



WBM の起動とカスタマイズ

Guard WBM にアクセスするには、まず CLI を使用して WBM のネットワーク アクセスを設定する必要があります。

この章は、次の内容で構成されています。

- [WBM のネットワーク アクセスの設定](#)
- [WBM の起動](#)
- [ログイン バナーの設定](#)
- [WBM ロゴの設定](#)

WBM のネットワーク アクセスの設定

WBM サービスをイネーブルにし、WBM から Guard へのネットワーク アクセスを許可するには、Guard の CLI を使用します。必要な設定変更を行うには、Administration ユーザ特権レベルまたは Configuration ユーザ特権レベルの権限を持つユーザとしてログインする必要があります。Guard の CLI へのアクセスと使用の詳細については、『Cisco Guard Configuration Guide』を参照してください。

WBM のネットワーク アクセスを設定するには、次の手順を実行します。

ステップ 1 コンソールまたは Secure Shell (SSH) 接続を使用して、Guard の CLI にログインします。

ステップ 2 次のコマンドをグローバル モードで入力して、設定モードに入ります。

```
admin@GUARD# configure
```

ステップ 3 次のコマンドを入力して、WBM サービスをイネーブルにします。

```
admin@GUARD-conf# service wbm
```

ステップ 4 次のコマンドを入力して、WBM から Guard へのアクセスを許可します。

```
admin@GUARD-conf# permit wbm ip-addr [ip-mask]
```

引数 *ip-addr* および *ip-mask* は、WBM から接続するときの接続元 IP アドレスを定義します。

次の例は、IP アドレス 192.168.30.32 を使用して接続する WBM のネットワーク アクセスを設定する方法を示しています。

```
admin@GUARD# configure
admin@GUARD-conf# service wbm
admin@GUARD-conf# permit wbm 192.168.30.32
```

Guard 上で WBM のネットワーク アクセスを設定した後は、CLI を終了し、Web ブラウザを使用して WBM を起動することができます。

WBM の起動

WBM を起動するには、次の手順を実行します。

- ステップ 1** Web ブラウザを開いて、Secure HTTP (HTTPS) を使用して Guard の IP アドレスを入力します。

```
https://Guard-ip-address/
```

Guard-ip-address 引数は、Guard の管理用 IP アドレスです。

Guard WBM のログイン ウィンドウが表示されます。

- ステップ 2** ユーザ名とパスワードを入力し、**OK** をクリックします。WBM のホーム ページが表示されます。



(注) TACACS+ 認証が設定されている場合、ユーザ認証にはローカル データベースではなく、TACACS+ ユーザ データベースが使用されます。TACACS+ サーバ上に詳細な認証アトリビュート (パスワードの有効期限など) が設定されている場合、Guard は、TACACS+ サーバ上のユーザの設定に基づいて、ユーザに新しいパスワードを要求したり、パスワードの有効期限が近づいたときに通知したりできます。

ユーザ認証方式を設定するには、Guard CLI を使用します。Guard の CLI へのアクセスと使用の詳細については、『Cisco Guard Configuration Guide』を参照してください。

Guard への接続に失敗した場合は、次のトラブルシューティング ヒントを確認してください。

- 有効なユーザ名とパスワードを入力したことを確認します。
- 正しい Guard 管理用 IP アドレスを入力したこと、および HTTPS を使用していることを確認します。
- WBM と Guard の両方のネットワーク接続を確認します。
- SSH を使用して WBM から Guard に接続できることを確認します。SSH を使用して接続することにより、WBM と Guard の間のネットワーク接続が確認されます。
- WBM サービスがイネーブルになっていて、WBM の IP アドレスから Guard へのアクセスが許可されていることを確認します (詳細については、[P.2-2 の「WBM のネットワーク アクセスの設定」](#)を参照)。

ログイン バナーの設定

ログイン バナーは、SSH セッション、コンソール ポート接続、または Guard に対する WBM セッションを開いたときにユーザ認証の前に画面に表示されるテキストです。

ログイン バナーは、次の位置に表示されます。

- CLI : パスワード ログイン プロンプトの前
- WBM : Guard ログイン ウィンドウの右側

ログイン バナーを設定するには、Guard **login-banner** CLI コマンドを使用します。必要な設定変更を行うには、Administration ユーザ特権レベルまたは Configuration ユーザ特権レベルの権限を持つユーザとしてログインする必要があります。

ログイン バナーの設定とインポートの詳細については、『Cisco Guard Configuration Guide』を参照してください。

WBM ロゴの設定

WBM Web ページに会社のロゴ（あるいは、カスタマイズした任意のロゴ）を追加することで、WBM インターフェイスをカスタマイズできます。

新しいロゴは、次の位置に表示されます。

- Guard Login ページでは、Cisco Systems ロゴの下
- Guard Login ページ以外のすべての WBM ページでは、Cisco Systems ロゴの右側

WBM ロゴを設定するには、Guard **copy wbm-logo** CLI コマンドを使用します。必要な設定変更を行うには、Administration ユーザ特権レベルまたは Configuration ユーザ特権レベルの権限を持つユーザとしてログインする必要があります。

WBM ロゴのインポートの詳細については、『Cisco Guard Configuration Guide』を参照してください。

