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できます。ユーザが WBM にログインしようとすると、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。

この章は、次の項で構成されています。

ユーザの認証および認可の方式について

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および認可します。

- ローカル：Guard は、ユーザ名とパスワードを Guard 自体の内部データベースと照合して認証します。ユーザ名ごとに、定義済みの一連のコマンド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できます。

  ローカルでの認証および認可の方式がデフォルトです。ローカルでのユーザの認証および認可は、WBM を使用して設定します。

- AAA（認証、認可、アカウンティング）：Guard は、1 台以上の TACACS+ サーバに常駐している外部データベースと照合してユーザ名とパスワードを認証します。ローカル認証とは異なり、AAA 認証では、コマンドごとにアクセス権を指定できます。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、アカウンティングを設定する機能も備えています。この機能を使用すると、ユーザが開始したイベント（Guard の設定変更など）を追跡できます。

  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。

定義済みのシステム ユーザ プロファイルの使用

Guard では、次の 2 つのシステム ユーザ プロファイルがローカル 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。初めて Guard にログインしたときは、admin ユーザ プロファイルに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、すべての CLI コマンドおよび WBM のウィンドウにアクセスできます。Guard を設定し、他のユーザ プロファイルを作成する場合は、admin 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、ユーザ名 riverhead を使用します。初めて Guard にログインしたときは、riverhead ユーザ プロファイルに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秘密鍵と公開鍵のペアを使用します。このため、ユーザの操作は必要なくなります。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 では、ローカル ユーザ データベースに定義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 プロファイルの使用」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。

ローカル ユーザ データベースに定義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 ペインの **Guard Summary** をクリックします。Guard の要約メニューが表示されます。

ステップ 2　Guard の要約メニューから **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 ペインの **Guard Summary** をクリックします。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 の要約メニューから **Users > Create user** を選択します。
- Guard の要約メニューから **Users > Users list** を選択し（Users List が表示されます）、**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。アルファベットで始まる 1 ～ 63 文字の英数字の文字列を入力します。大文字と小文字は区別されます。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。スペースを含まない 6 ～ 24 文字の文字列を入力します。大文字と小文字は区別されます。

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	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。 • **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、保護、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 ペインの **Guard Summary** をクリックします。Guard の要約メニューが表示されます。

ステップ 2　Guard の要約メニューから **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。

パスワードの変更

WBM を使用して、ユーザは自分のパスワードを変更できます。管理者は、自分のパスワードと他のユーザのパスワードを変更できます（P.3-9 の「別のユーザのパスワードの変更」を参照）。

自分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 ペインの **Guard Summary** をクリックします。Guard の要約メニューが表示されます。

ステップ 2　Guard の要約メニューから **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、スペースを含まない 6 ～ 24 文字の文字列にする必要があります。大文字と小文字は区別されます。

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、他のユーザのパスワードを変更できます。

他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 ペインの **Guard Summary** をクリックします。Guard の要約メニューが表示されます。

ステップ 2　Guard の要約メニューから **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　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、スペースを含まない 6 ～ 24 文字の大文字と小文字が区別される文字列とします。

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。

ユーザ特権レベルの変更

認可されたユーザは、ユーザ特権レベルを変更できます。

ユーザ特権レベルを変更するには、次の手順を実行します。

ステップ 1　情報領域で **Enable** をクリックします。

Enable Authentication ウィンドウが表示されます。

ステップ 2　Level ドロップダウン リストからユーザ特権レベルを選択します。次のいずれかから選択できます。

- admin：すべての WBM 機能にフル アクセスできます。
- 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。
- dynamic：監視と診断、保護、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。

ステップ 3　Password フィールドに特権レベル パスワードを入力します。

ステップ 4　**OK** をクリックして変更を適用します。

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の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
		acceptTh

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	ActivatePolicy
		AddPolicyThreshold
		AddService
		AddPolicyThreshold
		AddZoneIP
		ChangePolicyState
		ConfigLearn
		ConfigPolicies
		ConfigPolicy
		ConfigPolicies
		ConfigPolicy
		ConfigPolicyGroup
		ConfigPolicyTemplate
		ConfigPolicyThreshold
		ConfigZone
		CopyPacketDump
		CreateBypassFilter
		CreateExtendedFlexFilter
		CreateSnapshot
		CreateUserFilter
		CreateUserFilters
		CreateZone
		CreateZoneTemplate
		deactivate

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）	DeactivatePolicy 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。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 .*
} }
```