



ユーザ アクセスの管理

Guard へのアクセスは、ユーザ プロファイルの作成によって制御します。ユーザが WBM にログインしようとする、Guard がログインユーザ名とパスワードをユーザ プロファイル データベースと照合して、認証します。この章では、WBM を使用してユーザ プロファイルを作成および削除する方法について説明します。

この章は、次の項で構成されています。

- [ユーザ認証方式](#)
- [定義済みのシステム ユーザ プロファイル](#)
- [ユーザ リストの表示](#)
- [ユーザ プロファイルの作成](#)
- [ユーザ プロファイルの削除](#)
- [現在のユーザのパスワードの変更](#)
- [別のユーザのパスワードの変更](#)
- [TACACS+ サーバ上でのユーザ プロファイルの設定](#)

ユーザ認証方式

CLI を使用して Guard をどのように設定したかに応じて、Guard は次のいずれかまたは両方の方式を使用してユーザを認証します。

- ローカル認証：Guard は、Guard のデータベースに格納されているユーザ プロファイル情報と照合してユーザを認証します。ユーザ名ごとに、定義済みの一連のコマンド機能の実行をユーザに許可するためのユーザ特権レベルを、システム管理者が設定します。ローカル ユーザ認証は、WBM を使用して設定します。
- AAA（認証、認可、アカウンティング）サービス：Guard は、1 台以上の TACACS+ サーバのデータベースに格納されているユーザ プロファイル情報と照合してユーザを認証します。AAA サービスは、ユーザ認証とコマンド認可を設定する機能のほかに、ユーザが開始したイベント（Guard の設定変更など）を追跡するためのアカウンティング機能を備えています。Guard 上で AAA サービスをイネーブルにして TACACS+ サーバを定義するには、CLI を使用する必要があります。また、各 TACACS+ サーバもユーザ プロファイル情報を使用して設定する必要があります。

定義済みのシステム ユーザ プロファイル

Guard では、次の 2 つのユーザ プロファイル (システム ユーザ) がローカル データベース上に事前設定されています。

- **admin** : Guard 上で最初に CLI にアクセスするときは、このデフォルト ユーザ名を使用します。このシステム ユーザ プロファイルには、コンソール接続を使用した最初のログイン プロセスでパスワードを割り当てます。管理者としてログインすると、CLI コマンドに完全にアクセスできます。入力した **admin** パスワードは、**admin** ユーザ プロファイルに保存されます。Guard の動作を設定し、他のユーザ プロファイルを作成する場合は、このシステム ユーザ プロファイルを使用します。
- **riverhead** : Cisco Traffic Anomaly Detector は、Guard に最初にアクセスして Cisco Traffic Anomaly Detector と Guard の間に通信チャネルを確立するときに、このユーザ名を使用します。このシステム ユーザ プロファイルには、コンソール接続を使用した最初のログイン プロセスでパスワードを割り当てます。Cisco Traffic Anomaly Detector と Guard の間に最初の通信リンクが確立されると、2 つのデバイスは、以後の通信リンクを確立するときに SSL を使用します。このため、ユーザの操作が不要になります。**riverhead** システム ユーザ プロファイルには、**Dynamic** ユーザ特権レベルが設定されています。

システム ユーザのパスワードは変更できますが、システム ユーザを Guard のデータベースから削除することはできません。

初期設定が完了した後は、ユーザのアクションを監視できるように新しいアカウントを作成し、システム ユーザ アカウントは使用しないことをお勧めします。

ユーザリストの表示

WBM を使用すると、Guard へのアクセスを許可されているユーザのリストを表示できます。ユーザリストでは、ユーザプロファイルを追加または削除できます。ユーザリストは、次の2つのカテゴリに分かれています。

- **System users** : シスコによってあらかじめ定義されているユーザプロファイル。削除することはできません（「[定義済みのシステムユーザプロファイル](#)」の項を参照）。
- **Users** : システム管理者が定義するユーザプロファイル。

Guard へのアクセスを許可されているユーザのリストを表示するには、次の手順を実行します。

-
- ステップ 1** ナビゲーション ペインで **Guard Summary** を選択します。Guard の要約メニューが表示されます。
- ステップ 2** Guard の要約メニューの **Users > Users list** を選択します。Users List が表示されます。
-

ユーザ プロファイルの作成

ローカル データベースにユーザ プロファイルを作成するには、管理者アクセス権が必要です。



(注)

Guard が、ユーザの認証に認証用のローカル サービスと AAA サービス（または AAA サービスのみ）を使用するように設定されている場合は、認証に使用されるユーザ プロファイル情報も各 TACACS+ サーバ上で設定する必要があります（「[TACACS+ サーバ上でのユーザ プロファイルの設定](#)」の項を参照）。

新しいユーザ プロファイルを作成するには、次の手順を実行します。

- ステップ 1 ナビゲーション ペインで **Guard Summary** を選択します。Guard の要約メニューが表示されます。
- ステップ 2 次のいずれかの方法で、Create User 画面を表示します。
 - Guard の要約メニューの **Users > Create user** を選択します。
 - Guard の要約メニューの **Users > Users list** を選択します（Users List が表示されます）。次に、**Add** をクリックします。
- ステップ 3 [表 3-1](#) の説明に従って、ユーザ プロファイルのパラメータを定義します。

表 3-1 ユーザ プロファイルのパラメータ

パラメータ	説明
User name	ユーザ プロファイルの名前。先頭を英字にして、1 ～ 63 文字の英数字文字列を入力します。文字列にスペースを含めることはできませんが、アンダースコア (_) を含めることはできます。
Initial password	ユーザのパスワード。スペースを含めずに、6 ～ 24 文字の英数字文字列を入力します。

表 3-1 ユーザ プロファイルのパラメータ (続き)

パラメータ	説明
Type	<p>ユーザの特権レベル。ユーザの特権レベルを Type ドロップダウン リストから選択します。</p> <ul style="list-style-type: none"> • show : 監視操作と診断操作にアクセスできます。 • dynamic : 監視と診断、検出、およびラーニングに関する操作にアクセスできます。Dynamic 特権を持つユーザは、フレックスコンテンツ フィルタと動的フィルタを設定することもできます。 • config : ユーザ プロファイルの管理を除くすべての WBM 機能にフルアクセスできます。 • admin : すべての WBM 機能にフルアクセスできます。

ステップ 4 次のいずれかのオプションを選択します。

- **OK** : ユーザ プロファイル情報をローカル データベースに保存します。ユーザの詳細画面が表示され、新しいユーザ プロファイルのパラメータが示されます。
- **Clear** : User Form に追加した情報をすべて消去します。
- **Cancel** : 情報を保存せずに Create User 画面を終了します。Users List が表示されます。

ユーザ プロファイルの削除

ユーザ プロファイルを削除すると、認証がローカル ユーザ データベースのみを使用して実行されている場合、関連付けられているユーザが **Guard** にアクセスできなくなります。

ユーザ プロファイルを削除するには、次の手順を実行します。

-
- ステップ 1** ナビゲーション ペインで **Guard Summary** を選択します。Guard の要約メニューが表示されます。
 - ステップ 2** Guard の要約メニューの **Users > Users list** を選択します。Users List が表示されます。
 - ステップ 3** 削除するユーザ名の隣にあるチェックボックスをオンにし、**Delete** をクリックします。表示されているユーザ名をすべて選択して削除するには、User チェックボックスをオンにし、**Delete** をクリックします。削除の確認メッセージが表示されます。
 - ステップ 4** 次のいずれかのオプションを選択します。
 - **OK** : ユーザ プロファイルをローカル データベースから削除します。User List が表示されます。
 - **Cancel** : ユーザ削除要求を無視します。User List が表示されます。
-

現在のユーザのパスワードの変更

WBM を使用すると、すべてのユーザが各自のログインパスワードを変更できます。現在ログインしているユーザのパスワードを変更するには、次の手順を実行します。

-
- ステップ 1 ナビゲーション ペインで **Guard Summary** を選択します。Guard の要約メニューが表示されます。
 - ステップ 2 Guard の要約メニューの **Users > Change Password** を選択します。Change Password 画面が表示されます。
 - ステップ 3 既存のパスワードを Old Password フィールドに入力します。
 - ステップ 4 新しいパスワードを New Password フィールドに入力します。パスワードは、スペースを含まず、6 ~ 24 文字の英数字文字列にする必要があります。
 - ステップ 5 Confirm New Password フィールドで、新しいパスワードを再度入力します。
 - ステップ 6 次のいずれかのオプションを選択します。
 - **OK** : 新しいパスワードを Guard のデータベースのユーザ プロファイルに保存します。Guard の要約画面が表示されます。
 - **Cancel** : 情報を保存せずに Change Password 画面を終了します。Guard の要約画面が表示されます。
-

無効な既存パスワードを入力した場合や Guard が新しいパスワードを確認できない場合は、Guard がエラー メッセージを表示します。**Go Back** をクリックして手順を繰り返してください。

別のユーザのパスワードの変更

WBM を使用すると、admin ユーザ特権レベルを持つユーザは他のユーザに割り当てられているパスワードを変更できます。

別のユーザのパスワードを変更するには、次の手順を実行します。

-
- ステップ 1 ナビゲーション ペインで **Guard Summary** を選択します。Guard の要約メニューが表示されます。
 - ステップ 2 Guard の要約メニューの **Users > Users list** を選択します。Users List が表示されません。
 - ステップ 3 ユーザ名をクリックします。ユーザの詳細画面が表示されます。
 - ステップ 4 **Config** をクリックします。Config User 画面が表示されます。
 - ステップ 5 新しいパスワードを入力します。パスワードは、スペースを含まず、6 ～ 24 文字である必要があります。
 - ステップ 6 次のいずれかのオプションを選択します。
 - **OK**: 新しいパスワードをローカルデータベースのユーザ プロファイルに保存します。User List 画面が表示されます。
 - **Clear**: User Form に追加した情報をすべて消去します。
 - **Cancel**: 情報を保存せずに Config User 画面を終了します。User List 画面が表示されます。
-

TACACS+ サーバ上でのユーザ プロファイルの設定

この項の情報は、TACACS+ サーバ上で WBM ユーザ プロファイル情報を設定する必要がある管理者を対象としています。

定義済みのコマンド グループへのアクセス権を、ユーザ特権レベルによって指定することができます。表 3-2 に、TACACS+ サーバ上で設定できる WBM のコマンドおよびコマンド グループを示します。



(注)

コマンドは、すべて大文字と小文字が区別されます。

表 3-2 WBM のコマンド

特権レベル	TACACS+ コマンド グループ	コマンド
Show	WBM-Show	ChangeLocalOwnPassword
Dynamic	WBM-Dynamic	AcceptPendingDynFilter ActivateZone ConfigExtendedFlexFilter ConfigZoneFlexFilter CreateDynamicFilter DeleteAllDynamicFilters DeleteDynamicFilter RecommendationAccept RecommendationAcceptForever RecommendationIgnore RemoveDynamicFilters ZoneActivation

表 3-2 WBM のコマンド (続き)

特権レベル	TACACS+ コマンド グループ	コマンド
Configuration (config)	WBM-Config	acceptTh ActivatePolicy AddPolicyThreshold AddService AddPolicyThreshold AddZoneIP ChangePolicyState ConfigLearn ConfigPolicies ConfigPolicy ConfigPolicyGroup ConfigPolicyTemplate ConfigPolicyThreshold ConfigZone CopyPacketDump CreateBypassFilter CreateExtendedFlexFilter CreateSnapshot CreateUserFilter CreateUserFilters CreateZone CreateZoneTemplate deactivate DeactivatePolicy

表 3-2 WBM のコマンド (続き)

特権レベル	TACACS+ コマンド グループ	コマンド
Configuration (config) (続き)	WBM-Config (続き)	DeleteBypassFilters DeleteExtendedFlexFilter DeletePacketDump DeletePolicyThreshold DeleteReports DeleteSnapshot DeleteUserFilters DeleteZone DeleteZoneIP DeleteZones DeleteZoneTemplate ExportReports protectIP RemoveService RenamePacketDump SaveAsZone SavePoliciesRecommendations SetFtpServer StartPacketDump
Administration (admin)	WBM-Admin	CreateUser ConfigUser DeleteUsers DeleteUser



(注) 特権レベルを指定すると、その特権レベルに含まれているコマンドに関してのみアクセス権が付与されます。このため、設定機能へのアクセスをイネーブルにするには、**WBM-Dynamic** および **WBM-Config** にアクセスできるユーザ特権レベルを付与する必要があります。

次の例は、WBM の画面に対するユーザ **Robin** のアクセスを、TACACS+ サーバ上で **Dynamic** 特権レベルを指定して定義する方法を示しています。

```
user = Robin
{
cmd = WBM-Show
{
permit .*
}
}
cmd = WBM-Dynamic
{
permit .*
}
cmd = WBM-Config
{
deny .*
}
cmd = WBM-Admin
{
deny .*
} }
```

■ TACACS+ サーバ上でのユーザ プロファイルの設定