



設定 (Configure)

• 設定 (1 ページ)

設定

FMC にインストールされた修復モジュールを設定するには、FMC GUI で次の手順を実行します。

ステップ 1 ネットワーク内の Tetration Analytics (TA) サーバごとに修復モジュールのインスタンスを作成します。

1. [ポリシー (Policies)] > [アクション (Actions)] > [インスタンス (Instances)] に移動します。
2. ドロップダウン リストから修復モジュールを選択し、[追加 (Add)] をクリックします。

The screenshot shows the FMC GUI interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies' (selected), 'Devices', 'Objects', 'AMP', 'Intelligence', 'Deploy', and 'System'. Below this, there are sub-tabs: 'Access Control', 'Network Discovery', 'Application Detectors', 'Correlation', 'Actions', and 'Instances' (selected). The main content area shows 'Configured Instances' with a table that has columns for 'Instance Name', 'Module Name', and 'Version'. The table is currently empty, with the text 'No instances configured' displayed below it. Below the table, there is a section titled 'Add a New Instance' with a dropdown menu labeled 'Select a module type' showing 'Tetration/FirePOWER Remediation Module(v1.0.1)' and an 'Add' button.

3. [インスタンス名 (Instance Name)] を入力します (この例では、**rem-instance**) 。

4. TA サーバの IP アドレス、API キー、API シークレット、および問題のある可能性のあるホストが含まれる範囲を入力します。[作成 (Create)] をクリックします。

(注) API キーとシークレットは、この時点では TA サーバに対して検証されません。サイト管理者、カスタマーサポート、またはルートスコープオーナーロールは、API キーとシークレットを TA で最初に作成しておく必要があります。ここで使用する情報をコピーします。詳細については、『[TA API Configuration Guide](#)』を参照してください。

Overview Analysis **Policies** Devices Objects AMP Intelligence Deploy System

Access Control ▾ Network Discovery Application Detectors Correlation **Actions ▶ Instance**

Alerts Remediations

✔ Success ✕
 Created new instance rem-instance

Edit Instance

Instance Name: rem-instance

Module: Tetration/FirePOWER Remediation Module(v1.0.1)

Description:

Tetration Analytics IP:

Scope(e.g. Default):

API key
Retype to confirm:

API secret
Retype to confirm:

Configured Remediations

Remediation Name	Remediation Type	Description
No configured remediations available		

Add a new remediation of type

- [設定されている修復 (Configured Remediations)]で、修復のタイプを選択し (この例では、**Quarantine an IP on Tetration Analytics**)、[追加 (Add)]をクリックして新しい修復を追加します。
- [修復名 (Remediation Name)]を入力し (この例では、**quaran-rem**)、[作成 (Create)]をクリックします。

Overview Analysis **Policies** Devices Objects AMP Intelligence Deploy System

Access Control ▾ Network Discovery Application Detectors Correlation **Actions ▶ Instances**

Alerts Remediations Groups

Edit Remediation

Remediation Name

Remediation Type

Description

7. 設定した修復がテーブルに表示されます。[保存 (Save)]をクリックします。

Overview Analysis **Policies** Devices Objects AMP Intelligence Deploy System

Access Control ▾ Network Discovery Application Detectors Correlation **Actions ▶ Instance**

Alerts Remediations Group

Edit Instance

Instance Name rem-instance

Module Tetration/FirePOWER Remediation Module(v1.0.1)

Description

Tetration Analytics IP 172.26.46.68

Scope(e.g. Default) SBG

API key
Retype to confirm

API secret
Retype to confirm

Save Cancel

Configured Remediations

Remediation Name	Remediation Type	Description
quaran-rem	Quarantine an IP on Tetration Analytics	To quarantine a host

Add a new remediation of type Add

ステップ2 アクセス制御ポリシーを設定します（この例では、**rem-policy**）。

1. [ポリシー (Policies)] > [アクセス制御 (Access Control)] > [ルール (Rules)] に移動します。
2. [ルールの追加 (Add Rule)] をクリックします（たとえば、**block-ssh-add-tag**）。
3. [アクション (Action)] で [ブロック (Block)] を選択します。

- [ポート (Ports)] タブで、宛先ポートのプロトコルの一覧から [SSH] を選択し、[追加 (Add)] をクリックします。
- [保存 (Save)] をクリックします。
- [ロギング (Logging)] タブで、[接続開始時のログ (Log at Beginning of Connection)] を選択します。
重要 アクセスルールでロギングが有効になっていることを確認します。これにより、FMCはイベント通知を受信します。
- [保存 (Save)] をクリックします。

ステップ3 関連ルールを設定します。

- [ポリシー (Policies)] > [関連 (Correlation)] > [ルールの管理 (Rule Management)] に移動します。
- [ルール名 (Rule Name)] を入力し (この例では、**quaran-rule1**)、説明 (オプション) を入力します。
- [このルールのイベントタイプの選択 (Select the type of event for this rule)] セクションで、[接続イベントの発生 (a connection event occurs)] および [接続の開始時または終了時 (at either the beginning or the end of the connection)] を選択します。
- [条件を追加 (Add condition)] をクリックし、演算子を **OR** から **AND** に変更します。
- ドロップダウンリストで、[アクセスコントロールルール名 (Access Control Rule Name)]、[は (is)] を選択し、ステップ2で設定したアクセスコントロールルールの名前を入力します (この例では、**block-ssh-add-tag**)。

Overview Analysis **Policies** Devices Objects AMP Intelligence Deploy

Access Control ▾ Network Discovery Application Detectors **Correlation** Actions ▾ Alerts

Policy Management **Rule Management** White List Traffic Profiles

Rule Information + Add Connection Tracker + Add User Qualification + Add Hos

Rule Name

Rule Description

Rule Group

Select the type of event for this rule

If at either the beginning or the end of the connection ▾ and it meets the fol

+ Add condition + Add complex condition

✗

Rule Options + Add Inactive Period

Snooze If this rule generates an event, snooze for hours ▾

Inactive Periods There are no defined inactive periods. To add an inactive period, click "Add Inactive Period".

6. [保存 (Save)] をクリックします。

ステップ 4 関連ルールに、修復モジュールのインスタンスを応答としてアソシエートします。

1. [ポリシー (Policies)] > [相関 (Correlation)] > [ポリシーの管理 (Policy Management)] に移動します。
2. [ポリシーの作成 (Create Policy)] をクリックします。
3. [ポリシー名 (PolicyName)] を入力し (この例では、**correlation-policy**)、説明 (オプション) を入力します。
4. [Default Priority] ドロップダウンリストから、ポリシーのプライオリティを選択します。[なし (None)] を選択して、ルールのプライオリティのみ使用します。

5. [ルール追加 (Add Rules)] をクリックし、ステップ3で設定した関連ルールを選択し (この例では、**quaran-rule1**)、[追加 (Add)] をクリックします。

Overview Analysis **Policies** Devices Objects AMP Intelligence Deploy System

Access Control ▾ Network Discovery Application Detectors **Correlation** Actions ▾

Alerts Remediation

Policy Management Rule Management White List Traffic Profiles

Correlation Policy Information

Policy Name: correlation-policy

Policy Description: correlation policy for testing

Default Priority: None ▾

Policy Rules

Rule	Responses	Priority
quaran-rule1 add tag	This rule does not have any responses.	Default ▾

6. ルールの横にある [応答 (Responses)] アイコンをクリックし、ルールに応答を割り当てます (この例では、**quaran-rem**)。[更新 (Update)] をクリックします。

Overview Analysis **Policies** Devices Objects AMP Intelligence Deploy System

Access Control ▾ Network Discovery Application Detectors **Correlation** Actions ▾

Alerts Remediation

Policy Management Rule Management White List Traffic Profiles

Correlation Policy Information

Policy Name: correlation-policy

Policy Description: correlation policy for testing

Default Priority: None ▾

Policy Rules

Rule	Responses	Priority
quaran-rule1 add tag	quaran-rem (Remediation)	Default ▾

7. [保存 (Save)]をクリックします。
-

