



## 第 20 章 Management タブの概要

イベント、アドレス指定、サービス、およびユーザ情報を割り当てるには、Local Controller の管理機能を使用します。この情報は規則、クエリー内で、フォールス ポジティブを判別するために使用します。

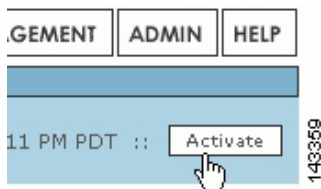
### アクティブ化

一般に、Management タブの変更が規則に含まれている場合は、この変更をアクティブにする必要があります。

### 管理の追加または変更のアクティブ化手順

**ステップ 1** 変更(または追加)が完了したら、**Activate** をクリックしてこれらをアクティブにします。

図 20-1 Activate ボタンのクリック



### イベント管理

Event Management サブタブを開くには、**Management > Event Management** タブの順にクリックします。

Event Management ページで、イベントやイベント グループの検索、フィルタリングのほか、イベント グループを処理できます。

### イベント説明または CVE 名の検索

イベント説明または Common Vulnerabilities and Exposures (CVE) 名の部分一致を検索できます。

**ステップ 1** 検索するテキストを **Search** フィールドに入力します。

**ステップ 2** **Search** をクリックします。

## 現在サポートされているすべての CVE リストの表示手順

---

**ステップ 1 Search** フィールドに CVE を入力します。

**ステップ 2 Search** をクリックします。

---

## イベント グループ

イベント グループを使用および作成することは、規則を利用するための最も強力な方法です。ここに記載されたイベントを取得し、グループ化してから、規則と組み合わせて使用することにより、ユーザは攻撃の検索に専念できます。

### イベント グループまたは重大度を基準としたフィルタリング手順

該当するリストで、グループまたは重大度を選択します。

### イベント グループの編集



**注** システム定義グループは編集できません。

---

**ステップ 1 Select Group** リスト内のグループを選択します。

**ステップ 2 Edit Group** をクリックします。

**ステップ 3 Chosen** および **Available** フィールドで各グループをクリックして、強調表示にします。強調表示を解除するには、再度クリックします。

**ステップ 4 Add** または **Remove** をクリックして、必要に応じて項目を強調表示にします。

**ステップ 5 Submit** をクリックします。

---

## グループの追加

**ステップ 1 Add** をクリックします。

**ステップ 2 Name** フィールドにグループ名を入力します。

**ステップ 3 Available** フィールドで、追加する各グループをクリックして、強調表示にします。強調表示を解除するには、再度クリックします。

**ステップ 4 Add** をクリックします。

**ステップ 5 Submit** をクリックします。

---

## IP 管理

**Management > IP Management** の順にクリックすると表示される IP Management ページでは、ネットワーク資産を定義できます。ネットワーク資産は、インスペクション規則、廃棄規則、レポートやクエリー、トポロジー検出スケジュールを作成するための基本要素として使用したり、レポート デバイスや軽減デバイスを定義する場合に使用したりします。資産はネットワーク、IP 範囲、またはホストとして定義できます。また、インスペクション規則で使用する名前付き変数も定義できます。

ホストに対して定義する脆弱性評価情報(特に OS [オペレーティング システム] のタイプやパッチ レベル、およびホストで稼働する既知のサービス)は、MARS でのフォールス ポジティブの判別に役立ちます。



**ヒント** View リスト ボックスに表示されるオブジェクトリストはフィルタリングできます。フィルタリング基準として選択できるのは、ホスト、ネットワーク、IP 範囲、または変数です。

### アドレス、ネットワーク、変数、またはホストの検索

**ステップ 1** 検索するテキストを **Search** フィールドに入力します。

**ステップ 2** **Search** をクリックします。

### グループを基準としたフィルタリング

**Select Group** リストで、グループを選択します。

### グループの編集

**ステップ 1** **Management > IP Management** の順に選択します。

IP Management ページが表示されます。

**ステップ 2** **Select Group** リスト内のグループを選択します。

**ステップ 3** **Edit Group** をクリックします。

**ステップ 4** **Chosen** および **Available** フィールド内の各グループをクリックして、強調表示にします。強調表示を解除するには、再度クリックします。

**ステップ 5** **Add** または **Remove** をクリックして、必要に応じて項目を強調表示にします。

**ステップ 6** **Submit** をクリックします。

### グループの追加

**ステップ 1** **Management > IP Management** の順に選択します。

IP Management ページが表示されます。

**ステップ 2** **Add Group** をクリックします。

**ステップ 3** Name フィールドにグループ名を入力します。

**ステップ 4** Available フィールドで、強調表示にするグループをクリックします。項目の強調表示を解除するには、再度クリックします。

**ステップ 5** Add をクリックして、選択した Event Type Groups を Chosen フィールドに移動します。

**ステップ 6** Submit をクリックします。

## ネットワーク、IP 範囲、または変数の追加

**ステップ 1** Management > IP Management の順に選択します。

IP Management ページが表示されます。

図 20-2 ネットワーク、IP 範囲、または変数の追加

**ステップ 2** Add をクリックします。

**ステップ 3** Type リストで、ネットワーク、IP 範囲、または変数を選択します。

**ステップ 4** タイプごとに、該当する情報を入力します。

- ・ Network: 名前、ネットワーク IP、ネットワーク マスク
- ・ IP Range: 名前および範囲
- ・ Variable: 変数名

**ステップ 5** Submit をクリックします。

## ホストの追加

ホストは MARS 内では、次のいずれかの結果として、手動、または自動で定義されます。

- ・ Admin > Security and Monitoring Devices タブで定義されるレポート デバイスまたは軽減デバイス
- ・ Admin > Security and Monitoring Devices タブで定義されるレポート デバイスによって管理されるホスト (Cisco Security Agent が稼働しているホストや、CSA 管理コンソールから提供されたログを処理するときに MARS で検出されたホストなど)
- ・ MARS システムのホストとアクティブに相互作用するために特定するアセット (アラートを使用して Syslog メッセージを転送する際に転送先となるサードパーティ製の Syslog サーバなど)
- ・ トポロジ検出中にシステムが検出するホスト (Cisco Catalyst スイッチで ARP キャッシュ テーブルを処理する場合など)。
- ・ 考えられる攻撃対象など、以前に疑わしいとみなされていたセッションに関するホスト。この場合、MARS はホストに Nessus および nmap ポート スweep を実行して、ホストが被害を受けていないかどうかを識別します。

こうしたさまざまな方法で、HTML インターフェイスの IP Management ページで多数のホストを定義できます。MARS と互換性がある脆弱性評価パッケージがない場合は、これらのホストに関する情報をできるだけ多く指定する必要があります。詳細については、「デバイスの脆弱性評価に関する情報」を参照してください。



**注** ホストを追加しようとして、定義済みのホストとの競合を検出した場合、トラブルシューティングの詳細については「デバイスの削除」を参照してください。

ホストを手動で追加する手順は、次のとおりです。

**ステップ 1** Management > IP Management の順に選択します。

IP Management ページが表示されます。

**ステップ 2** Add をクリックします。

**ステップ 3** Type リストで host を選択します。

**図 20-3** ホストの一般情報

**ステップ 4** Name フィールドにホスト名を入力します。

**ステップ 5** Access IP フィールドで、このホストからログ イベントをプルするために使用するアドレス、または検出した攻撃の調査中に動的な脆弱性評価を実行する場合の接続に使用するアドレスを識別します。

**ステップ 6** ホストが Windows、Solaris、または Linux で稼働している場合は、Operating System フィールドで対応する値を選択します。それ以外の場合は、Generic が選択されていることを確認します。

**ステップ 7** ネットワークで NetBIOS が稼働している場合は、このホストに対応した名前を入力します。

NetBIOS は名前登録および名前解決サービスを提供します。MARS はこの設定を使用して、攻撃パスの分析およびアドレス解決を実行します。

**ステップ 8** Add IP/Mask をクリックして、インターフェイスに IP アドレスおよびマスクを追加します。

**ステップ 9** Enter Interface Information で、インターフェイスの名前、IP アドレス、およびネットワーク マスクの値を入力します。

**ステップ 10** デュアルホーミング ホストを使用している場合は、Add Interface をクリックして、インターフェイスを追加できます。

**ステップ 11** 脆弱性評価情報を指定するには、「デバイスの脆弱性評価に関する情報」に進みます。

---

## ホスト情報の編集

---

**ステップ 1** Management > IP Management の順に選択します。

**ステップ 2** 編集するホストの横にあるチェックボックスをオンにします。

**ステップ 3** インターフェイスまたは IP マスク情報を編集している場合は、ここで変更し、**Submit** をクリックします。

**ステップ 4** ホストのプロパティを編集する必要がある場合は、**Properties** をクリックします。

**ステップ 5** 必要に応じて OS を変更し、**Next** をクリックします。

**ステップ 6** サービスまたはアプリケーションを変更するには、オプション ボタンを選択して古いサービスを削除し、**Delete** をクリックします。

**ステップ 7** **Add Service** をクリックして、ステップ 3 に進みます。

---

## サービス管理

Service Management サブタブを開くには、**Management > Service Management** タブの順にクリックします。

サービスは送信元ポート、宛先ポート、およびプロトコルの組み合わせです。Service Management ページに、サービス、サービスの説明、ポート、およびプロトコルが表示されます。Service Management ページで、ネットワークのサービスを処理できます。

## サービスの検索

---

**ステップ 1** 検索するテキストを **Search** フィールドに入力します。

**ステップ 2** **Search** をクリックします。

サービス グループを基準としてフィルタリングする手順は、次のとおりです。

該当するリストで、グループを選択します。

---

## サービス グループの追加

---

**ステップ 1** **Add** をクリックします。

**ステップ 2** **Name** フィールドにグループ名を入力します。

**ステップ 3** **Available** フィールドで、項目をクリックして選択します。項目の選択を解除するには、再度クリックします。

**ステップ 4** **Add** をクリックします。

**ステップ 5** **Submit** をクリックします。

---

## サービス グループの編集



---

**注** システム定義グループは編集できません。

---

**ステップ 1 Select Group** リスト内のグループを選択します。

**ステップ 2 Edit Group** をクリックします。

**ステップ 3 Chosen** および **Available** フィールド内の各グループをクリックして、強調表示にします。強調表示を解除するには、再度クリックします。

**ステップ 4 Add** または **Remove** をクリックして、強調表示にした項目を必要に応じて移動します。

**ステップ 5 Submit** をクリックします。

---

## サービスの追加

**ステップ 1 Add** をクリックします。

**ステップ 2** サービスの詳細を入力します。

**ステップ 3 Submit** をクリックします。

---

## サービスの編集

**ステップ 1** サービスの横にあるチェックボックスをオンにします。

**ステップ 2 Edit** を検索します。

**ステップ 3** 変更し、**Submit** をクリックします。

---

## サービスの削除

**ステップ 1** サービスの横にあるチェックボックスをオンにします。

**ステップ 2 Delete** をクリックします。

**ステップ 3** 確認ページで、**Yes** をクリックします。

---

## ユーザ管理

User Management ページでは、MARS システムのユーザおよび管理者を管理できます。これらのユーザが属する役割やグループも管理対象に含まれます。このページでは、新しいユーザ アカウントを定義して、HTML インターフェイスの特定の機能にアクセスできるようになります。有効な電子メール アドレスやページの番号など、ユーザ固有の通知設定をユーザに対して定義できます。システム全体の設定の一部(ページや携帯電話のサービス プロバイダー設定など)も、このページからのみアクセスできます。User Management ページにアクセスするには、**Management > User Management** または **Admin > User Management** の順にクリックします。

MARS には、4 つの異なるユーザ役割があります。これらは、HTML インターフェイスにアクセスする必要があるすべてのユーザに割り当てられます。

- ・ *Admin* — 完全な読み取り/書き込み権限があります。この役割のユーザは、目的の役割を持つ新規ユーザを定義できます。
- ・ *Security Analyst* — 完全な読み取り権限を持ちますが、書き込み権限はレポートに限定されています。この役割のユーザは、Notifications Only 役割を持つ新規ユーザのみを定義できます。
- ・ *Operator* — 読み取り専用の権限を持ちます。この役割のユーザは、新規ユーザを定義できません。
- ・ *Notifications Only* — このユーザ役割には、MARS HTML インターフェイスにアクセスする権限がありません。この役割は、電子メール、SMS、ページ通知などの通知を受信するユーザを識別する場合に使用します。

役割はシステムで定義されていますが、ユーザ グループはユーザが定義、編集、および削除できます。詳細については、「ユーザ グループの作成」および「ユーザ グループに対するユーザの追加または削除」を参照してください。

セキュリティを高めるために、MARS アプライアンスに強力なパスワードを設定することを推奨します。ユーザ名およびパスワードを定義する場合は、次の注意事項に従ってください。

ログイン名およびパスワードに関する注意事項:

- ・ 英数字を指定できる。
- ・ 特殊文字を使用できる (!, @, # など)。
- ・ 一重または二重引用符 ( ` および ` ") は使用できません。
- ・ 大文字と小文字が区別される。

ログイン名の最大文字数は 20、パスワードの最大文字数は 64 です。

## 新規ユーザの追加

新規ユーザを定義する場合は、ユーザ名、パスワード、役割、連絡先、および通知情報を指定します。

新しいユーザを追加する手順は、次のとおりです。

---

**ステップ 1** **Management > User Management** タブで、**Add** をクリックします。User Configuration ページが表示されます (図 20-4 を参照)。

図 20-4 User Configuration ページ

Role: Admin

Login: admin

Password: [masked]

Re-enter password: [input field]

First Name: admin

Last Name: admin

Organization: Cisco Systems, Inc.

Email: admin@aaa.com

SMS: 8885551212@servprov.com

Work Phone: 8885551212

Home Phone: 000000123

Fax: 00000000

Pager: 000000123 (Cell phone or pager numbers go: 0000000000)

Service Provider: servprov [Edit Provider]

Cancel Submit

**ステップ 2 Role** フィールドで、目的のユーザの **Role** を選択します。

- **Admin**: Local Controller を完全に使用できます。
- **Notification Only**: Local Controller アプライアンスのユーザでないユーザは、この役割を使用して、Admin、Security Analyst、または Operator 以外のユーザにアラートを送信します。
- **Operator**: 読み取り専用の権限を持ちます。
- **Security Analyst**: Admin タブにアクセスできない点を除いて、Local Controller を完全に使用できます。

**ステップ 3** 必要に応じて、ユーザのパスワードを作成または変更します。

**ステップ 4** ユーザーの証明書および個人情報を入力します。

入力する情報は次のとおりです。

- 名
- 姓
- 組織名
- 電子メール アドレス
- Short Message Service (SMS) 番号 (例: 8885551212@servprov.com)
- 勤務先の電話番号
- 自宅の電話番号
- FAX 番号
- ページャの番号 — 5552345678 などの携帯電話の番号も入力できます。

**ステップ 5** ページャによる通知を作成する場合は、次の「サービス プロバイダーの追加 (携帯電話/ページャ)」に進みます。それ以外の場合は、**Submit** をクリックして、ユーザの追加手順を完了します。

## サービス プロバイダーの追加(携帯電話/ページ)

ページによる通知を設定するには、次の手順を実行して、サービス プロバイダー(携帯電話またはページの会社)を追加します。

**ステップ 1** **Service Provider** フィールドで、**New Provider** を選択します。追加フィールドが表示されます(図 20-5 を参照)。

新しいサービス プロバイダーを追加すると、プルダウン メニューに読み込まれます。

図 20-5 新しいプロバイダーの選択および連絡先の入力

**ステップ 2** **Provider Name** フォールドに、サービス プロバイダーの名前を入力します。

**ステップ 3** **Provider Phone No** フィールドに、サービス プロバイダーの電話番号を入力します。

この番号は、サービス プロバイダーが IXO/TAP プロトコルを使用して英数字メッセージを受信するために使用する電話番号です。フォーマットは、通常の電話番号と同様です(18001234567 など)。1-800-1234567 のフォーマットも指定できます。PBX(構内交換機)外部の番号にアクセスするために「9」をダイヤルする必要がある場合は、電話番号全体の前に「9,」を入力します(例:9,1-800-1234567)。

**ステップ 4** **Provider Baudrate** フィールドに、サービス プロバイダーが指定したボー レートを入力します。

このボー レートは、指定した電話番号に対してサービス プロバイダーが要求しているボー レートです。一般的な値は 1200、2400、4800、および 9600 です。

ボー レートの詳細については、ご使用のサービス プロバイダーの Web サイトを参照してください。

**ステップ 5** **Submit** をクリックして、User Configuration ページを閉じ、**User Management** タブに戻ります。

## ユーザの検索

**ステップ 1** 検索するテキストを **Search** フィールドに入力します。

**ステップ 2** **Search** をクリックします。

## ユーザの編集または削除

**ステップ 1** **Management User** タブで、ユーザ名の横にあるチェックボックスをオンにします。

**ステップ 2** **Delete** をクリックして、ユーザを削除します。

**ステップ 3** **Edit** をクリックして、ユーザの設定情報を変更します。  
User Configuration ページが表示されます。

**ステップ 4** User Configuration ページを編集します。

**ステップ 5** **Submit** をクリックします。

---

## ユーザ グループの作成

**ステップ 1** **Add Group** をクリックします。

**ステップ 2** **Name** フィールドにグループ名を入力します。

**ステップ 3** グループにユーザを追加するには、右側のリストで目的のユーザのチェックボックスをオンにします。 **Add** をクリックします。チェックした名前が、ダイアログボックスの左側に移動します。

**ステップ 4** グループからユーザを削除するには、Ctrl キーを押しながら左側のユーザをクリックして、選択します。 **Remove** をクリックします。選択した名前がダイアログボックスの右側に移動します。

**ステップ 5** **Submit** をクリックします。

---

## ユーザ グループに対するユーザの追加または削除

カスタム ユーザ グループに対してユーザを追加または削除する手順は、次のとおりです。



**注** Admin、Operator、Notification、および Security Analyst はシステム グループであるため、編集できません。ユーザは役割に対応したユーザ グループに自動的に追加されます。

**ステップ 1** **Select Group** フィールドでユーザ グループを選択します。グループのメンバーが表示されます。

**ステップ 2** **Edit Group** をクリックします。User Group ダイアログボックスが表示されます。

**ステップ 3** グループにユーザを追加するには、右側のリストで目的のユーザのチェックボックスをオンにします。 **Add** をクリックします。チェックした名前が、ダイアログボックスの左側に移動します。

**ステップ 4** グループからユーザを削除するには、Ctrl キーを押しながら左側のユーザをクリックして、選択します。 **Remove** をクリックします。選択した名前がダイアログボックスの右側に移動します。

**ステップ 5** **Submit** をクリックします。 **User Management** タブが再び表示されます。

---

## グループを基準としたフィルタリング

**Select Group** リストで、グループを選択します。グループのメンバーのみが表示されます。

