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 Services（WAAS）デバイス用の管理ログインの認証、許可、アカウンティング（AAA）を設定する方法について説明します。

この章の内容は、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 アカウントとロールに基づくアカウント）を一元的に作成し、管理します。詳細については、第 8 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 という用語は、WAE アプライアンス、WAE ネットワーク モジュール（NME-WAE ファミリのデバイス）、および WAAS を実行する SM-SRE モジュールを指します。

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、モニタ、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、そのユーザのユーザ名、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に対して次の認証、許可、アカウンティング（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。ネットワーク内で認証されたユーザに対して権限を許可または拒否します。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作業を追跡する処理です。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.7-32）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 を使用して 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 を使用して、データセンター WAE またはブランチ オフィス 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 サービスとエンティティへのアクセスが許可されます。

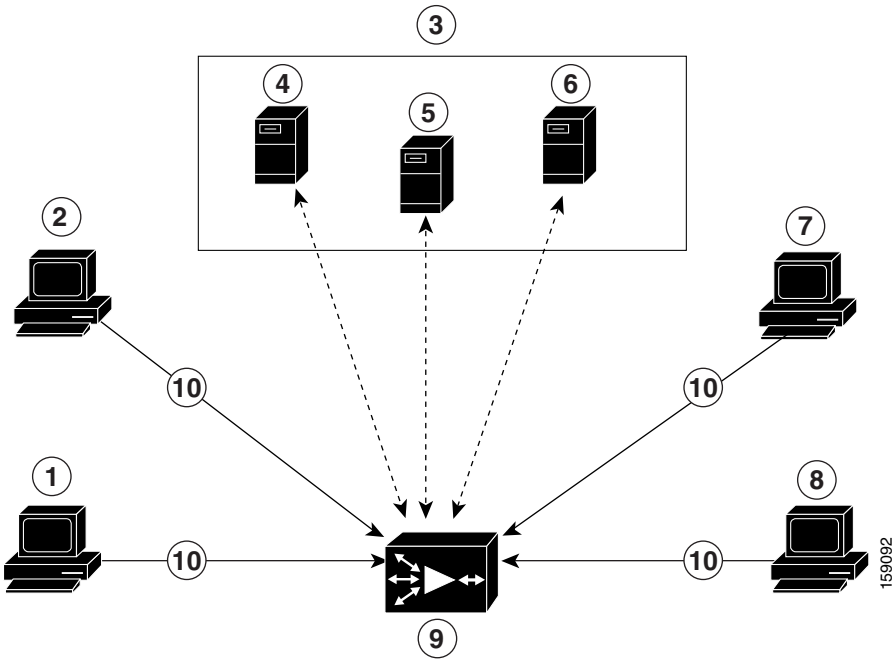
（注）　WAAS デバイスごとに、ユーザ名が admin の 1 つの管理者アカウントが必要です。定義済みの superuser アカウントのユーザ名は変更できません。定義済みの superuser アカウントのユーザ名は admin である必要があります。

WAAS デバイスを初期設定した後で、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 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.8-6）を参照してください。

図 7-1 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）を使用して 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 7-1　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 デバイスへの管理ログイン 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 8 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 でロールベースのユーザまたはユーザ グループのアカウントも作成する必要があります。

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.7-4）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.7-5）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 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	イネーブル
管理設定の許可	イネーブル
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	ディセーブル
TACACS+ ポート	ポート 49
TACACS+ ログイン認証（コンソールおよび Telnet）	ディセーブル
TACACS+ ログイン許可（コンソールおよび Telnet）	ディセーブル
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）	ディセーブル
RADIUS ログイン許可（コンソールおよび Telnet）	ディセーブル
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	ディセーブル
Windows ドメイン ログイン許可	ディセーブル
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に認証に使用される 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。	ヌル ストリング
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	ディセーブル
Kerberos サーバのホスト名または IP アドレス（指定した Kerberos 領域用のキー発行局（KDC）を稼働しているホスト）	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

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
Kerberos ローカル領域（WAAS 用のデフォルト領域）	kerberos-realm：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）	ヌル ストリング

（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.7-5）の説明に従い、WAAS Central Manager GUI を使用してこれらのデフォルト値を変更します。

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 ユーティリティが含まれます。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一元的に設定する場合は、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 デバイスで使用するよう設定するログイン認証方式を決定します（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.7-7）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.7-12）
- 「TACACS+ サーバ認証設定について」（P.7-14）
- 「Windows ドメイン サーバ認証設定の構成」（P.7-16）

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.7-27）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。ローカル認証を無効にし、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、無効な場合は、システムをデフォルトの状態に設定します（表 7-1 を参照）。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。このように指定されていないと、WAAS デバイスで、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に、デフォルトでローカル認証方式と許可方式の段階に進みません。

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 デバイスに対してローカルであり、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な場合に、その他のすべての認証方式を無効にすると、ローカル認証は自動的に再度有効になります。

ローカル ログイン認証は、他の 1 つまたは複数の管理ログイン認証方式を有効にした後でだけ無効にできます。ただし、ローカル ログイン認証が無効な場合は、他のすべての管理ログイン認証方式を無効にしたときに、ローカル ログイン認証が自動的に再度有効になります。コンソール接続と Telnet 接続に異なる管理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、3 次ログイン方式として Windows を使用し、4 次ログイン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。この方法に従うと、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。

この項では、管理ログイン認証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

この項では、WAAS デバイスまたはデバイス グループ用のリモート ログイン設定とアクセス コントロール設定を一元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

セキュア シェル（SSH）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、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、モニタ、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キーの長さ、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 機能を一元的に有効にするには、次の手順に従ってください。

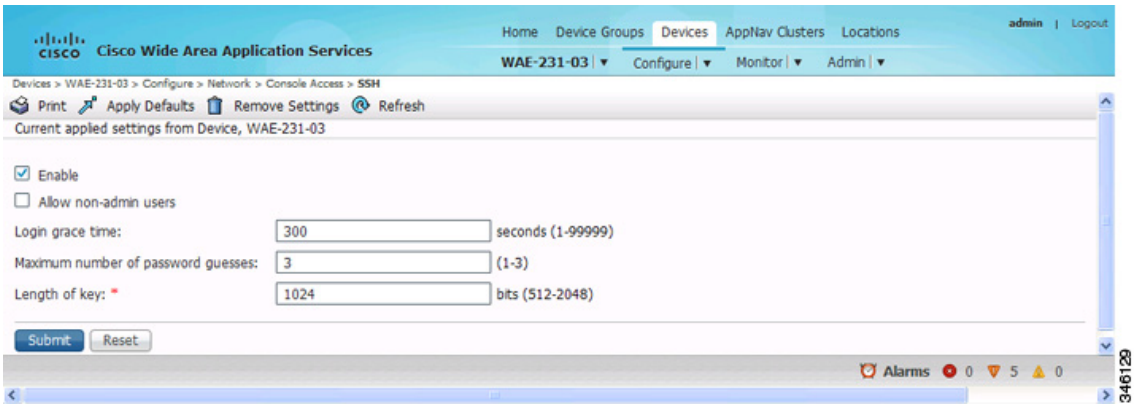
ステップ 1　WAAS Central Manager メニューから、[Devices] > [*device-name*]（または [Device Groups] > [*device-group-name*]）を選択します。

ステップ 2　[Configure] > [Network] > [Console Access] > [SSH] を選択します。

[SSH Configuration] ウィンドウが表示されます （図 7-2 を参照）。

（注）　SSH バージョン 1 プロトコルはサポートされなくなりました。SSH バージョン 2 プロトコルのみが WAAS デバイスによってサポートされます。

図 7-2　[SSH Configuration] ウィンドウ



ステップ 3　[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 4　[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。デフォルトでは、このオプションは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。superuser 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 デバイスだけに制限されています。superuser 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 5　[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 6　[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 セッションでは、3 回のパスワード試行が許可されます。

ステップ 7　[Length of key] フィールドで、SSH キー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、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ホスト キーと公開ホスト キーの両方を必ず生成してください。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 デーモンの公開キーが、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キーを再生成する場合は、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キー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 公開キーで更新されます。

ステップ 8　[Submit] をクリックして、設定を保存します。

デフォルト設定またはデバイス グループ設定の適用後に保存されていない変更がある場合は、[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にだけ表示されます。

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にだけ表示されます。

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 コンフィギュレーション コマンドを使用します。

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に、Telnet セッションを使用してそれ以降の設定作業を行うことができます。

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

（注）　Telnet は、Internet Explorer ではサポートされていません。[Device Dashboard] から [Telnet] ボタンを使用する場合は、異なる Web ブラウザを使用してください。

WAAS デバイスまたはデバイス グループで Telnet サービスを一元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 メニューから、[Devices] > [*device-name*]（または [Device Groups] > [*device-group-name*]）を選択します。

ステップ 2　[Configure] > [Network] > [Console Access] > [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 3　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ために、[Telnet Enable] チェックボックスの選択を解除します。

ステップ 4　[Submit] をクリックして、設定を保存します。

デフォルト設定またはデバイス グループ設定の適用後に保存されていない変更がある場合は、[Current Settings] 行の横に、「Click Submit to Save」メッセージが赤で表示されます。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にだけ表示されます。

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にだけ表示されます。

あとでデバイス（またはデバイス グループ）で Telnet サービスを一元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 コンフィギュレーション 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 コンフィギュレーション 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表示します。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

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 メニューから、[Devices] > [*device-name*] を選択します。

ステップ 2　[Configure] > [Network] > [Console Access] > [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 3　MOTD 設定を有効にするために、[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、およびログイン バナーのフィールドが有効になります。

ステップ 4　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] フィールド、[EXEC Process Creation Banner] フィールド、および [Login Banner] フィールドには、最大 1024 文字を入力できます。改行文字（または Enter キー）は、システムで \n と解釈されるため、2 文字として数えられます。MOTD テキストでは、`、%、^、" 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 5　[EXEC Process Creation Banner] フィールドで、ユーザがデバイスの EXEC シェルに入力したときに 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 6　[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 7　設定を保存するために、[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一元的に設定するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager メニューから、[Devices] > [*device-name*]（または [Device Groups] > [*device-group-name*]）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　[Configure] > [Network] > [Console Access] > [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。デフォルト値は、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。

デフォルト設定またはデバイス グループ設定の適用後に保存されていない変更がある場合は、[Current Settings] 行の横に、「Click Submit to Save」メッセージが赤で表示されます。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にだけ表示されます。

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にだけ表示されます。

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 コンフィギュレーション 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一元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 メニューから、[Devices] > [*device-name*]（または [Device Groups] > [*device-group-name*]）を選択します。

ステップ 2　[Configure] > [Network] > [Console Access] > [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 3　[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 4　[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。設定ミスから回復するには、WAE をリブートし、キャリア検知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 5　[OK] をクリックして作業を続行します。

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 コンフィギュレーション 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めることを決定した場合は、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.7-12）
- 「TACACS+ サーバ認証設定について」（P.7-14）
- 「TACACS+ サーバ設定の構成」（P.7-15）
- 「Windows ドメイン サーバ認証設定の構成」（P.7-16）
- 「LDAP サーバ署名」（P.7-24）

RADIUS サーバ認証設定の構成

RADIUS は、ネットワーク アクセス サーバ（NAS）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、ユーザ データグラム プロトコル（UDP）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。このキー自体は、ネットワーク経由で送信されません。

（注） RADIUS プロトコルの動作方法の詳細については、RFC2138、『*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、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。

複数の RADIUS サーバを設定できる場合は、順番に認証が試みられます。最初のサーバに到達不能の場合、ファーム内のその他のサーバでの認証試行が順に行われていきます。サーバに到達不能という以外の何らかの理由で認証に失敗した場合は、ファーム内の他のサーバでの認証試行は行われません。

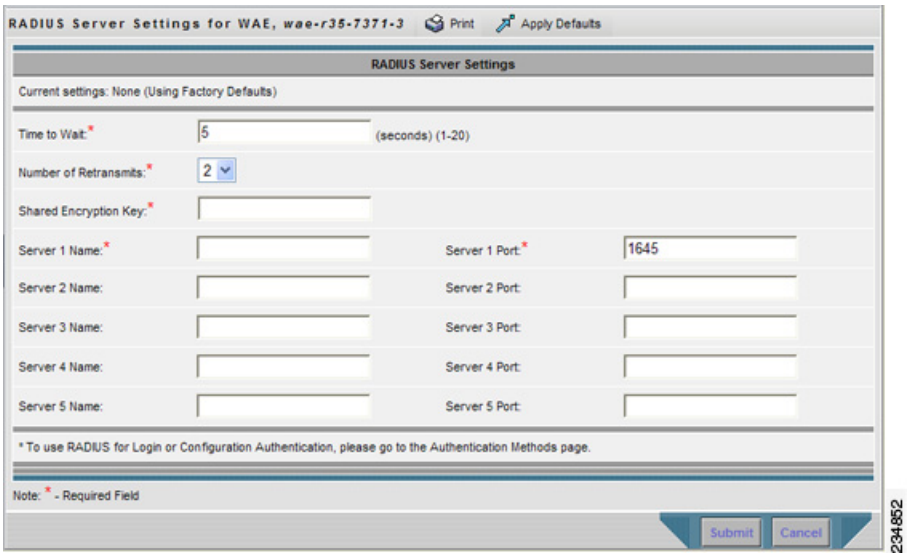
ヒント WAAS Central Manager は、ユーザ認証情報をキャッシュしません。したがって、ユーザは、すべての要求について RADIUS サーバに対して再認証されます。多数の認証要求によるパフォーマンスの低下を防止するには、RADIUS サーバと同じ場所またはできるだけ近くの場所に WAAS Central Manager デバイスを設置して、認証要求をできるだけ迅速に処理するようにします。

WAAS デバイスまたはデバイス グループ用の RADIUS サーバ設定を一元的に構成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager メニューから、[Devices] > [*device-name*]（または [Device Groups] > [*device-group-name*]）を選択します。

ステップ 2　[Configure] > [Security] > [AAA] > [RADIUS] を選択します。[RADIUS Server Settings] ウィンドウが表示されます（図 7-3 を参照）。

図 7-3　[RADIUS Server Settings] ウィンドウ



ステップ 3　[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、タイムアウトするまで 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 4　[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 5　[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キーを入力します。

（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。スペース、左一重引用符（`）、二重引用符（"）、パイプ（|）、または疑問符（?）の文字は使用しないでください。

ステップ 6　[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 7　[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。最小限、1 つのポートを指定する必要があります。5 つの異なるポートが許可されます。

ステップ 8　[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.7-27）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 コンフィギュレーション コマンドを使用できます。

TACACS+ サーバ認証設定について

TACACS+ は、ネットワーク装置と中央データベースの間で Network Access Server（NAS）情報を交換し、ユーザまたはエンティティのアイデンティティを判別することにより、ネットワーク装置に対するアクセスを制御します。TACACS+ は TACACS の拡張バージョンであり、RFC 1492 によって指定された 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安定した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、設定、またはトラブルシューティングのために 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。

ユーザが制限付きのサービスを要求すると、TACACS+ により、MD5 暗号化アルゴリズムに基づいてユーザのパスワード情報が暗号化され、TACACS+ パケット ヘッダーが付加されます。このヘッダー情報には、送信パケット（たとえば認証パケットなど）のタイプ、パケット順序番号、使用されている暗号の種類、パケットの全長が記述されています。次に、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 つのサービスのいずれか、またはすべてを使用できます。

パケットを受信した TACACS+ サーバは、次のように動作します。

- 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。

1 つのプライマリ TACACS+ サーバと 2 つのバックアップ TACACS+ サーバを設定できます。まず、プライマリ サーバで認証試行が行われます。プライマリ サーバに到達不能の場合、ファーム内のその他のサーバでの認証試行が順に行われていきます。サーバに到達不能という以外の何らかの理由で認証に失敗した場合は、ファーム内の他のサーバでの認証試行は行われません。

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、米国国防総省（RFC 1492）の原案から派生したものであり、シスコは非特権モードと特権モードのアクセス コントロールを強化するために 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ーシップに基づいて、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.8-3）を参照）。TACACS+ 設定ファイルで、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。

外部ユーザ グループに基づいてロールおよびドメインをダイナミックに割り当てるには、シェルのカスタム属性をサポートする TACACS+ サーバが必要です。たとえば、これらの属性は Cisco ACS 4.x および 5.1 以降でサポートされています。

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+ サーバと同じ場所またはできるだけ近くの場所に 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+ サーバ設定の構成

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 プロンプトで **enable** EXEC コマンドを入力し、パスワードの入力を求められたときに、admin 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）　このことは、WAAS ユーザがログイン認証に TACACS+ を使用している場合にも適用されます。

WAAS デバイスまたはデバイス グループ用の TACACS+ サーバ設定を一元的に構成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager メニューから、[Devices] > [*device-name*]（または [Device Groups] > [*device-group-name*]）を選択します。

ステップ 2　[Configure] > [Security] > [AAA] > [TACACS+] を選択します。[TACACS+ Server Settings] ウィンドウが表示されます

（注）　AAA Command Authorization が有効になっている場合は、TACACS+ サーバの設定を変更したり削除したりすることはできません。

ステップ 3　認証用に ASCII 形式のパスワードを使用するために、[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 タイプは、パスワード認証プロトコル（PAP）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は、パスワード タイプを ASCII に変更できます。

ステップ 4　[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 5　[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 6　[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キーを入力します。

（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。スペース、左一重引用符（`）、二重引用符（"）、パイプ（|）、シャープ記号（#）、疑問符（?）、またはバックスラッシュ（\）の文字は使用しないでください。キーの長さは 32 文字に制限されています。

ステップ 7　[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。

デフォルト ポート（49）を変更する場合は、[Primary Server Port] フィールドにポートを入力します。

ステップ 8　[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。

デフォルト ポート（49）を変更する場合は、[Secondary Server Port] フィールドにポートを入力します。

ステップ 9　[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。

デフォルト ポート（49）を変更する場合は、[Tertiary Server Port] フィールドにポートを入力します。

（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 10　[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.7-27）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 コンフィギュレーション 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。RADIUS と TACACS+ の認証スキームは、Windows ドメイン認証と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 ドメイン認証が使用されます。

- 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

WAAS Central Manager デバイス、個別の WAAS デバイス、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限り、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。WAAS は、Windows Server 2000、Windows Server 2003、または Windows Server 2008 だけで稼働している Windows ドメイン コントローラによる認証をサポートします。

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」（P.7-17）
- 「Windows ドメイン コントローラからの WAE の登録解除」（P.7-23）

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。

（注） Central Manager がバージョン 4.2.3a 以降で、バージョン 4.2.3 または 4.2.1 を実行している WAAS デバイスで Windows ドメインを設定する場合は、Central Manager で [Windows Domain Server Settings] ページを使用できません。以下の手順の後に説明するように、**windows-domain diagnostics net** CLI コマンドを使用する必要があります。

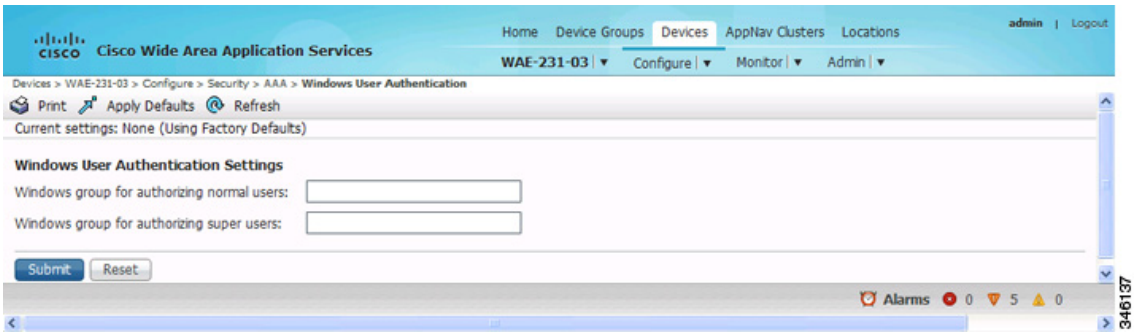
WAAS デバイスまたはデバイス グループ用の Windows ドメイン サーバ設定を構成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager メニューから、[Devices] > [*device-name*]（または [Device Groups] > [*device-group-name*]）を選択します。

ステップ 2　[Configure] > [Security] > [AAA] > [Windows User Authentication] を選択します。[Windows User Authentication] ウィンドウが表示されます。（図 7-4 を参照してください）。

（注） ワークグループ設定は Windows ドメイン認証においてのみ必要です。ドメイン参加には必要ありません。ドメイン参加のみを実行する場合は、ワークグループ設定を省略しても構いません。

図 7-4　[Windows User Authentication]



ステップ 3　[Windows group for authorizing normal users] フィールドで、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、管理者ユーザ アカウントの特権レベルが 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）　デフォルトでは、WAE で設定された Windows ドメイン許可用のユーザ グループは、事前に定義されません。

ステップ 4　[Windows group for authorizing super users] フィールドで、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、管理者ユーザ アカウントの特権レベルが 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。

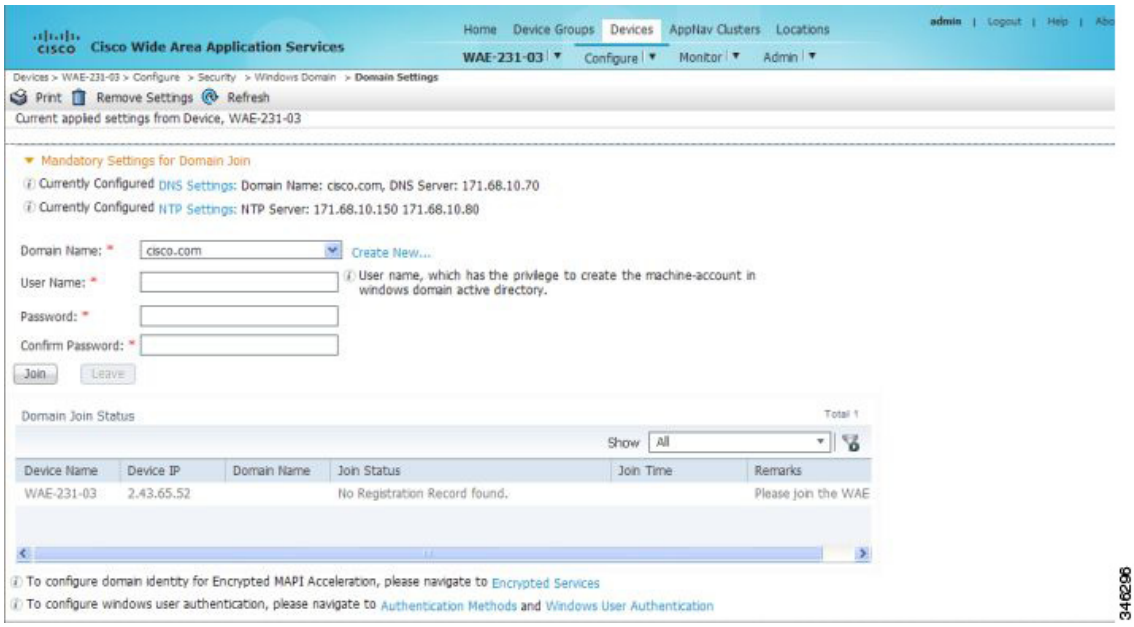
（注）　WAE で Windows ドメイン管理グループを設定することに加えて、Microsoft Windows 2000、2003、または 2008 サーバで Windows ドメイン管理グループを設定する必要があります。Windows ドメイン管理特権ユーザ グループと通常のユーザ グループを作成する必要があります。特権ユーザ グループのグループ スコープが global に設定されていることを確認し、新しく作成した管理グループにユーザ メンバを割り当て、Windows ドメイン特権ユーザ グループにユーザ アカウント（たとえば、winsuper ユーザ）を追加します。Windows サーバで 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 セッションを使用してこの 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 5　WAAS Central Manager メニューから、[Devices] > [*device-name*]（または [Device Groups] > [*device-group-name*]）を選択します。

ステップ 6　[Configure] > [Security] > [Windows Domain] > [Domain Settings] を選択します。[Domain Settings] ウィンドウが表示されます。（図 7-5 を参照してください）。

図 7-5　ドメインの設定



（注）　5.1.1 よりも前の WAAS バージョンでは、関連の WINS サーバとワーク グループまたはドメイン名が選択したデバイス（またはデバイス グループ）に対して定義されていない場合、図 7-5 に示すように、情報メッセージがこのウィンドウの上部に表示され、これらの関連する設定が現在定義されていないことが通知されます。これらの設定を定義するには、[Configure] > [Network] > [WINS] を選択します。

Windows ドメイン参加の場合、ドメイン名、DNS サーバ、および NTP 設定は必須の前提条件になります。Windows ドメイン コントローラと WAAS デバイスでは、Kerberos 認証が成功するために、時間が同期している必要があります。AAA 機能を完全に使用するには、ワークグループおよび WINS サーバも設定する必要があります。

5.1.1 よりも前の WAAS バージョンでは、NetBIOS 名を Windows ドメイン参加のために設定する必要はありません。未設定のままにした場合は、参加中の NetBIOS 名として、ホスト名の最初の 15 文字が自動的に割り当てられます。以降の WAAS バージョンについては、NetBIOS 名、WINS サーバ、およびワークグループの設定は、Windows ドメイン認証の設定のためには必要ではありません。

ステップ 7　ドロップダウン リストからドメイン名を選択するか、または [Create New] をクリックして新しいローカル ドメイン名を作成します。

ステップ 8　WAAS デバイス（またはデバイス グループ）が以前のバージョンのソフトウェアを実行していない場合は、次の手順に進みます。

a.　選択したデバイス（またはデバイス グループ）への管理ログインの共有されたセキュアな認証方式として、[Kerberos] または [NTLM] を選択します。デフォルトの認証プロトコルは Kerberos です。

（注）　WAAS バージョン 5.0.1 以降では、NTLM プロトコルを使用した Windows ドメイン ユーザのログイン認証は推奨されていません。Windows ドメイン ユーザ ログイン認証には、Kerberos プロトコルを使用することを推奨します。

WAAS バージョン 5.1.1 以降では、NTLM プロトコルを使用した Windows ドメイン ユーザ認証はサポートされていません。

暗号化 MAPI アクセラレーションには、Kerberos プロトコルを使用する必要があります。

Kerberos を使用して Kerberos 領域、Kerberos サーバ、およびドメイン コントローラを自動的に取得する場合は、[Auto Detect The Parameters] ボタンをクリックします。ドメイン、DNS、および NTP のパラメータを最初に設定する必要があります。このオプションは NTLM ではサポートされていません。

パラメータについてデバイスを照会すると、成功または失敗を示すステータス メッセージが画面に表示されます。このプロセスは即座には完了しない場合があり、自動検出プロセスが完了するまでステータス メッセージは表示されません。

成功した場合はパラメータを確認し、必要に応じて編集できます。パラメータを確認したら、値を送信できます。

自動検出に失敗した場合は、設定されたドメイン /DNS 設定を確認し、設定を手動で入力する必要があります。その後に、値を送信できます。

（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。

Kerberos 認証を使用した Windows ドメイン参加の場合、発信トラフィック用のファイアウォールで、53 UDP/TCP、88 UDP/TCP、123 UDP、135 TCP、137 UDP、139 TCP、389 UDP/TCP、445 TCP、464 UDP/TCP および 3268 TCP のポートを開いておく必要があります。

Kerberos の場合は、次の手順を省略します。

b. NTLM の場合は、ドロップダウン リストから [version 1] または [version 2] 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。

（注）　暗号化 MAPI アクセラレーションには NTLM を使用できません。

- NTLM バージョン 1 は、Active Directory を使用する Windows 98 や 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 コントローラを使用する場合は、Kerberos の使用を推奨します。
- 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に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にだけ、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。

次の手順は省略します。

c. [Kerberos 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 暗号キー配信局の完全修飾名または IP アドレスを入力します。Kerberos 認証方式の選択時に [Auto Detect The Parameters] ボタンをクリックした場合、これらのフィールドはすでに入力されています。

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。この大文字の使用は、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。

d. [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。

[Submit] をクリックすると、Central Manager が WAAS デバイスに要求を送って（バージョン 4.2.x 以上の場合）ドメイン コントローラ名を解決することにより、この名前を検証します。ドメイン コントローラを解決できない場合は、有効な名前の送信を要求されます。デバイスがオフラインの場合は、デバイス接続の確認を要求されます。デバイス グループを設定している場合、ドメイン コントローラ名は、このページが受け入れられる前に、各デバイスで検証されません。デバイスでドメイン コントローラ名を解決できない場合、このページでの設定の変更は、そのデバイスに適用されません。

e. [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 で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. [User Name] フィールドに、指定した Windows ドメイン コントローラのユーザ名（domain\username またはドメイン名とユーザ名）を入力します。これは、Active Directory における管理権限（コンピュータをドメインに追加する権限）を持つユーザのユーザ名およびパスワードである必要があります。

WAAS デバイス（またはデバイス グループ）が以前のバージョンのソフトウェアを実行している場合は、[Domain Join] タブをクリックする必要があります。NTLM の場合、ユーザ クレデンシャルには Domain Users グループに属するすべての通常のユーザを指定できます。Kerberos の場合、ユーザ クレデンシャルは Domain Admins グループに属するユーザにする必要がありますが、システムのデフォルト Administrator ユーザにする必要はありません。

（注）　Windows ドメイン サーバ認証を使用するには、WAAS デバイスは Windows ドメインに参加する必要があります。登録のためには、Windows ドメインにマシンを参加させる権限があるユーザ クレデンシャルが必要です。ログ ファイルを含めて、登録に使用されるユーザ クレデンシャルが、クリア テキストで表示されることはまったくありません。WAAS は、Windows Active Directory の構造またはスキーマを変更しません。

（注）　マシン アカウントを使用する暗号化 MAPI アクセラレーションには、ドメイン参加が必要です。

b. [Password] フィールドに、指定した Windows ドメイン コントローラ アカウントの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 コントローラのパスワードを再び入力します。

d. （任意。WAAS デバイス（またはデバイス グループ）が以前のバージョンのソフトウェアを実行している場合）必要に応じて、[Organizational Unit] フィールドに組織単位の名前を入力します（Kerberos 認証の場合のみ）。

e. [Join] ボタンをクリックします。

（注）　[Join] ボタンをクリックすると、WAAS Central Manager は、SSH を使用して、すぐに WAAS デバイス（またはデバイス グループのすべてのデバイス）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 の背後にあり、外部 IP アドレスを持っている場合）、登録要求はデバイス（またはデバイス グループ）によって実行されます。

登録要求のステータスが [Domain Join Status] テーブルに表示されます。

f. WAAS デバイス（またはデバイス グループ）が以前のバージョンのソフトウェアを実行している場合は、[Show Join Status] ボタンをクリックして登録要求のステータスを表示します。

結果が更新されるまでには数秒かかる場合があります。参加要求が失敗すると、結果が [Domain Join Status] テーブルに表示されます。

g. 数分待ってから再試行して、更新された認証ステータスを確認します。

要求が正常に終了した場合は、ドメイン登録ステータスが [Domain Join Status] テーブルに表示されます。

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.7-27）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 ではなく、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 **windows-domain join** および **Kerberos**（共有されたセキュアな認証方式として Kerberos を使用する場合）のコマンドを参照してください。

最初に、**ip** 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、IP ドメイン名および IP ネームサーバを設定する必要があります。

次に、**ntp** 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適切な NTP サーバを設定します。

次に、次のグローバル コンフィギュレーション コマンドを使用して、Windows ドメイン管理のスーパーグループおよび通常のグループを設定します。

```
WAE(config)# windows-domain administrative group super-user group_name
WAE(config)# windows-domain administrative group normal-user group_name
```

次に、次のコマンドを使用して、設定した Windows ドメイン サーバに WAAS デバイスを登録します。

```
WAE# windows-domain join domain-name DomainName user UserName
```

特定の組織ユニットにマシン アカウントを作成するには、次のコマンドを使用します。

```
WAE# windows-domain join domain-name DomainName organization-unit OUName user UserName
```

最後に、次のコマンドを使用して、管理ログイン認証と許可の設定として、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
```

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は、共有されたセキュアな認証方式として Kerberos を使用している限り、WAAS Central Manager から直接登録解除できます。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。

（注） 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。また、暗号化された MAPI でマシン アカウント ドメイン アイデンティティが使用される場合は、ドメインの離脱を実行する前にそのアイデンティティを削除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 メニューから、[Devices] > [*device-name*]（または [Device Groups] > [*device-name*]）を選択します。

ステップ 2　[Configure] > [Security] > [AAA] > [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 7-6（P.7-29）を参照）。

ステップ 3　[Authentication Login Methods] と [Authorization Methods] セクションの下で、WINDOWS に設定されたそれぞれのドロップダウン リストを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.7-27）を参照してください。

ステップ 4　[Submit] をクリックして、設定を保存します。

ステップ 5　[Configure] > [Security] > [Windows Domain] > [Domain Settings] を選択します。WAAS デバイス（またはデバイス グループ）が以前のバージョンのソフトウェアを実行している場合は、[Domain Join] タブをクリックします。

ステップ 6　（任意）管理者のユーザ名とパスワードを [Administrator Username] フィールド、[Password] フィールド、および [Confirm Password] フィールドに入力します。登録解除を行うために、ドメイン コントローラはユーザ名とパスワードを要求します。

ステップ 7　[Leave] ボタンをクリックします。

（注）[Leave] ボタンをクリックすると、WAAS Central Manager は SSH を使用してすぐに登録解除要求を WAAS デバイス（またはデバイス グループ）に送信します。登録解除要求によって、デバイスは指定された Windows ドメイン コントローラから登録解除するよう指示されます。

暗号化 MAPI を設定してマシン アカウントを使用している場合は、デバイスの登録解除要求を行えません。脱退を続行する前に、マシン アカウント アイデンティティを削除する必要があります。

登録解除要求のステータスが [Domain Join Status] テーブルに表示されます。

ステップ 8　WAAS デバイス（またはデバイス グループ）が以前のバージョンのソフトウェアを実行している場合は、数分間待機してから [Show Join Status] ボタンをクリックして登録解除要求のステータスを確認します。

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
```

（注）暗号化された MAPI のマシン アカウント アイデンティティが設定されている場合は、最初に削除する必要があります。マシン アカウント アイデンティティを削除するには、**no windows-domain encryption-service** 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。

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

```
WAE# windows-domain leave user UserName password Password
```

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。

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送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。

トランスポート層セキュリティ（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 組の暗号キーが必要です。

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 署名が必要となるように設定するときは、クライアント WAE でも 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、サーバとの通信が影響を受け、ユーザ認証、グループ ポリシー設定、およびログイン 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（[Programs] > [Administrative Tools] > [Certification Authority]）。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（[Start] > [Programs] > [Administrative Tools] > [Domain Controller Security Policy]）。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 コントローラで LDAP 署名が必要となるように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 上での LDAP 署名の設定」（P.7-25）
- 「クライアント WAE 上の LDAP サーバ署名の無効化」（P.7-26）

クライアント WAE 上での 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、改変される可能性があり、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
WAE(config)# smb-conf section "global" name "ldap ssl" value "yes"
```

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 username%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
```

この時点で、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 CentralManager 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 ユーザ認証に関連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 ドメイン認証に関連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 "yes"
```

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）を一元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.7-4）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+ サーバ認証設定について」（P.7-14）、「RADIUS サーバ認証設定の構成」（P.7-12）、および「Windows ドメイン サーバ認証設定の構成」（P.7-16）を参照してください。

デフォルトでは、WAAS デバイスは、何らかの理由で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 デバイスのデフォルトを変更するには、[Devices] > [*device-name*] を選択し、メニューから [Configure] > [Security] > [AAA] > [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] チェックボックスを選択し、[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、[Device Groups] > [*device-group-name*] を選択し、メニューから [Configure] > [Security] > [AAA] > [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] チェックボックスを選択し、[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、認証が何らかの別の理由で失敗した場合ではなく、管理ログイン認証サーバに到達できない場合にだけ、次の認証方式を照会します。WAAS デバイス上の RADIUS 設定または TACACS+ 設定のキーが正しくないために、認証サーバが到達不能になる場合があります。

複数の TACACS+ サーバまたは RADIUS サーバを設定できる場合は、まずプライマリ サーバで認証が試みられます。プライマリ サーバに到達できなければ、TACACS+ ファームまたは RADIUS ファーム内のその他のサーバでの認証試行が順に行われていきます。サーバに到達不能という以外の何らかの理由で認証に失敗した場合は、ファーム内の他のサーバでの認証試行は行われません。このプロセスは、[Failover to next available authentication method] チェックボックスの設定に関係なく適用されます。

（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. 次のどちらかになります。
   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にだけ、認証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。

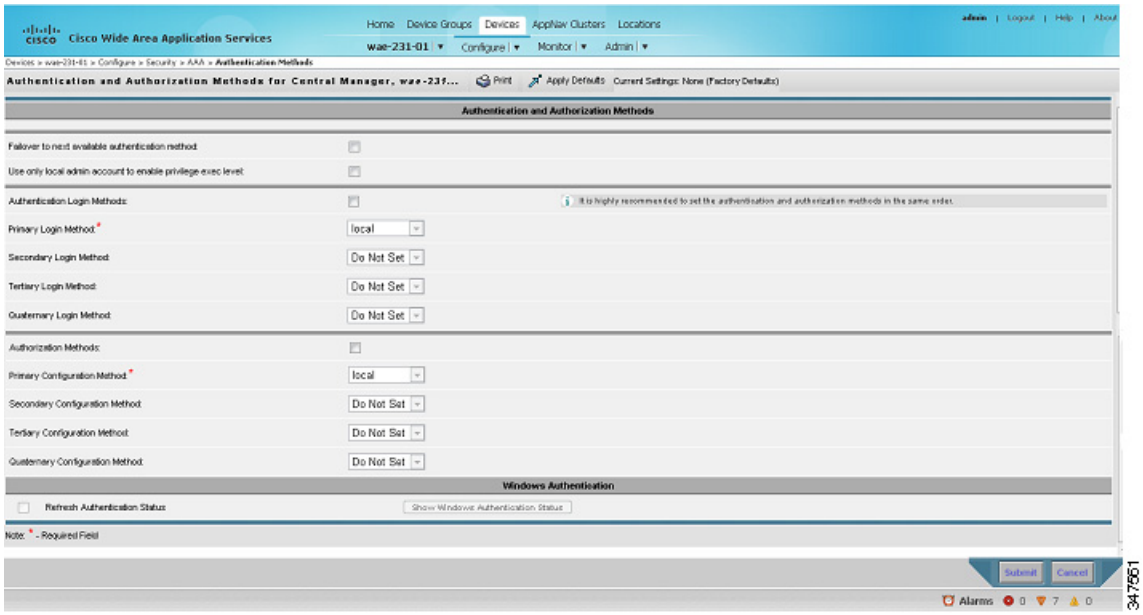
すべての認証データベースの使用が有効になっている場合は、フェールオーバーの理由に基づき、選択された優先順位で、すべてのデータベースが照会されます。フェールオーバーの理由が指定されていない場合は、すべてのデータベースがその優先順位で照会されます。たとえば、最初にプライマリ認証データベースが照会され、次にセカンダリ認証データベースが照会され、次に第 3 のデータベースが照会され、最後に第 4 の認証データベースが照会されます。

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 メニューから、[Devices] > [*device-name*]（または [Device Groups] > [*device-group-name*]）を選択します。

ステップ 2　[Configure] > [Security] > [AAA] > [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 7-6 を参照）。

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



ステップ 3　[Failover to next available authentication method] チェックボックスを選択すると、プライマリ認証サーバが到達不可能な場合にだけ、セカンダリ認証データベースが照会されます。このチェックボックスの選択を解除し、プライマリ認証方式が何らかの理由のために失敗した場合は、他の認証方式が試行されます。

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）の両方のセカンダリ方式として、ローカル方式を設定します。

[Use only local admin account to enable privilege exec level] チェックボックスをオンにして、ローカル admin ユーザのアカウントとパスワードを使用してイネーブル認証を設定します。この場合、イネーブル アクセス要求は、外部認証サーバには送信されませんが、WAE で処理されます。これは、ローカル「admin」ユーザのアカウントとパスワードだけを使用して特定のパスワードを確認し、アクセスできるようにます。

ステップ 4　[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 5　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）がログイン認証を管理するため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）がログイン認証を管理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により、指定した外部サードパーティ サーバ（TACACS+、RADIUS、または Windows ドメイン サーバ）が到達不可能な場合でも、WAAS 管理者は、ローカル認証および許可方式を使用して、WAAS デバイス（またはデバイス グループ内のデバイス）に引き続きログインできます。

ステップ 6 [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、コンソールおよび Telnet 接続試行、セキュア FTP（SFTP）セッション、および Secure Shell（SSH バージョン 2）セッションに適用されます。

ステップ 7 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、許可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 3 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 3 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。

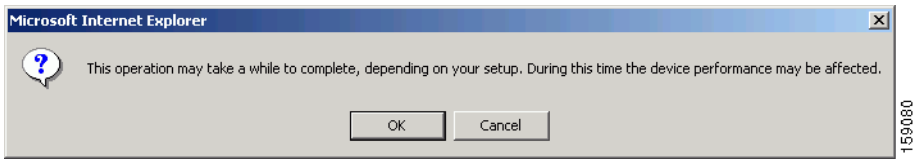
c. [Tertiary Configuration Method] ドロップダウン リストから、[local]、[TACACS+]、[RADIUS]、または [WINDOWS] を選択します。このオプションは、最初の方式と第 2 の方式が失敗した場合に、選択したデバイス（またはデバイス グループ）が管理特権を決定するために使用する必要がある方式を指定します。

d. [Quaternary 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、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 8　認証ステータスを更新するには、ボックスを選択し、[Show Windows Authentication Status] ボタンをクリックします。このオプションを使用できるのは、Windows が認証方式および許可方式として設定されている場合だけです。

認証要求のステータスを更新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 7-7 を参照してください）。

図 7-7　確認ダイアログボックス



[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は、エラー ダイアログを受け取ります。数分待ってから再試行して、更新された認証ステータスを確認します。

ステップ 9　[Submit] をクリックして、設定を保存します。

（注）Windows 認証または許可方式を有効にした場合、Central Manager は、WAE（バージョン 4.2.1 以降）を照会して、Windows ドメインに登録されていることを確認します。これには、[Submit] をクリックした後に最大 1 分かかることがあります。この処理の確認を求めるメッセージが表示されます。処理を進めるには、[OK] をクリックする必要があります。バージョン 4.1.x 以前の WAE またはデバイス グループを設定している場合、Central Manager によって WAE は照会されず、各 WAE が適切に登録されていることを確認する必要があります。システムの動作は不明である（WAE が登録されていない場合）ことを知らせるメッセージが表示され、[OK] をクリックしなければ先に進みません。

（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 コンフィギュレーション 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。

AAA コマンド許可の設定

コマンド許可は、外部 AAA サーバを通じて、CLI ユーザによって実行された各コマンドの許可を行います。CLI ユーザによって実行されたコマンドはすべて、許可されなければ実行されません。RADIUS、Windows ドメイン、およびローカル ユーザは影響を受けません。

（注） CLI インターフェイスを通じて実行されたコマンドだけが、コマンド許可の対象となります。

コマンド許可を有効にする場合は、TACACS+ サーバで「permit null」を指定して、引数のない許可コマンドを実行できるようにする必要があります。

WAAS デバイスまたはデバイス グループのコマンド許可を設定するには、次の手順を実行します。

ステップ 1　WAAS Central Manager メニューから、[Devices] > [*device-name*]（または [Device Groups] > [*device-group-name*]）を選択します。

ステップ 2　[Configure] > [Security] > [AAA] > [Command Authorization Settings] を選択します。[Command Authorization] ウィンドウが表示されます

ステップ 3　[Command Authorization Level] チェックボックスで、必要なレベルをオンにします。

- レベル 0：ユーザのレベル（通常ユーザかスーパー ユーザか）に関係なく、EXEC コマンドだけが、実行される前に TACACS+ サーバによって許可されます。グローバル コンフィギュレーション コマンドは許可されません。
- レベル 15：ユーザのレベル（通常ユーザかスーパー ユーザか）に関係なく、EXEC コマンドとグローバル コンフィギュレーション レベルのコマンドの両方が、実行される前に TACACS+ サーバによって許可されます。

（注） コマンド許可を設定するには、その前に TACACS+ サーバを設定しておく必要があります。

ステップ 4　[Submit] をクリックして、設定を保存します。

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+ サーバ認証設定について」（P.7-14）を参照）。

（注） デバイスに対して AAA アカウンティングを有効にする場合は、コマンド処理中の遅延を回避するために TACACS+ サーバへのアクセスを許可する IP ACL 条件を最初のエントリ位置に作成することを強く推奨します。IP ACL については、第 9 章「WAAS デバイス用の IP ACL の作成および管理」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一元的に構成するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager メニューから、[Devices] > [*device-name*]（または [Device Groups] > [*device-group-name*]）を選択します。

ステップ 2　[Configure] > [Security] > [AAA] > [AAA Accounting] を選択します。[AAA Accounting Settings] ウィンドウが表示されます

ステップ 3　[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）がリロードなどのユーザに関連しないシステム レベル イベントをいつ追跡するかを指定し、イベント用のアカウンティングをアクティブにするキーワードを選択します。

ステップ 4　[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 シェルとユーザ ログインおよびログアウトに関するイベントをいつ追跡するかを指定し、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するキーワードを選択します。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 5　[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）ですべてのコマンドをいつ追跡するかを指定し、superuser でない管理（通常のユーザ）レベルですべてのコマンドのアカウンティングをアクティブにするキーワードを選択します。

ステップ 6　[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）ですべてのコマンドをいつ追跡するかを指定し、superuser 管理ユーザ レベルですべてのコマンドのアカウンティングをアクティブにするキーワードを選択します。

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に、応答しなくなることがあります。

表 7-2 で、イベントの種類のオプションについて説明します。

表 7-2　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了時に、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、イベントの開始時に開始レコード アカウンティング通知、イベントの終了時に停止レコード 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 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。TACACS+ アカウンティング サーバが start アカウンティング レコードを確認したかどうかには関係なく、要求されたユーザ サービスが開始されます。
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 7　[Enable] チェックボックスを選択して、TACACS+ サーバに対する AAA アカウンティングを有効にします。

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 コンフィギュレーション 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.17-58）を参照してください。