ユーザ アクセスの管理

Detector モジュールへのアクセスは、ユーザ プロファイルを作成すること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と、Detector モジュールはユーザ プロファイルのデータベースと照合してログイン ユーザ名とパスワードを認証します。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

Detector モジュールは、ユーザが CLI を使って Detector モジュールを設定する方法に応じて、次の方法のいずれかまたは両方を使用してユーザ認証を実行します。

- ローカル認証：Detector モジュールは、Detector モジュール データベースに存在するユーザ 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 サービス（認証、認可、アカウンティング）：Detector モジュールは、1 つ以上の TACACS+ サーバのデータベースに存在するユーザ プロファイル情報と照合してユーザを認証します。ユーザ認証とコマンド認可の設定に加えて、AAA サービスには、Detector モジュールの設定変更など、ユーザが開始したイベントを追跡できるアカウンティング機能が含まれています。CLI を使用して AAA サービスをイネーブルにし、Detector モジュールに TACACS+ サーバを定義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

Detector モジュールのローカル データベースには、次の 2 つのユーザ プロファイル（システム ユーザ）があらかじめ設定されています。

- admin : Detector モジュールの CLI に初めてアクセスするときに、このデフォルト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。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。このシステム ユーザ プロファイルを使用して、Detector モジュールの動作を設定し、他のユーザ プロファイルを作成します。
- riverhead : Detector モジュールは、Cisco Anomaly Guard Module に初めてアクセスするときに、このユーザ名を使用し、Detector と Cisco Anomaly Guard Module との間に通信チャネルを確立します。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。Detector と Cisco Anomaly Guard Module との間に最初の通信リンクが確立されると、これら 2 つのデバイスは SSL を使用して以降の通信リンクを確立します。このとき、ユーザが介入する必要はありません。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、Detector モジュール データベースからシステム ユーザを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、Detector モジュールへのアクセスが現在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。

Detector モジュールへのアクセスが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、**Detector Summary** を選択します。Detector モジュールの要約メニューが表示されます。

ステップ 2　Detector モジュールの要約メニューの **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）　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）を使用してユーザを認証するように Detector モジュールが設定されている場合、認証の目的で使用される各 TACACS+ サーバにもユーザ プロファイル情報を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、**Detector Summary** を選択します。Detector モジュール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。

- Detector モジュールの要約メニューの **Users > Create user** を選択します。
- Detector モジュールの要約メニューの **Users > Users list** を選択してから（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。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。
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、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

ローカル ユーザ データベースだけを使用して認証が実行される場合、ユーザ プロファイルを削除すると、そのプロファイルに関連付けられているユーザが Detector モジュール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、**Detector Summary** を選択します。Detector モジュールの要約メニューが表示されます。

ステップ 2　Detector モジュールの要約メニューの **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、**Detector Summary** を選択します。Detector モジュールの要約メニューが表示されます。

ステップ 2　Detector モジュールの要約メニューの **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 Detector モジュール データベースのユーザ プロファイルに保存します。Detector モジュール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。Detector モジュールの要約画面が表示されます。

現在無効のパスワードを入力した場合、または Detector モジュールが新しいパスワードを確認できない場合、Detector モジュールはエラー 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、**Detector Summary** を選択します。Detector モジュールの要約メニューが表示されます。

ステップ 2　Detector モジュールの要約メニューの **Users > Users list** を選択します。Users List が表示されます。

ステップ 3　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

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
		ConfWormSrcIPs
		ConfigZone
		CopyPacketDump
		CreateBypassFilter
		CreateExtendedFlexFilter
		CreateSnapshot
		CreateUserFilter
		CreateUserFilters
		CreateZone

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）	CreateZoneTemplate
		deactivate
		DeactivatePolicy
		DeleteBypassFilters
		DeleteExtendedFlexFilter
		DeletePacketDump
		DeletePolicyThreshold
		DeleteReports
		DeleteSnapshot
		DeleteUserFilters
		DeleteZone
		DeleteZoneIP
		DeleteZones
		DeleteZoneTemplate
		ExportReports
		protectIP
		RemoveService
		RenamePacketDump
		SaveAsZone
		SavePoliciesRecommendations
		SetFtpServer
		StartPacketDump

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
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 .*
} }
```