します。

（注） [Message of the Day (MOTD) Banner] [EXEC Process Creation Banner] [Login Banner] フィールドは、最大 1024 文字入力できます。改行文字（または Enter）は、システムは \n と解釈するため、2 文字として数えられます。MOTD テキストでは、`、%、^、および " などの特殊文字を使用できません。テキストにこれらの特殊文字が含まれる場合、WAAS ソフトウェアは MOTD 出力からその文字を削除します。

ステップ 6　[EXEC Process Creation Banner] フィールドで、ユーザがデバイスの EXEC シェルを入力したときの EXEC プロセス作成バナーとして表示される文字列を入力します。

ステップ 7　[Login Banner] フィールドで、ユーザがデバイスにログインするときに、MOTD バナーのあとに表示される文字列を入力します。

ステップ 8　設定を保存するには、**[Submit]** をクリックします。

WAAS デバイス用の実行タイムアウト設定の構成

WAAS デバイスまたはデバイス グループで非アクティブな Telnet セッションを開いておく時間の長さを集中的に設定するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインから、**[My WAN] > [Manage Devices]**（または **[Manage Device Groups]**）を選択します。

ステップ 2　実行タイムアウトを設定したいデバイス（またはデバイス グループ）の横にある **[Edit]** アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、**[Admin] > [Login Access Control] > [Exec Timeout]** を選択します。

ステップ 4　[Exec Timeout] フィールドで、アクティブ セッションがタイムアウトする時間（分）を指定します。デフォルトは、15 分です。

WAAS デバイスとの Telnet セッションは、このフィールドに指定した時間の間、非アクティブのまま開いておくことができます。実行タイムアウト時間が経過すると、WAAS デバイスは自動的に Telnet セッションを閉じます。

ステップ 5　**[Submit]** をクリックして、設定を保存します。

デフォルトまたはデバイス グループ設定を適用したあとでまだ保存されていない変更があると、[Current Settings] 行の横に、「Click Submit to Save」メッセージが赤い色で表示されます。また、**[Reset]** ボタンをクリックすると、以前の設定に戻すことができます。**[Reset]** ボタンは、デフォルトまたはグループ設定を適用して現在のデバイス設定を変更し、まだ変更を送信していない場合だけ表示されます。

変更した設定を保存せずにこのウィンドウを終了しようとすると、変更を送信するように警告するダイアログボックスが表示されます。このダイアログボックスは、Internet Explorer ブラウザを使用している場合のみ表示されます。

CLI から Telnet セッション タイムアウト を設定するには、**exec-timeout** グローバル設定コマンドを使用できます。

WAAS デバイス用の回線コンソール キャリア検出の設定

WAAS デバイスをモデムに接続して呼び出しを受信する予定の場合は、キャリア検出を有効にする必要があります。

（注）　デフォルトでは、この機能は、WAAS デバイスで無効になっています。

WAAS デバイスまたはデバイス グループ用のコンソール回線キャリア検出を集中的に 有効にするには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインから、**[My WAN] > [Manage Devices]**（または **[Manage Device Groups]**）を選択します。

ステップ 2　設定したいデバイス（またはデバイス グループ）の横にある **[Edit]** アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、**[Admin] > [Login Access Control] > [Console Carrier Detect]** を選択します。[Console Carrier Detect Settings] ウィンドウが表示されます。

ステップ 4　**[Enable console line carrier detection before writing to the console]** チェック ボックスを選択して、設定するためのウィンドウを有効にします。

ステップ 5　**[Submit]** をクリックして、設定を保存します。

キャリア検知ピンが配線されていない空のモデム ケーブルを使用すると、キャリア検知信号が検出されるまで WAE がコンソールで応答しないように見えることを説明するメッセージが表示されます。構成の不具合から回復するには、WAE をリブートし、キャリア検出設定を無視するように 0x2000 起動フラグを設定する必要があります。

ステップ 6　**[OK]** をクリックして続行します。

CLI からコンソール回線キャリア検出を設定するには、**line console carrier-detect** グローバル設定コマンドを使用できます。

WAAS デバイス用のリモート認証サーバ設定の構成

ログイン認証方式に 1 台または複数の外部認証サーバを含む予定の場合は、WAAS Central Manager GUI で認証方式を設定する前に、これらのサーバ設定を構成する必要があります。ここでは、次の内容について説明します。

- RADIUS サーバ認証設定の構成（p.6-14）
- TACACS+ サーバ認証設定の構成（p.6-17）
- TACACS+ 有効化パスワード属性の設定（p.6-18）
- Windows ドメイン サーバ認証設定の構成（p.6-19）
- LDAP サーバ署名（p.6-26）

RADIUS サーバ認証設定の構成

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。

RADIUS 認証クライアントは、WAAS ソフトウェアを実行するデバイスに常駐します。有効にすると、これらのクライアントは認証要求を中央の RADIUS サーバへ送信します。RADIUS サーバには、ユーザ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。

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、監視、設定、またはトラブルシューティングのためにデバイスを設定するために WAAS デバイスに最初にログインしたときに実行されます。RADIUS 認証は、デフォルトでは無効になっています。RADIUS 認証とその他の認証方式は同時に有効にすることができます。また、最初に使用する方式を指定することもできます。

ヒント WAAS Central Manager は、ユーザ認証情報をキャッシュしません。したがって、ユーザは、すべての要求について RADIUS サーバに対して再認証されます。多数の認証要求によるパフォーマンスの低下を防止するには、RADIUS サーバと同じ位置またはできるだけ近くに WAAS Central Manager デバイスを設置して、認証要求をできるだけ迅速に処理するようにします。

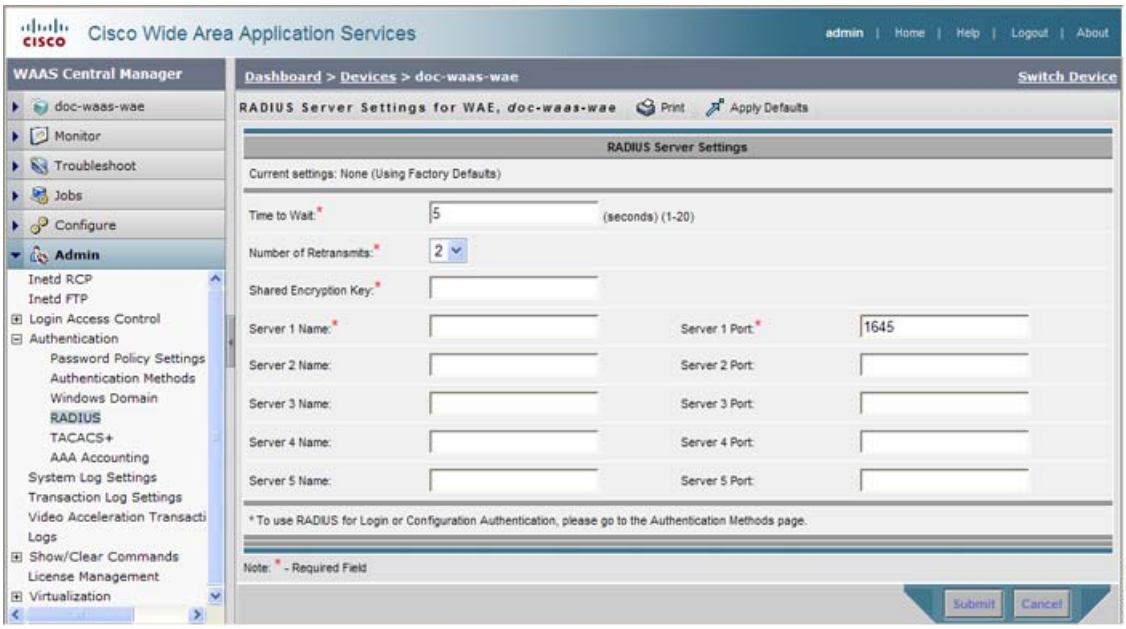
WAAS デバイスまたはデバイス グループ用の RADIUS サーバ設定を集中的に構成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインから、**[My WAN] > [Manage Devices]**（または **[Manage Device Groups]**）を選択します。

ステップ 2　設定したいデバイス（またはデバイス グループ）の横にある **[Edit]** アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、**[Admin] > [Authentication] > [RADIUS]** を選択します。[RADIUS Server Settings] ウィンドウが表示されます（図 6-4 を参照）。

図 6-4　[RADIUS Server Settings] ウィンドウ



ステップ 4　[Time to Wait] フィールドに、デバイスまたはデバイス グループが、タイムアウトする前に RADIUS サーバから応答を待つ必要がある時間を指定します。範囲は、1 ～ 20 秒です。デフォルト値は 5 秒です。

ステップ 5　[Number of Retransmits] フィールドに、RADIUS サーバに接続するときに許可する再試行回数を指定します。デフォルト値は 2 回です。

ステップ 6　[Shared Encryption Key] フィールドに、RADIUS サーバと通信するために使用する秘密鍵を入力します。

（注）　WAAS デバイス（RADIUS クライアント）で RADIUS キーを設定する場合は、必ず、外部の RADIUS サーバにも同一のキーを設定してください。

ステップ 7　[Server Name] フィールドに、RADIUS サーバの IP アドレスまたはホスト名を入力します。5 つの異なるホストが許可されます。

ステップ 8　[Server Port] フィールドに、RADIUS サーバを受信する UDP ポート番号を入力します。少なくとも 1 つのポートを指定する必要があります。5 つの異なるホストが許可されます。

ステップ 9　**[Submit]** をクリックして、設定を保存します。

これで、「WAAS デバイス用の管理ログイン認証および許可方式の有効化」（p.6-29）の説明に従って、この WAAS デバイスまたはデバイス グループ用の管理ログイン認証および許可方式として、RADIUS を有効にすることができます。

CLI から RADIUS 設定を構成するには、**radius-server** グローバル設定コマンドを使用できます。

TACACS+ サーバ認証設定の構成

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 NAS 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+ デー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、監視、設定、またはトラブルシューティングのための WAE を設定するために WAAS デバイスに最初にログインしたときに実行されます。

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、AAA 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+ 設定では、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。WAAS デバイスで暗号鍵を設定する場合は、TACACS+ サーバで設定した暗号鍵と同じ暗号鍵を設定する必要があります。TACACS+ クライアントとサーバは、暗号鍵を使用して、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、デフォルトでは無効になっています。TACACS+ 認証とローカル認証は同時に有効にすることができます。

TACACS+ データベースは、ユーザが WAAS デバイスにアクセスする前にユーザを検査します。TACACS+ は、Department of Defense（DoD; 米国国防総省）（RFC 1492）の原案から派生したものであり、シスコシステムズは非特権モードと特権モードのアクセス制御を強化するために TACACS+ を使用しています。WAAS ソフトウェアは、TACACS+ だけをサポートしています。TACACS や拡張 TACACS は、サポートしていません。

ユーザ認証に TACACS+ を使用している場合は、TACACS+ サーバで定義したユーザ グループと一致する WAAS ユーザ グループ名を作成できます。その後、TACACS+ サーバで定義したグループのメンバシップに基づいて、WAAS でユーザに動的にロールとドメインを割り当てることができます。（「アカウントの操作」[p.7-3] を参照してください）。TACACS+ コンフィギュレーション ファイルで、次のように各ユーザに関連グループ名を指定する必要があります。

```
user = tacusr1 {
 default service = permit
 service = exec
 {
   waas_rbac_groups = admin,groupname1,groupname2
   priv-lvl = 15
 }
 global = cleartext "tac"
}
```

各ユーザの属するグループを、グループごとにカンマで区切って waas_rbac_groups 属性に表示します。

ヒント WAAS Central Manager はユーザ認証情報をキャッシュしないので、ユーザはすべての要求について TACACS に対して再認証されます。多数の認証要求によるパフォーマンスの低下を防止するには、TACACS+ サーバと同じ位置またはできるだけ近くに WAAS Central Manager デバイスを設置して、認証要求をできるだけ迅速に処理するようにします。

TACACS+ 有効化パスワード属性の設定

WAAS ソフトウェアの CLI EXEC モードでは、システム動作の設定、表示、およびテストを実行できます。このモードは、ユーザと特権の 2 つのアクセス レベルに分かれています。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（superuser または admin 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有効化パスワードを定義できる有効化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 カウント（特権レベル 0）で WAAS デバイス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:
```

（注） この注意事項は、WAAS 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。

WAAS デバイスまたはデバイス グループ用の TACACS+ サーバ設定を集中的に構成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインから、**[My WAN] > [Manage Devices]**（または **[Manage Device Groups]**）を選択します。

ステップ 2　設定したいデバイス（またはデバイス グループ）の横にある **[Edit]** アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、**[Admin] > [Authentication] > [TACACS+]** を選択します。[TACACS+ Server Settings] ウィンドウが表示されます

ステップ 4　認証用に ASCII 型（平文）のパスワードを使用するには、**[Use ASCII Password Authentication]** チェック ボックスを選択します。

デフォルトのパスワード型は、Password Authentication Protocol（PAP; パスワード認証プロトコル）です。ただし、認証パケットを ASCII クリアテキストで送信する場合、パスワード型を ASCII に変更できます。

ステップ 5　[Time to Wait] フィールドで、デバイスがタイムアウトを待つ時間の長さを指定します。範囲は、1 ～ 20 秒です。デフォルト値は 5 秒です。

ステップ 6　[Number of Retransmits] フィールドに、TACACS+ サーバに接続するときに許可する再試行回数を指定します。範囲は、1 ～ 3 回です。デフォルト値は 2 回です。

ステップ 7　[Security Word] フィールドに、TACACS+ サーバと通信するために使用する秘密鍵を入力します。

（注）　WAAS デバイス（TACACS+ クライアント）で TACACS+ キーを設定する場合は、必ず、外部の TACACS+ サーバにも同一のキーを設定してください。

ステップ 8　[Primary Server] フィールドに、TACACS+ サーバの IP アドレスまたはホスト名を入力します。

ステップ 9　[Secondary Server] フィールドに、TACACS+ サーバの IP アドレスまたはホスト名を入力します。

ステップ 10　[Tertiary Server] フィールドに、TACACS+ サーバの IP アドレスまたはホスト名を入力します。

（注）　最大 2 台のバックアップ TACACS+ サーバを指定できます。

ステップ 11　**[Submit]** をクリックして、設定を保存します。

これで、「WAAS デバイス用の管理ログイン認証および許可方式の有効化」（p.6-29）の説明に従って、この WAAS デバイスまたはデバイス グループ用の管理ログイン認証および許可方式として、TACACS+ を有効にすることができます。

CLI から TACACS+ 設定を構成するには、**tacacs** グローバル設定コマンドを使用できます。

Windows ドメイン サーバ認証設定の構成

Windows ドメイン コントローラは、チャレンジ / レスポンスまたは共有秘密認証方式を使用して WAAS ソフトウェア サービスへのアクセスを制御するように設定できます。システム管理者は、FTP、SSH、または Telnet セッションを使用して、あるいは 1 つのユーザ アカウント（ユーザ名 / パスワード / 特権）でコンソールまたは WAAS Central Manager GUI を使用して、WAAS デバイスにログインできます。Windows ドメイン認証では、RADIUS および TACACS+ 認証方式を同時に設定できます。Windows ドメイン認証を有効にすると、さまざまな認証ログイン統計情報をログに記録するように設定できます。ログ ファイル、統計カウンタ、および関連情報は、いつでも消去できます。

WAAS ネットワークでは、次の場合に Windows ドメイン認証を使用します。

- WAAS Central Manager GUI へのログイン
- WAE Device Manager GUI へのログイン
- 任意の WAAS デバイスでの CLI 設定
- 切断モードの操作

WAAS Central Manager デバイス、個別の WAAS デバイス（たとえば、Core WAE または Edge WAE）、またはデバイスのグループ用の Windows 認証を設定できます。WAAS デバイスで Windows ドメイン認証を設定するには、一連の Windows ドメイン認証設定を構成する必要があります。

（注）　Windows ドメイン認証は、WAAS デバイスに 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。デバイスが正しく登録されていない場合、認証と許可は実行されません。

ここでは、次の内容について説明します。

WAAS デバイス上の Windows ドメイン サーバ設定の構成

認証に使用する Windows ドメイン コントローラの名前と IP アドレス、またはホスト名を知っている必要があります。

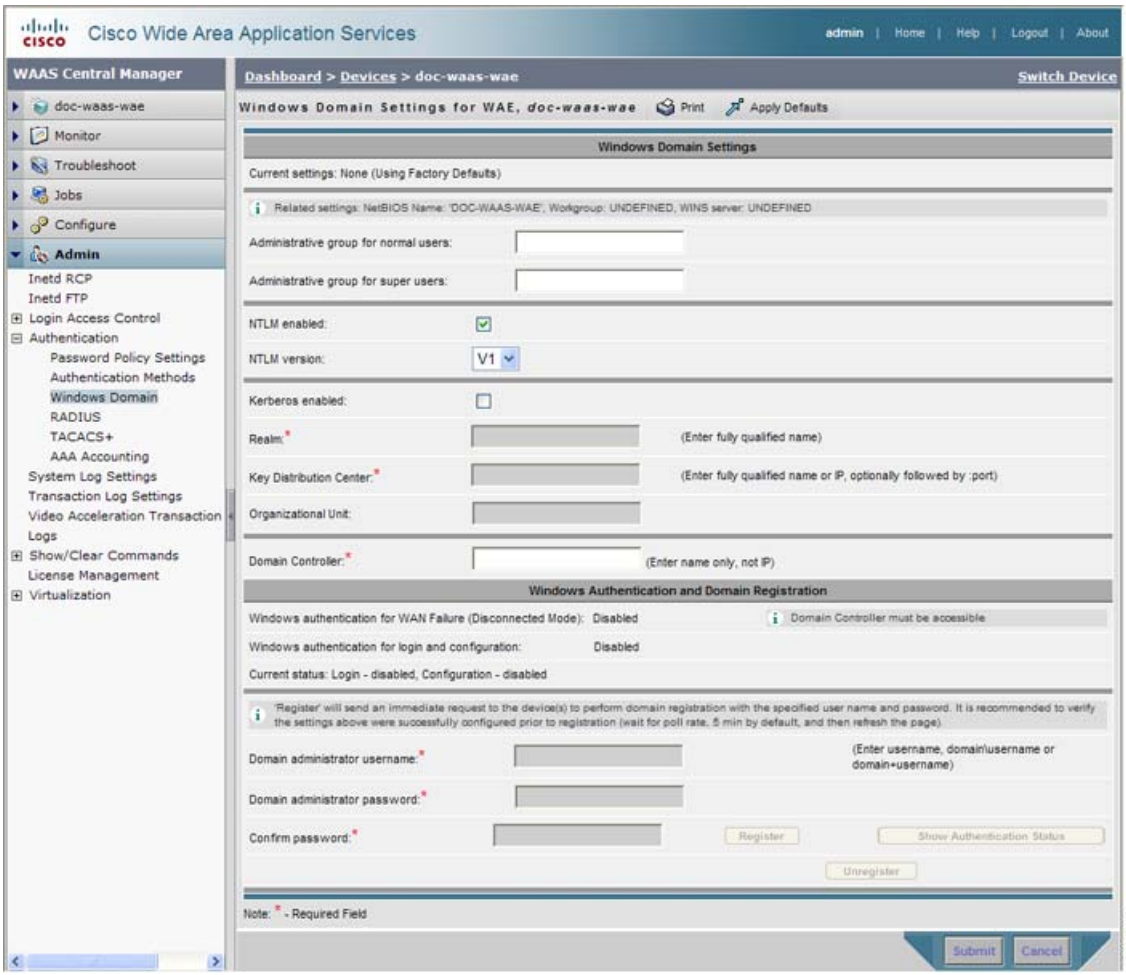
WAAS デバイスまたはデバイス グループ用の Windows ドメイン サーバ設定を構成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインから、**[My WAN] > [Manage Devices]**（または **[Manage Device Groups]**）を選択します。

ステップ 2　設定したいデバイス（またはデバイス グループ）の横にある **[Edit]** アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、**[Admin] > [Authentication] > [Windows Domain]** を選択します。[Windows Domain Server Settings] ウィンドウが表示されます（図 6-5 を参照）。

図 6-5　[Windows Domain Server Settings] ウィンドウ



（注）　選択したデバイス（またはデバイス グループ）用に関連する WINS サーバおよびワークグループまたはドメイン名が定義されていない場合、図 6-5 に示すように、このウィンドウの一番上に、関連する設定が定義されていないことを知らせる情報メッセージが表示されます。これらの設定を定義するには、**[Configure] > [Network] > [Windows Name Services]** を選択します。

ステップ 4　[Administrative group for normal users] フィールドにグループの名前を入力して、選択したデバイス（またはデバイス グループ）へのアクセスに制限がある特権レベルが 0 の通常のユーザ（superuser でない管理者）用の管理グループを指定します。

（注）　デフォルトで、WAE に設定されている Windows ドメイン許可用のユーザ グループは、事前に定義されていません。

ステップ 5　[Administrative group for superusers] フィールドにグループの名前を入力して、選択したデバイス（またはデバイス グループ）に完全にアクセスできる特権レベルが 15 の特権ユーザ（superuser である管理者）用の管理グループを指定します。

（注）　WAE で Windows ドメイン管理グループを設定することに加えて、Microsoft Windows 2000 または 2003 サーバで Windows ドメイン管理グループを設定する必要があります。Windows ドメイン管理特権ユーザ グループと通常のユーザ グループを作成する必要があります。特権ユーザ グループのグループ スコープが global に設定されていることを確認し、新しく作成した管理グループにユーザ メンバを割り当て、Windows ドメイン特権ユーザ グループにユーザ アカウント（たとえば、winsuper ユーザ）を追加します。Windows サーバで Windows ドメイン管理グループを設定する方法については、Microsoft 社のマニュアルを参照してください。

ユーザが Telnet セッション、FTP、または SSH セッションを通じてこの WAE にアクセスしようとすると、WAE は Active Directory ユーザ データベースを使用して管理アクセス要求を認証するように設定されます。

ステップ 6　次のように、選択したデバイス（またはデバイス グループ）への管理ログイン用の安全な共有認証方式として NTLM または Kerberos を選択します。

（注）　ユーザがドメイン アカウントにログインする Windows 2000 以上が動作する Windows システムには、Kerberos バージョン 5 が使用されます。

- NTLM を有効にするには、**[NTLM enabled]** チェック ボックスを選択します。
- NTML バージョン 1 を選択するには、**[NTLM enabled]** チェック ボックスを選択します。デフォルトでは、NTLM バージョン 1 が選択されます。

  NTLM バージョン 1 は、Active Directory を使用する Windows 98、Windows NT などの従来のシステム、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。Windows 2000 SP4 または Windows 2003 のドメイン コントローラ の使用には、Kerberos 認証を推奨します。
- NTLM バージョン 2 を選択するには、ドロップダウン リストから **[V2]** を選択します。

  NTLM バージョン 2 は、Windows 98 と Active Directory を実行している Windows システム、Windows NT 4.0（Service Pack 4 以降）、Windows XP、Windows 2000、および Windows 2003 で使用されます。WAAS プリント サーバの NTLM バージョン 2 のサポートを有効にすると、NTLM または LM を使用するクライアントへはアクセスできなくなります。

注意　すべてのクライアントのセキュリティ ポリシーが [Send NTLMv2 responses only/Refuse LM and NTLM] に設定されている場合のみ、プリント サーバでの NTLM バージョン 2 サポートを有効にします。

- Kerberos を選択するには、**[Kerberos enabled]** チェック ボックスを選択します。[Realm] フィールドに、WAAS デバイスが存在する領域の完全修飾名を入力します。[Key Distribution center] フィールドに、Kerberos 暗号鍵配信局の完全修飾名または IP アドレスを入力します。必要な場合、[Organizational Unit] フィールドに組織単位の名前を入力します。

すべての Windows 2000 ドメインは、Kerberos 領域です。Windows 2000 ドメイン名は DNS ドメイン名でもあるため、Windows 2000 ドメイン名用の Kerberos 領域名は常に大文字です。この大文字化は、Kerberos バージョン 5 プロトコル資料（RFC-4120）での領域名として DNS 名を使用する勧告に従っており、Kerberos に基づく他の環境との相互運用性だけに影響します。

ステップ 7　[Domain Controller] フィールドに、Windows ドメイン コントローラの名前を入力します。

ドメイン コントローラ名が無効の場合、またはドメイン コントローラが利用できない場合でも、ドメインは登録できます。登録プロセスでは smb.conf ファイルの パスワード サーバ フィールドのドメイン コントローラ名が使用されるためです。smb.conf ファイルの優先順位リストで共通に使用される形式は、「*DomainControllerName*, *」または「*」（アスタリスク）です。Samba ではまず、名前でドメイン コントローラを探し、見つからない場合は「*」でワークグループの利用可能なドメイン コントローラを探します。この動作により、ドメイン コントローラが利用できなくてもドメインを登録することができます。

ステップ 8　**[Submit]** をクリックします。

（注）　**[Submit]** をクリックし、指定した変更が WAAS Central Manager データベースにコミットされたことを確認してください。ステップ 9 の横に入力するドメイン管理者のユーザ名とパスワードは、WAAS Central Manager のデータベースに格納されません。

ステップ 9　選択したデバイス（またはデバイス グループ）を Windows ドメイン コントローラに登録するには、次の手順に従ってください。

a. [Domain Administrator username] フィールドに、指定した Windows ドメイン コントローラの管理ユーザ名（domain\username またはドメイン名とユーザ名）を入力します。

b. [Domain Administrator password] フィールドに、指定した Windows ドメイン コントローラの管理パスワードを入力します。

c. [Confirm password] フィールドに、指定した Windows ドメイン コントローラの管理パスワードを入力します。

d. **[Register]** ボタンをクリックします。

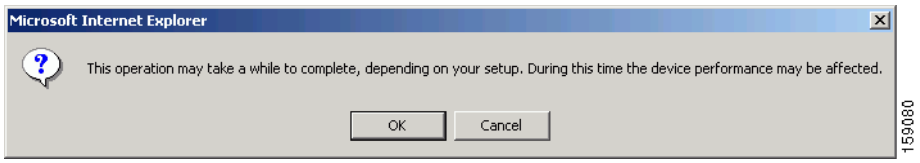
（注）　**[Register]** ボタンをクリックすると、WAAS Central Manager は、SSH を使用して、ただちに WAAS デバイス（またはデバイス グループ）へ登録要求を送信します（指定したドメイン管理者パスワードは、SSH で暗号化されます）。登録要求は、指定したドメイン管理者のユーザ名とパスワードを使用して、指定した Windows ドメイン コントローラへのドメイン登録を実行するように、デバイスに指示します。デバイスにアクセスできる場合（NAT の後ろにあり、外部 IP アドレスを持っている場合）、デバイス（またはデバイス グループ）は登録要求を実行します。

e. 登録要求のステータスを確認するには、数分経ってから **[Show Authentication Status]** ボタンをクリックします。

[Refresh Authentication Status] チェック ボックスを選択したあとで **[Show Authentication Status]** ボタンをクリックしてもかまいません。このボックスを選択すると、WAAS Central Manager は、ドメイン登録ステータスの更新をデバイスに問い合わせます。選択を外すと、Central Manager のローカル キャッシュのステータスが取得されます。

[Show Authentication Status] ボタンをクリックすると、認証要求ステータスを表示するかどうかを問うダイアログ ボックスが表示されます（図 6-6 を参照）。

図 6-6　確認ダイアログボックス



f. **[OK]** をクリックして続行するか、**[Cancel]** をクリックして要求を取り消します。

要求が失敗した場合、エラー ダイアログを受信します。数分経ってから、再試行して更新された認証ステータスを参照してください。

要求が正常に終了した場合、ドメイン登録ステータスは、図 6-5 の下の部分の [Windows Authentication] と [Domain Registration] 見出しの下に表示されます。さらに、ウィンドウ認証と切断モードのステータスもこの部分に表示されます。

Windows のドメイン設定後に、Windows の認証を有効にするプロセスを完了するには、「WAAS デバイス用の管理ログイン認証および許可方式の有効化」（p.6-29）の説明に従って、[Authentication Methods] ウィンドウを使用して、Windows をデバイスに対する認証および許可方式としてと設定する必要があります。

WAAS CLI でなく、WAAS Central Manager GUI を使用して、Windows ドメイン サーバ設定を構成することを推奨します。ただし、CLI を使用したい場合は、『*Cisco Wide Area Application Services Command Reference*』で次のコマンドを参照してください。**windows-domain** と **kerberos**（共有認証方式 Kerberos を使用中の場合）

次に、次のコマンド（Kerberos 認証の場合）を使用して、設定した Windows ドメイン サーバに WAAS デバイスを登録し、検査します。

```
WAE# windows-domain diagnostics net  "ads join -U AdminUsername%AdminPassword"
WAE# windows-domain diagnostics net  "ads testjoin -U AdminUsername%AdminPassword"
```

NTLM 認証の場合は、次のコマンドを代わりに使用します。

```
WAE# windows-domain diagnostics net  "rpc join -U AdminUsername%AdminPassword"
WAE# windows-domain diagnostics net  "rpc testjoin -U AdminUsername%AdminPassword"
```

最後に、次のコマンドを使用して、管理ログイン認証および許可設定として Windows ドメインを有効にします。

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

切断モードで内容要求の認証を有効にするには、**authentication content-request windows-domain disconnected-mode enable** 設定コマンドを使用します。

Windows ドメイン コントローラからの WAE の登録解除

Windows ドメイン コントローラから WAE デバイスを登録解除する場合、Kerberos 共有認証方式を使用している場合は、WAAS Central Manager から直接行うことができます。NTLM メソッドを使用している場合、WAAS Central Manager を使用して WAE を登録解除できません。ドメイン コントローラにログインし、デバイス登録を手動で削除する必要があります。

デバイスを登録解除する前に、デバイスに対するウィンドウズ認証を無効にする必要があります。

WAE デバイスを登録解除するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインから、**[My WAN] > [Manage Devices]**（または **[Manage Device Groups]**）を選択します。

ステップ 2　登録解除したいデバイス（またはデバイス グループ）の横にある **[Edit]** アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、**[Admin] > [Authentication] > [Authentication Methods]** を選択します。[Authentication and Authorization Methods] ウィンドウが表示されます（図 6-7 [p.6-31] を参照）。

ステップ 4　[Authentication Login Methods] と [Authorization Methods] セクションの両方の下で、WINDOWS に設定してあるそれぞれのドロップダウン リストを何か別のものに変更します。設定の変更の詳細については、「WAAS デバイス用の管理ログイン認証および許可方式の有効化」（p.6-29）を参照してください。

ステップ 5　**[Submit]** をクリックして、設定を保存します。

ステップ 6　ナビゲーション ペインで、**[Admin] > [Authentication] > [Windows Domain]** を選択します。[Windows Domain Server Settings] ウィンドウが表示されます（図 6-5 を参照）。

ステップ 7　（任意）管理者のユーザ名とパスワードを、[Domain administrator username] [Domain administrator password] および [Confirm password] フィールドに入力します。ユーザ名とパスワードは必須ではありませんが、登録解除にドメイン コントローラが必要とする場合もあります。

ステップ 8　スクロール ダウンして **[Unregister]** ボタンをクリックします。

（注）　**[Unregister]** ボタンをクリックしたとき、WAAS Central Manager はただちに登録解除要求を WAAS デバイス（またはデバイス グループ）に SSH を使用して送信します。登録解除要求によって、指定された Windows ドメイン コントローラからデバイスを登録解除します。

a. 登録解除要求のステータスを確認するには、数分経ってから **[Show Authentication Status]** ボタンをクリックします。認証要求のステータスを表示するためにこの要求を続行するかどうかを確認するダイアログボックスが表示されます（図 6-6 を参照）。

b. **[OK]** をクリックして続行するか、**[Cancel]** をクリックして要求を取り消します。

CLI を使用して WAE デバイスを登録解除する場合、まず次のコマンドを使用して Windows 認証を無効にする必要があります。

```
WAE(config)# no authentication login windows-domain enable
WAE(config)# no authentication configuration windows-domain enable
```

次に、WAAS デバイスを Windows ドメイン サーバから次のコマンドを使用して登録解除します（Kerberos 認証の場合）。

```
WAE# windows-domain diagnostics net  "ads leave -U AdminUsername%AdminPassword"
```

NTLM 認証では、WAAS デバイスを登録解除する CLI コマンドがありません。

Edge WAE 用の自動マシン アカウント パスワード変更の無効化

認証用に Windows ドメイン コントローラが設定され、Edge WAE で切断モードが有効になっている WAAS ネットワークでは、WAN 障害時にドメイン コントローラは内容要求を認証します。デフォルトで、Windows ドメイン コントローラは、認証プロセスの一環として自動マシン アカウント パスワード変更を実行します。Edge WAE 用のマシン アカウント パスワードは 7 日周期で Edge WAE とドメイン コントローラの間で自動的にネゴシエートされ、変更されます。ただし、認証サービスが停止している場合、このプロセスは実行されず、Edge WAE 用のマシン アカウント パスワードは失効します。

この状況を防止するには、Edge WAE 用の自動マシン アカウント パスワード変更を無効にすることを推奨します。次の手順は、グループ ポリシー エディタを使用して、Windows XP および Windows Server 2003 用の自動マシン アカウント パスワード変更を無効にする方法を示しています。他の Windows オペレーティング システム用の自動マシン アカウント パスワード変更を無効にする方法の詳細については、Microsoft 社の [Help and Support] ページを参照してください。

グループ ポリシー エディタを使用して Edge WAE 用の自動的なマシン アカウント パスワード変更を無効にするには、次の手順に従ってください。

ステップ 1　Windows ドメイン コントローラで、**[スタート]** をクリックし、**[プログラム名を指定して実行]** を選択します。

ステップ 2　プロンプトに **Gpedit** と入力し、**[OK]** をクリックします。

ステップ 3　[Local Computer Policy]、[Windows Settings]、[Security Settings]、[Local Policies]、[Security Settings]、[Local Policies]、[Security] オプションを展開します。

ステップ 4　次の設定を行います。ドメイン メンバー：マシン アカウントのパスワード変更を無効にします（DisablePasswordChange）。

LDAP サーバ署名

LDAP サーバ署名は、Microsoft Windows Server のネットワーク セキュリティ設定の設定オプションです。このオプションは、Lightweight Directory Access Protocol（LDAP）クライアント用の署名要件を制御します。LDAP 署名は、LDAP パケットがネットワークの途中で改変されていないことを確認し、パッケージ データが既知の送信元から発信されたことを保証するために使用されます。Windows Server 2003 の管理ツールは、LDAP 署名を使用して、管理ツールの実行インスタンスと管理対象サーバ間の通信の安全を確保します。

トランスポート レイヤ セキュリティ（TLS、RFC 2830）プロトコルを使用してインターネット通信のプライバシーを保護することで、クライアント / サーバアプリケーションは、盗聴、改変、またはメッセージの偽造を防止して通信できます。TLS v1 は、Secure Sockets Layer（SSL）に似ています。TLS は、通常の LDAP 接続（ldap://:389）で SSL と同じ暗号化を提供し、安全な接続（ldaps://:636）で動作します。TLS プロトコルは、サーバ証明書を使用して、暗号化された安全な接続を LDAP サーバに提供します。クライアント認証には、クライアント証明書と 1 組の暗号鍵が必要です。

WAAS ソフトウェアでは、ドメイン セキュリティ ポリシー用の *LDAP サーバ署名要求* オプションを「Require signing（署名が必要）」に設定すると、Windows 2003 ドメインでのログイン認証がサポートされます。LDAP サーバ署名機能により、WAE はドメインに参加してユーザを安全に認証できます。

（注）　Windows ドメイン コントローラで LDAP 署名が必要と設定するときは、クライアント WAE にも LDAP 署名を設定する必要があります。LDAP 署名を使用するようにクライアントを設定しないと、サーバとの通信に影響があり、ユーザ認証、グループ ポリシー設定、およびログオン スクリプトが失敗する場合があります。サーバの証明書を持つ Microsoft サーバに認証局サービスをインストールします（［すべてのプログラム］>［管理ツール］>［認証局］）。Microsoft サーバで LDAP サーバ署名要件プロパティを有効にします（［スタート］>［すべてのプログラム］>［管理ツール］>［ドメイン コントローラのセキュリティ ポリシー］）。表示されるウィンドウで、ドロップダウン リストから **[Require signing]** を選択し、**[OK]** をクリックします。

Windows ドメイン コントローラを LDAP 署名が必要と設定する方法については、Microsoft 社のマニュアルを参照してください。

ここでは、次の内容について説明します。

- クライアント WAE 上の LDAP 署名の設定（p.6-27）
- クライアント WAE 上の LDAP サーバ署名の無効化（p.6-29）

クライアント WAE 上の LDAP 署名の設定

Windows 2003 ドメイン コントローラで、クライアント（WAE など）に LDAP 要求に署名することを要求するセキュリティ設定を構成できます。署名のないネットワーク トラフィックは、途中で傍受されたり、改変される場合があり、一部の組織は、LDAP サーバでの中間者攻撃を防止するために LDAP サーバ署名を義務付けています。LDAP 署名は、個別の WAE 単位で設定できます。システム レベルでは設定できません。さらに、WAAS CLI を使用して WAE 上の LDAP 署名を設定する必要があります。WAAS GUI（WAAS Central Manager GUI または WAE Device Manager GUI）では、LDAP 署名を設定できません。

デフォルトで、LDAP サーバ署名は、WAE で無効になっています。WAE でこの機能を有効にするには、次の手順に従ってください。

ステップ 1　WAE で LDAP サーバ署名を有効にします。

```
WAE# configure terminal
WAE(config)# smb-conf section "global" name "ldap ssl" value "start_tls"
```

ステップ 2　WAE で設定を保存します。

```
WAE(config)# exit
WAE# copy run start
```

ステップ 3　WAE で、現在動作している LDAP クライアントの設定を確認します。

```
WAE# show smb-conf
```

ステップ 4　WAE を Windows ドメインに登録します。

```
WAE# windows-domain diagnostics net "ads join -U Administrator%password"
```

ステップ 5　WAE でユーザ ログイン認証を有効にします。

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

ステップ 6　WAE でユーザ ログイン許可を有効にします。

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

ステップ 7　WAE でログインの認証と許可の現在の設定を確認します。

```
WAE# show authentication user
Login Authentication:    Console/Telnet/Ftp/SSH Session
-------------------------- ------------------------------
local                                enabled (secondary)
Windows domain           enabled (primary)
Radius                             disabled
Tacacs+                           disabled

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

これで、WAE は、Active Directory ユーザを認証するように設定されています。Active Directory ユーザは、Telnet、FTP、または SSH を使用して WAE に接続できます。また、WAAS GUI（WAAS Central Manager GUI または WAE Device Manager GUI）を使用して WAE にアクセスできます。

ステップ 8　Windows ドメイン ユーザ認証に関係する統計情報を表示します。ユーザ認証が行われるたびに、統計情報が追加されます。

```
WAE# show statistics windows-domain
Windows Domain Statistics
  ----------------------------------------------
  Authentication:
    Number of access requests:                    9
    Number of access deny responses:              3
    Number of access allow responses:             6
  Authorization:
    Number of authorization requests:             9
    Number of authorization failure responses:    3
    Number of authorization success responses:    6
  Accounting:
    Number of accounting requests:                0
    Number of accounting failure responses:       0
    Number of accounting success responses:       0

WAE# show statistics authentication
    Authentication  Statistics
    -------------------------------------
    Number of access requests:        9
    Number of access deny responses:  3
    Number of access allow responses: 6
```

ステップ 9　WAE に関する統計情報を消去するには、**clear statistics** EXEC コマンドを使用します。

- すべてのログイン認証統計情報を消去するには、**clear statistics authentication** EXEC コマンドを入力します。
- Windows ドメイン認証に関係する統計情報だけを消去するには、**clear statistics windows-domain** EXEC コマンドを入力します。
- すべての統計情報を消去するには、**clear statistics all** EXEC コマンドを入力します。

クライアント WAE 上の LDAP サーバ署名の無効化

WAE 上の LDAP サーバ署名を無効にするには、次の手順に従ってください。

ステップ 1　Windows ドメインから WAE の登録を解除します。

```
WAE# windows-domain diagnostics net "ads leave -U Administrator"
```

ステップ 2　ユーザ ログイン認証を無効にします。

```
WAE# configure
WAE(config)# no authentication login windows-domain enable primary
```

ステップ 3　WAE で LDAP サーバ署名を無効にします。

```
WAE(config)# no smb-conf section "global" name "ldap ssl" value "start_tls"
```

WAAS デバイス用の管理ログイン認証および許可方式の有効化

この項では、WAAS デバイスまたはデバイス グループ用のさまざまな管理ログイン認証および許可方式（認証設定）を集中的に有効にする方法について説明します。

注意　ローカル認証および許可を無効にする前に、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。ローカル認証が無効で、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、WAAS デバイスにログインできないことがあります。

デフォルトで、WAAS デバイスは、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。WAAS デバイスは、すべての認証データベースが無効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、「管理ログインの認証および許可のデフォルト設定」（p.6-5）を参照してください。

（注）　これらの設定を構成し、送信する前に、WAAS デバイス（またはデバイス グループ）用の TACACS+、RADIUS、または Windows サーバ設定を構成する必要があります。WAAS デバイスまたはデバイス グループでこれらのサーバ設定を構成する方法については、「TACACS+ サーバ認証設定の構成」（p.6-17）、「RADIUS サーバ認証設定の構成」（p.6-14）、および「Windows ドメイン サーバ認証設定の構成」（p.6-19）を参照してください。

デフォルトで、WAAS デバイスは、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。WAAS Central Manager GUI を使用して、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します。

- WAAS デバイス用のデフォルトを変更するには、**[My WAN] > [Manage Devices]** を選択します。デフォルトのログイン認証フェールオーバー方式を変更したい WAAS デバイスの名前の横にある **[Edit]** アイコンをクリックし、ナビゲーション ペインから **[Admin] > [Authentication] > [Authentication Methods]** を選択します。表示されるウィンドウで **[Failover to next available authentication method]** ボックスを選択し、**[Submit]** をクリックします。
- デバイス グループのデフォルトを変更するには、**[My WAN] > [Manage Device Groups]** を選択します。デフォルトのログイン認証フェールオーバー方式を変更したい WAAS デバイスの名前の横にある **[Edit]** アイコンをクリックし、ナビゲーション ペインから **[Admin] > [Authentication] > [Authentication Methods]** を選択します。表示されるウィンドウで **[Failover to next available authentication method]** ボックスを選択し、**[Submit]** をクリックします。

[failover to next available authentication method] オプションを有効にすると、WAAS デバイス（またはデバイス グループ内のデバイス）は、認証が失敗した場合でなく、管理ログイン認証サーバに到達できない場合のみ、認証が何らかの別の理由で失敗した場合を除いて、次の認証方式を照会します。

（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。

[failover to next available authentication method] オプションが *enabled*（有効）の場合は、次のガイドラインに従ってください。

- WAAS デバイス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。
- WAAS デバイス（またはデバイス グループ内のデバイス）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。
- 認証と許可（設定）の両方のセカンダリ方式として、ローカル データベース方式を設定します。

たとえば、[failover to next available authentication method] オプションが有効で、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. WAAS デバイス（またはデバイス グループ内のデバイス）は、管理ログイン要求を受信すると、外部の RADIUS 認証サーバを照会します。
2. 次のどちらかが実行されます。
   a. RADIUS サーバが到達可能である場合、WAAS デバイス（またはデバイス グループ内のデバイス）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、WAAS デバイス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会して）、管理者の認証を試みます。

（注）　ローカル データベースは、この RADIUS サーバが使用できない場合のみ、認証だけのためにアクセスされます。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）は、認証のためにローカル データベースはアクセスされません。

逆に、[failover to next available authentication method] オプションが *disabled*（無効）の場合は、WAAS デバイス（またはデバイス グループ内のデバイス）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にアクセスします。

すべての認証データベースの使用が有効になっている場合は、フェールオーバーの理由に基づき、選択された優先順位の順番で、すべてのデータベースが照会されます。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で照会されます。たとえば、最初にプライマリ認証データベースが照会され、次にセカンダリ認証データベースが照会され、最後に第 3 のデータベースが照会されます。

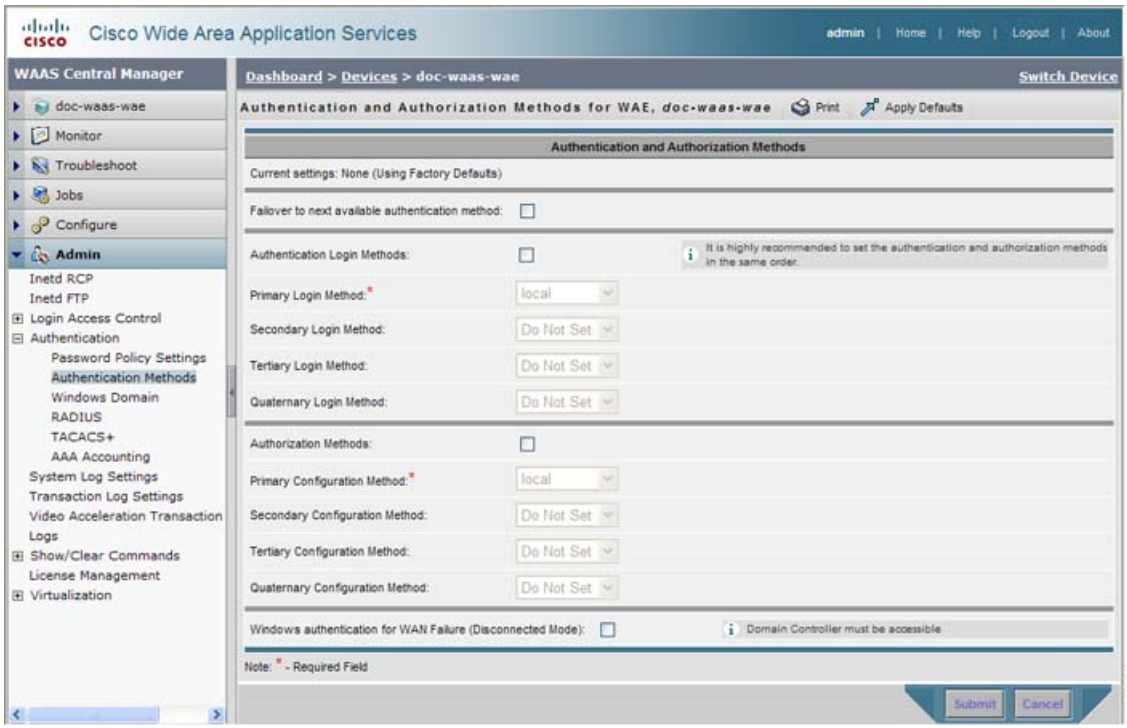
WAAS デバイスまたはデバイス グループ用のログイン認証および許可方式を指定するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインから、**[My WAN] > [Manage Devices]**（または **[Manage Device Groups]**）を選択します。

ステップ 2　設定したいデバイス（またはデバイス グループ）の横にある **[Edit]** アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、**[Admin] > [Authentication] > [Authentication Methods]** を選択します。[Authentication and Authorization Methods] ウィンドウが表示されます（図 6-7 を参照）。

図 6-7　[Authentication and Authorization Methods] ウィンドウ



ステップ 4　**[Failover to next available authentication method]** チェック ボックスを選択して、1 次認証サーバに到達できない場合のみ 2 次認証データベースを照会します。

この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。認証と許可（設定）の両方の 2 次方式として、必ず、ローカル方式を設定してください。

ステップ 5　**[Authentication Login Methods]** チェック ボックスを選択して、ローカル、TACACS+、RADIUS、または Windows データベースを使用して認証特権を有効にします。

ステップ 6　選択したデバイスまたはデバイス グループが使用するログイン認証方式の順序を指定します。

a. [Primary Login Method] ドロップダウン リストから、**[local]**、**[TACACS+]**、**[RADIUS]**、または **[WINDOWS]** を選択します。このオプションは、選択したデバイス（またはデバイス グループ）が、管理ログイン認証に使用する必要がある最初の方式を指定します。

b. [Secondary Login Method] ドロップダウン リストから、**[local]**、**[TACACS+]**、**[RADIUS]**、または **[Windows]** を選択します。このオプションは、最初の方式が失敗した場合に、選択したデバイス（またはデバイス グループ）が管理ログイン認証に使用する必要がある方式を指定します。

c. [Tertiary Login Method] ドロップダウン リストから、**[local]**、**[TACACS+]**、**[RADIUS]**、または **[Windows]** を選択します。このオプションは、最初の方式と第 2 の方式が失敗した場合に、選択したデバイス（またはデバイス グループ）が管理ログイン認証に使用する必要がある方式を指定します。

d. [Quaternary Login Method] ドロップダウン リストから、**[local]**、**[TACACS+]**、**[RADIUS]**、または **[Windows]** を選択します。このオプションは、最初の方式、第 2 の方式、および第 3 の方式が失敗した場合に、選択したデバイス（またはデバイス グループ）が管理ログイン認証に使用する必要がある方式を指定します。

（注）　ログイン認証方式と許可方式の優先順位リストの最後の方式として、ローカル方式を指定することを強く推奨します。この方法に従うことで、指定した外部のサードパーティ サーバ（TACACS+、RADIUS、または Windows ドメイン サーバ）に到達可能できない場合でも、WAAS 管理者は、ローカル認証方式と許可方式を使用して WAAS デバイスにログインできます。

ステップ 7　**[Authentication Methods]** チェック ボックスを選択して、ローカル、TACACS+、RADIUS、または Windows データベースを使用して認証特権を有効にします。

（注）　許可特権は、コンソールと Telnet の接続試行、安全な FTP（SFTP）セッション、およびセキュア シェル（SSH、バージョン 1 およびバージョン 2）セッションに適用されます。

ステップ 8　選択したデバイス（またはデバイス グループ）が使用する必要があるログイン許可（設定）方式の順序を指定します。

（注）　管理ログインの認証方式と許可方式を同じ順序で設定することを強く推奨します。たとえば、管理ログイン認証と許可の両方の 1 次ログイン方式として RADIUS を使用し、2 次ログイン方式として TACACS+ を使用し、第 3 の方式として Windows を使用し、第 4 の方式としてローカル方式を使用するように、WAAS デバイスを設定します。

a. [Primary Configuration Method] ドロップダウン リストから、**[local]**、**[TACACS+]**、**[RADIUS]**、または **[WINDOWS]** を選択します。このオプションは、選択したデバイス（またはデバイス グループ）が、管理特権を決定するために使用する必要がある最初の方式を指定します。

（注） （ステップ 4 で）**[Failover to next available authentication method]** チェック ボックスを選択した場合は、必ず、[Primary Configuration Method] ドロップダウン リストから **[TACACS+] または [RADIUS]** を選択して、1 次許可（設定）方式として TACACS+ または RADIUS 方式を設定してください。

b. [Secondary Configuration Method] ドロップダウン リストから、**[local]**、**[TACACS+]**、**[RADIUS]**、または **[WINDOWS]** を選択します。このオプションは、最初の方式が失敗した場合に、選択したデバイス（またはデバイス グループ）が管理特権を決定するために使用する必要がある方式を指定します。

（注） （ステップ 4 で）**[Failover to next available authentication method]** チェック ボックスを選択した場合は、必ず、[Secondary Configuration Method] ドロップダウン リストから **[local]** を選択して、2 次許可（設定）方式として ローカル方式を設定してください。

c. [Tertiary Configuration Method] ドロップダウン リストから、**[local]**、**[TACACS+]**、**[RADIUS]**、または **[WINDOWS]** を選択します。このオプションは、最初の方式と第 2 の方式が失敗した場合に、選択したデバイス（またはデバイス グループ）が管理特権を決定するために使用する必要がある方式を指定します。

d. [Quaternary Login Method] ドロップダウン リストから、**[local]**、**[TACACS+]**、**[RADIUS]**、または **[WINDOWS]** を選択します。このオプションは、最初の方式、第 2 の方式、および第 3 の方式が失敗した場合に、選択したデバイス（またはデバイス グループ）が管理特権を決定するために使用する必要がある方式を指定します。

ステップ 9　**[Windows authentication for WAN Failure (Disconnected Mode)]** チェック ボックスを選択して、切断モードでの内容要求認証を有効にします。切断モードは、WAFS レガシー モードを使用している場合にのみ使用できます。

この機能を有効にすると、Windows ドメイン サーバは、切断モードで内容要求を認証します。デフォルトで、この機能は、WAE で無効になっています。

この機能を有効にする場合は、WAE 用の自動アカウント パスワード変更を無効にすることを推奨します。詳細については、「Edge WAE 用の自動マシン アカウント パスワード変更の無効化」（p.6-26）を参照してください。

（注） 切断モードに対する Windows 認証は、「Windows ドメイン サーバ認証設定の構成」（p.6-19）の説明に従って、NTLM を [Windows Domain setting] ウィンドウで共有認証方式として選択した場合のみ動作します。

ステップ 10　**[Submit]** をクリックして、設定を保存します。

（注）　Windows 認証方式を有効にした場合は、アクティブになるまで約 15 秒かかります。Windows 認証ステータスの確認や、Windows 認証が必要な操作を実行するまでに、少なくとも 15 秒待ってください。

CLI からログイン認証および許可方式を設定するには、**authentication** グローバル設定コマンドを使用できます。デバイスに対して Windows ドメイン認証および許可方式を有効にする前に、デバイスを Windows ドメイン コントローラで登録する必要があります。

WAAS デバイス用の AAA アカウンティングの設定

アカウンティングは、すべてのユーザの操作と操作が行われた日時を追跡します。監査証跡または接続時間やリソース使用量（転送バイト数）の課金に使用できます。デフォルトで、アカウンティングは、無効になっています。

WAAS アカウンティング機能は、TACACS+ サーバ ログ機能を使用します。アカウンティング情報は、TACACS+ サーバだけに送信されます。コンソールや他のデバイスには送信されません。WAAS デバイスの syslog ファイルは、アカウンティング イベントをローカルに記録します。syslog に保存されるイベントの形式は、アカウンティング メッセージの形式と異なります。

TACACS+ プロトコルを使用すると、WAAS デバイスと中央サーバの間で、AAA 情報を効率的に通信できます。TACACS+ プロトコルは、TCP を使用して、クライアントとサーバの間に信頼できる接続を確立します。WAAS デバイスは、認証および許可要求とアカウンティング情報を TACACS+ サーバへ送信します。

（注）　WAAS デバイス用の AAA アカウンティング設定を構成する前に、WAAS デバイス用の TACACS+ サーバ設定を構成する必要があります（「TACACS+ サーバ認証設定の構成」[p.6-17] を参照してください）。

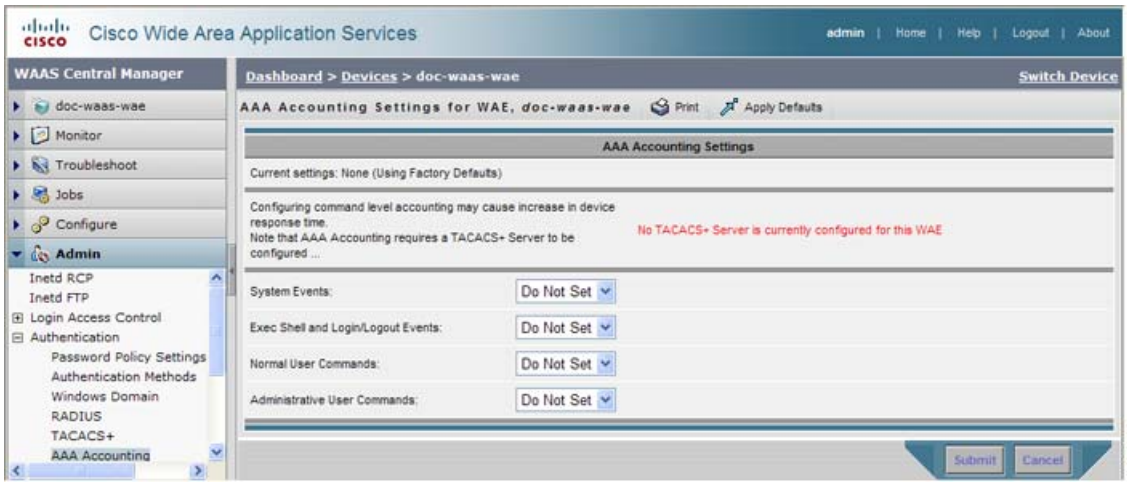
WAAS デバイスまたはデバイス グループ用の AAA アカウンティング設定を集中的に構成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager GUI ナビゲーション ペインから、**[My WAN] > [Manage Devices]**（または **[Manage Device Groups]**）を選択します。

ステップ 2　設定したいデバイス（またはデバイス グループ）の横にある **[Edit]** アイコンをクリックします。

ステップ 3　ナビゲーション ペインで、**[Admin] > [Authentication] > [AAA Accounting]** を選択します。[AAA Accounting Settings] ウィンドウが表示されます（図 6-8 を参照）。

図 6-8　[AAA Accounting Settings] ウィンドウ



ステップ 4　[System Events] ドロップダウン リストから、選択したデバイス（またはデバイス グループ）がシステム レベルイベントを追跡する必要がある場合を指定する、ユーザに関連していない [reloads] のようなキーワードを選択して、システム イベント用のアカウンティングをアクティブにします。

ステップ 5　[Exec Shell and Login/Logout Events] ドロップダウン リストから、選択したデバイス（またはデバイス グループ）が EXEC シェルおよびユーザのログインとログアウト イベントを追跡する必要がある場合を指定するキーワードを選択して、EXEC モード プロセス用のアカウンティングをアクティブにします。レポートには、ユーザ名、日付、開始時刻と終了時刻、および WAAS デバイスの IP アドレスが記載されます。

ステップ 6　[Normal User Commands] ドロップダウン リストから、選択したデバイス（またはデバイス グループ）が通常のユーザ特権レベル（特権レベル 0）でのすべてのコマンドを追跡する必要がある場合を指定するキーワードを選択して、superuser でない管理（通常のユーザ）レベルでのすべてのコマンド用のアカウンティングをアクティブにします。

ステップ 7　[Administrative User Commands] ドロップダウン リストから、選択したデバイス（またはデバイス グループ）が superuser 特権レベル（特権レベル 15）でのすべてのコマンドを追跡する必要がある場合を指定するキーワードを選択して、superuser 管理レベルでのすべてのコマンド用のアカウンティングをアクティブにします。

注意　**wait-start** オプションを使用する前に、WAAS デバイスが TACACS+ サーバで設定され、正常にサーバにアクセスできることを確認してください。WAAS デバイスは、設定されている TACACS+ サーバにアクセスできない場合応答しなくなることがあります。

表 6-2 に、イベントの種類のオプションについて説明します。

表 6-2　AAA アカウンティング用のイベントの種類

GUI パラメータ	機能
イベントの種類のオプション	
stop-only	WAAS デバイスは、指定されたアクティビティまたはイベントの終わりに、停止レコード アカウンティング通知を TACACS+ アカウンティング サーバへ送信します。
start-stop	WAAS デバイスは、イベントの最初に開始レコード アカウンティング通知、イベントの終わりに停止レコード アカウンティング通知を TACACS+ アカウンティング サーバへ送信します。 開始アカウンティング レコードは、バックグラウンドで送信されます。開始アカウンティング レコードが TACACS+ アカウンティング サーバによって受信応答されたかどうかに関係なく、要求されたユーザ サービスが開始します。
wait-start	WAAS デバイスは、開始アカウンティング レコードと停止開始アカウンティング レコードの両方を TACACS+ アカウンティング サーバへ送信します。ただし、要求されたユーザ サービスは、開始アカウンティング レコードが受信応答されるまで開始しません。停止アカウンティング レコードも送信されます。
Do Not Set	指定したイベント用のアカウンティングが無効になります。

ステップ 8　**[Submit]** をクリックして、設定を保存します。

CLI から AAA アカウンティング設定を構成するには、**aaa accounting** グローバル設定コマンドを使用できます。

監査証跡ログの表示

WAAS Central Manager デバイスは、システムでのユーザの操作をログに記録します。ログに記録される唯一の操作は、WAAS ネットワークを変更する操作です。WAAS システムでユーザの操作の記録を表示する詳細については、「監査証跡ログの表示」（p.16-39）を参照してください。