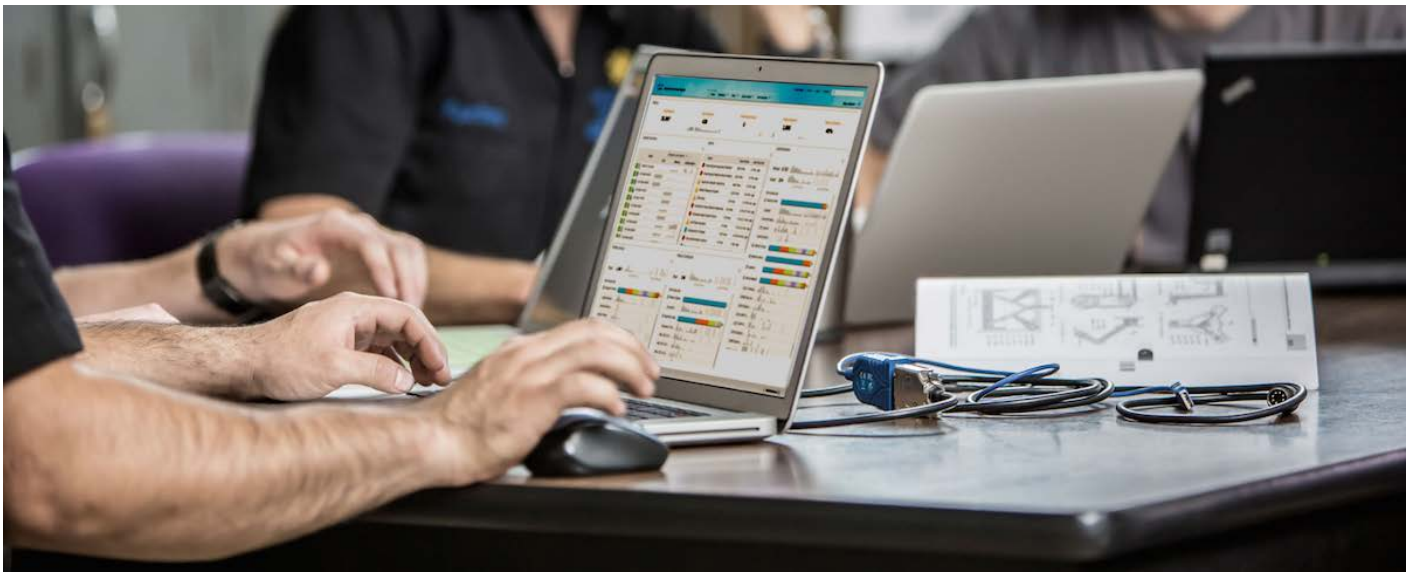


Cisco FireSIGHT および ISE の脅威を迅速に封じ込めるためのソリューション

目次

このドキュメントについて **4**
技術概要 **5**
FireSIGHT レルム設定 **8**
LDAP 接続の設定 8
サンプル ユーザ LDAP 情報 10
pxGrid を使用したスタンドアロン環境の自己署名証明書用の ISE の設定 **11**
ISE 識別自己署名証明書の ISE 信頼証明書ストアへのエクスポート 11
自己署名証明書用の FireSIGHT Management Center の設定 **14**
自己署名証明書を使用する pxGrid エージェントの設定 19
CA 署名操作用にカスタマイズされた pxGrid テンプレート **22**
pxGrid を使用したスタンドアロン環境の CA 署名証明書用の ISE の設定 **26**
CA 署名証明書用の FireSIGHT Management Center の設定 **30**
CA 署名証明書を使用する pxGrid エージェントの設定 32
FireSIGHT pxGrid 修復モジュール **34**
FireSIGHT pxGrid 修復モジュールのアップロード 34
新しいインスタンスの作成 34
FireSIGHT pxGrid 軽減タイプの作成 35
検疫 35
ポートバウンス 35
再認証 36
シャットダウン 36
強制終了 37
検疫解除 37
FireSIGHT pxGrid 侵入ポリシー **39**
FireSIGHT 接続ルール **44**
ISE EPS サービスと検疫許可ポリシーの設定 **47**
FireSIGHT Management Center 相関ポリシー **49**
検疫 49
テスト 51
ポートバウンス 53
テスト 55

Cisco Systems © 2016

ポートシャットダウン 58
テスト 60
再認証 63
テスト 65
強制終了 68
テスト 70
検疫解除相関ポリシー 73
テスト 75
トラブルシューティング 78
ISE pxGrid サービスが起動しない 78
pxGrid エージェント証明書エラー メッセージ 78
FireSiGHT Management Center が ISE と通信していない 78
FireSIGHT Management Center に相関イベントがまったく表示されない 78
FireSIGHT が軽減試行に失敗した 78
軽減試行で「ルックアップ失敗」 78
pxGrid 接続障害により FireSIGHT Management Console からのエラー メッセージが syslog に記録される 79
ISE システム ストアへのインポートによる自己署名証明書の検証 80
不具合の解決 82
pxGrid & Identity マッピング サービスが再起動する 82
アクティブな pxGrid ノードが GUI に反映されない。CLI には反映される 82
参考資料 83

このドキュメントについて

このマニュアルは、FireSIGHT Management Center（5.4）を導入することに関心のある、シスコ エンジニアとお客様に向けて作成されています。ここでは、エンドポイントでアクションを実行することを目的に、pxGrid（platform exchange Grid）の Adaptive Network Control（ANC）軽減アクションを使用する Cisco Identity Service Engine（ISE 1.3 以降）の同時導入を想定しています。FireSIGHT Management Center 5.4 のみが対象であり、FireSIGHT Management Center 6.0 は対象外である点に注意してください。

このマニュアルでは、自己署名証明書および pxGrid 対応の認証局（CA）署名証明書を使用するスタンドアロン環境で、ISE を使用した FireSIGHT Management Center の設定について詳しく説明します。pxGrid 修復モジュール、pxGrid エージェントのインストール、および設定の詳細情報を説明します。pxGrid 修復モジュールは pxGrid ANC 軽減機能として、検疫、ポートバウンス、ポート遮断、再認証、強制終了、および検疫解除を提供します。pxGrid エージェントは FireSIGHT Management Center と ISE pxGrid ノード間の証明書情報および ISE pxGrid ノード接続情報を提供します。相関ポリシー、ルール、修復のタイプは、ANC の軽減アクション タイプごとに定義されます。

読者は、FireSIGHT Management Center と Identity Service Engine（ISE）のアクセス コントロール システムについて一定の知識が必要です。前提条件として、FireSIGHT Management Center 5.4 およびスタンドアロン ISE 1.3 または ISE 1.4 環境がインストールされている必要があります。FireSIGHT Management Center 5.4 は ISE 2.0 でもテスト済みです。

このマニュアルのテストでは、次のソフトウェア バージョンを使用しました。

- FireSIGHT Management Center 5.4
- FireSIGHT アプライアンス仮想センサー 5.4
- Cisco Identity Services Engine ISE 1.3 および ISE 1.4
- FireSIGHT pxGrid 修復モジュール 1.0
- FireSIGHT pxGrid Agent 1.0
- Microsoft CA 2008 R2 Enterprise

分散 ISE 環境で ISE pxGrid を設定する場合は、「参考資料」の項のリンクを参照してください。pxGrid クライアントとして Mac を使用し、CA 署名証明書および自己署名証明書を使用する導入ガイドも参考資料として含まれています。

技術概要

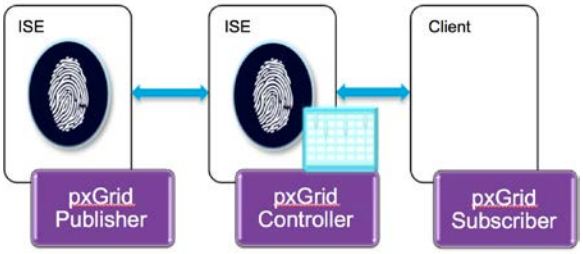
シスコの Platform Exchange Grid（pxGrid）はマルチベンダーのプラットフォーム間で IT インフラストラクチャ内のネットワーク システム コラボレーションを実現します。たとえば、セキュリティ モニタリングと検知システム、ネットワーク ポリシー プラットフォーム、アセットおよび設定管理、アイデンティティおよびアクセス管理のプラットフォーム、そして事実上その他のあらゆる IT 運用プラットフォームが対象です。pxGrid は Identity Services Engine（ISE）ポリシー サーバを使用して、認証、認可、およびアクセス制御（AAA）を提供します。

pxGrid フレームワークは次のコンポーネントで構成されます。

pxGrid パブリッシャ：該当トピックや機能を公開します。

pxGrid コントローラ：すべての pxGrid クライアントの認証、許可、機能、およびサブスクリプション リストを管理します。

pxGrid サブスクライバ（別名「pxGrid クライアント」）：公開された pxGrid トピックをサブスクライブします。



FireSIGHT ISE 修復モジュールは pxGrid クライアントであり、ISE パブリッシュ/サブスクライブ方式による軽減アクションを提供します。

ISE はセッション ディレクトリおよびエンドポイント保護サービスを公開します。セッション ディレクトリは pxGrid セクション オブジェクトの ISE セッション ディレクトリ内にある既存の属性を公開します。これには次が含まれます。

セッション状態

IP アドレス

ユーザ名

ユーザの AD ドメイン

MAC

NAS IP アドレス

TrustSec セキュリティ グループ名

エンドポイント プロファイル名

プロファイリング ポリシー名

ポスチャ ステータス

監査セッション ID

アカウンティング セッション IP（RADIUS AV ペア内、最終更新日時）

エンドポイント保護サービスは次の pxGrid ANC 軽減オブジェクトを公開します。

検疫

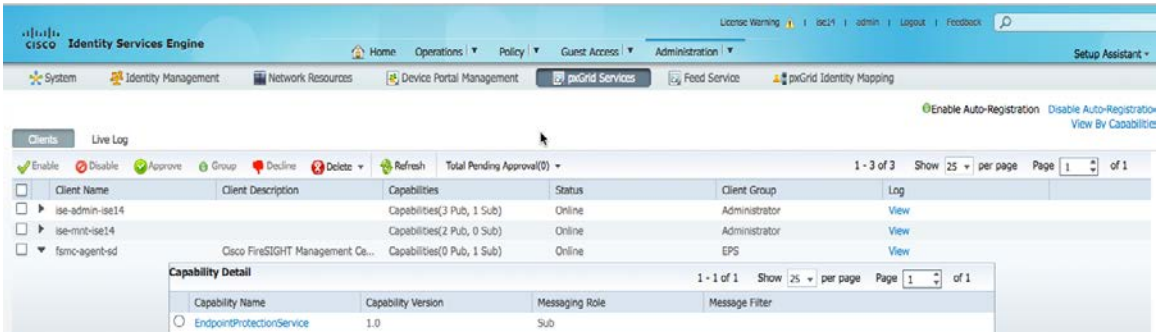
検疫解除

強制終了

ポート バウンス

シャットダウン

FireSIGHT エージェントは pxGrid クライアントとして ISE pxGrid ノードに登録され、pxGrid ANC の軽減アクションを実行するために、エンドポイント保護サービス トピックおよび EPS セッション グループをサブスクライブします。



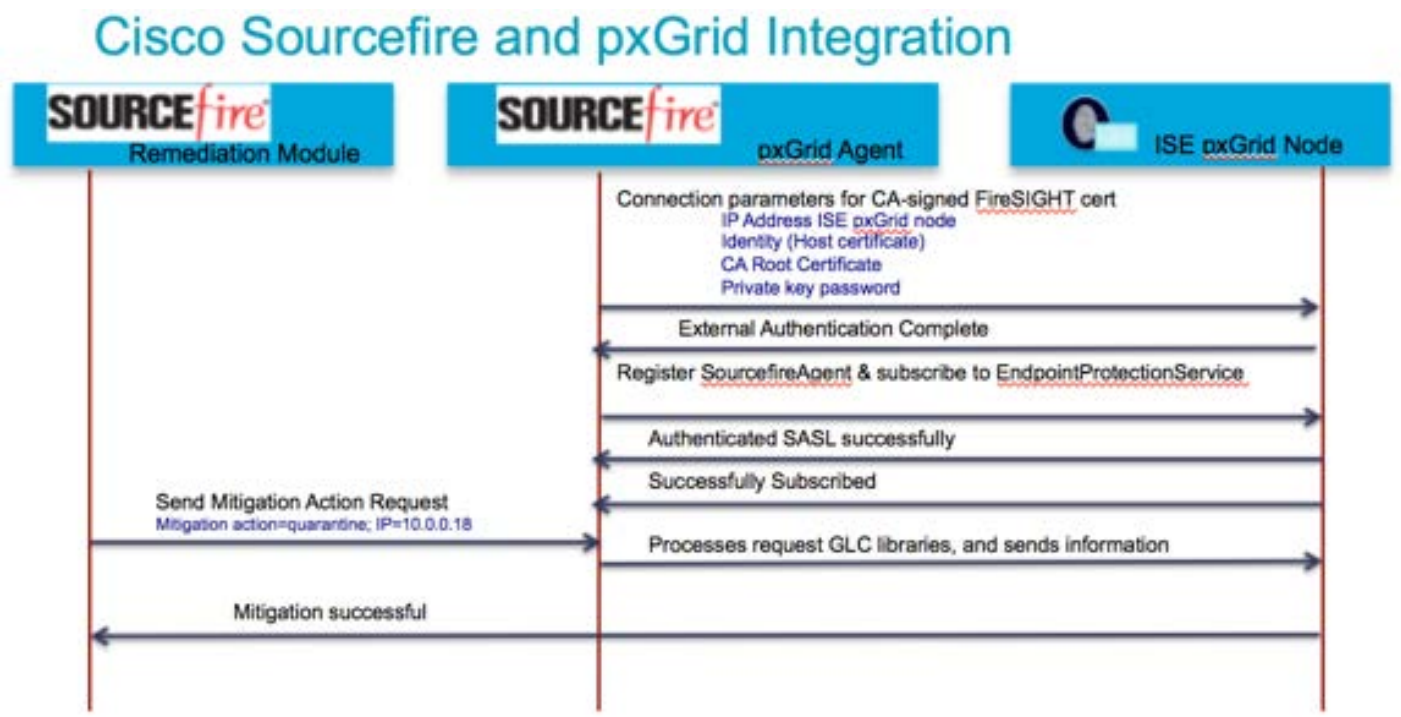
実際の FireSIGHT pxGrid 統合は、pxGrid エージェントおよび pxGrid 修復モジュールを FireSIGHT Management Center にアップロードすることによって実現します。

pxGrid エージェントのインストールは次の 3 つの機能を果たします。

pxGrid サービスとサポート ライブラリのインストール

- pxGrid 接続パラメータの設定。たとえば、pxGrid ノード IP アドレス、ホスト/アイデンティティ証明書、ホスト秘密キー証明書、および信頼できる CA ルートなどがあります。
- pxGrid サービスの開始、pxGrid 修復モジュールからの軽減アクション要求の処理、および ISE pxGrid ノードへの情報送信を行います。
- pxGrid 修復モジュールはすべての pxGrid のインタラクションを pxGrid サービスに転送し、ISE pxGrid ノードから通知結果を受信します。

FireSIGHT pxGrid 修復モジュールは pxGrid ANC 軽減アクション要求を FireSIGHT pxGrid サービスに送信します。FireSIGHT pxGrid サービスはこれらの要求を pxGrid GCL ライブラリに基づいて処理した後、この情報を ISE pxGrid ノードへ送信します。FireSIGHT Management Center がエンドポイントのユーザ ログオン/ログオフ情報およびオペレーティング システムの詳細情報を取得できるようにするため、Microsoft AD レルムはホストとユーザに対するネットワーク検出が有効になるように設定されます。

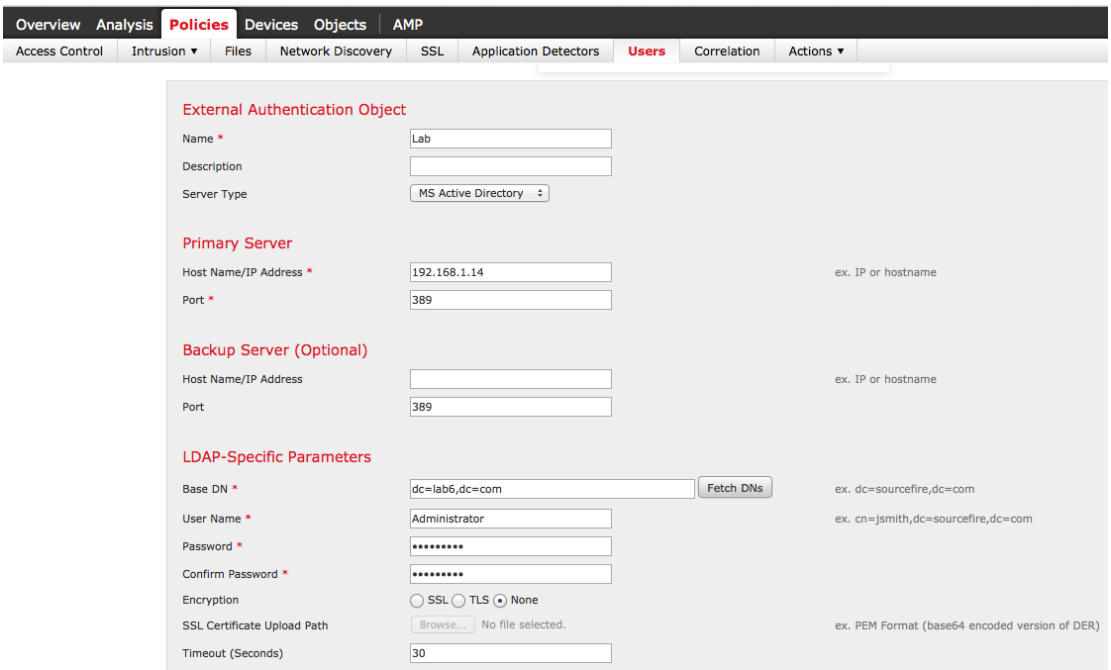

Cisco Sourcefire and pxGrid Integration
SOURCEfire
Remediation Module
SOURCEfire
pxGrid Agent
ISE pxGrid Node
Connection parameters for CA-signed FireSIGHT cert
IP Address ISE pxGrid node
Identity (Host certificate)
CA Root Certificate
Private key password
External Authentication Complete
Register SourcefireAgent & subscribe to EndpointProtectionService
Authenticated SASL successfully
Successfully Subscribed
Send Mitigation Action Request
Mitigation action=quarantine; IP=10.0.0.18
Processes request GLC libraries, and sends information
Mitigation successful

FireSIGHT レルム設定

LDAP ユーザ情報を提供する認証サーバを定義します。また、ユーザ ログオン/ログオフの詳細およびホスト情報とオペレーティング システムの詳細を提供するために、ユーザ認識とネットワーク検出を有効にします。

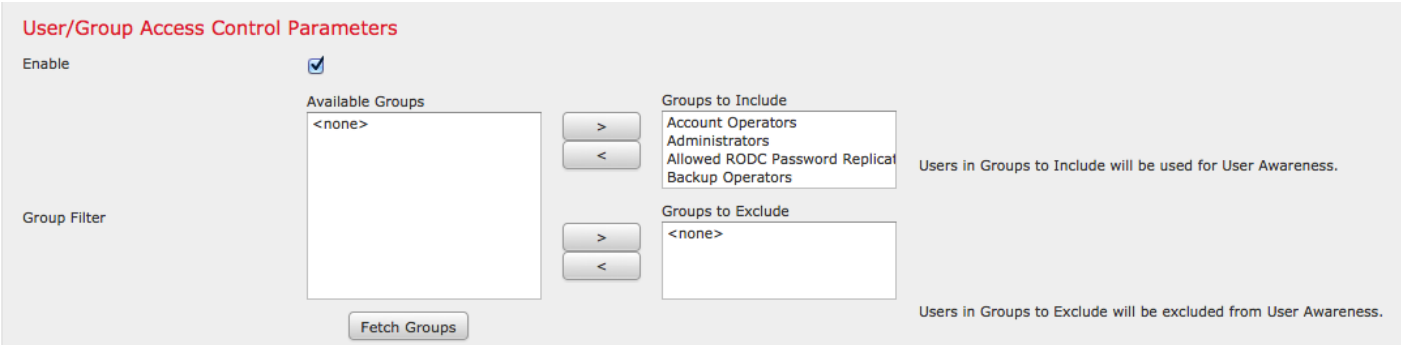
LDAP 接続の設定

ステップ 1 [ポリシー（Policies）] -> [ユーザ（Users）] -> [LDAP接続の追加（Add LDAP Connection）] を選択し、次の入力を行います。



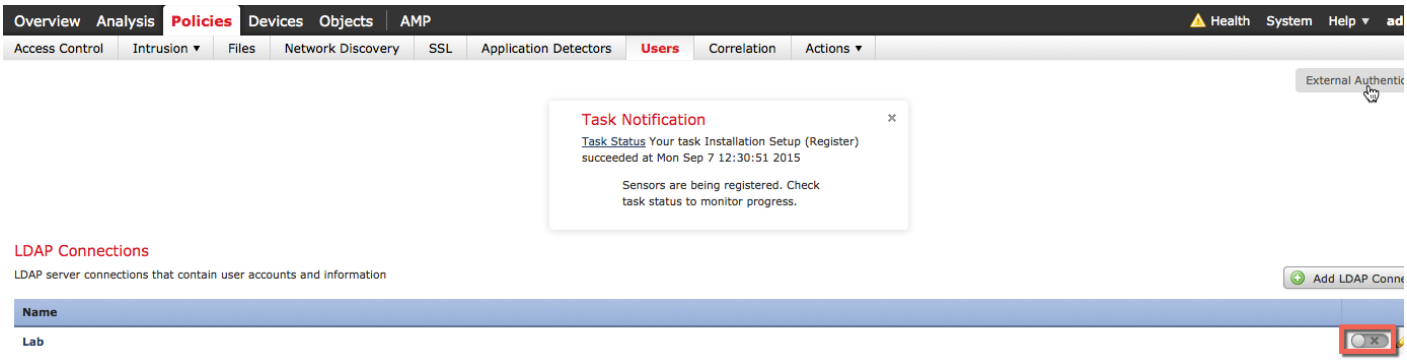
ステップ 2 [ユーザ/グループアクセスコントロールパラメータ（User/Group Access Control Parameters）] で [有効化（Enable）] をオンにし、グループを指定します。

注：ユーザ認識を行うためには、すべてのグループを含めます。

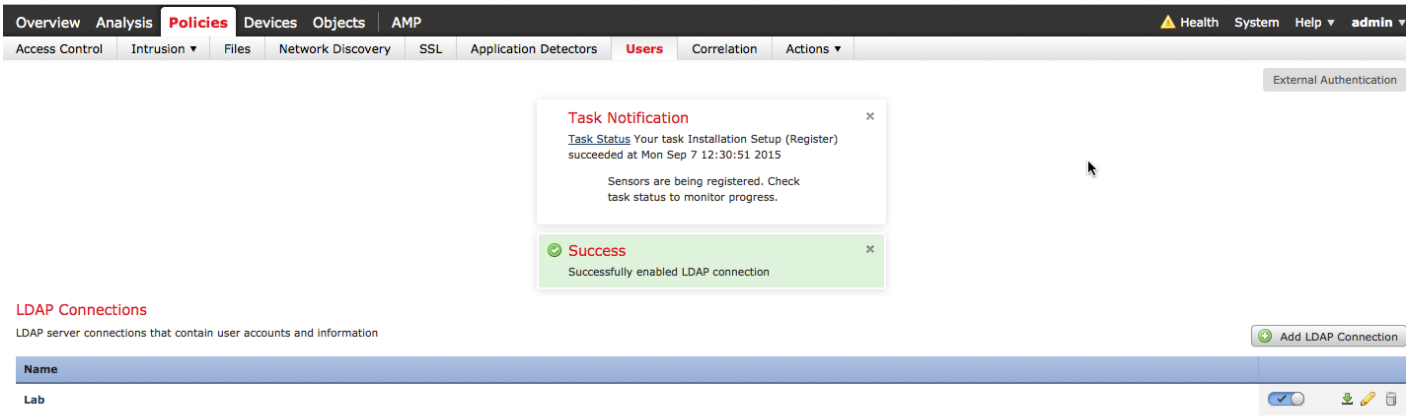


ステップ 3　テストおよび保存を行います。

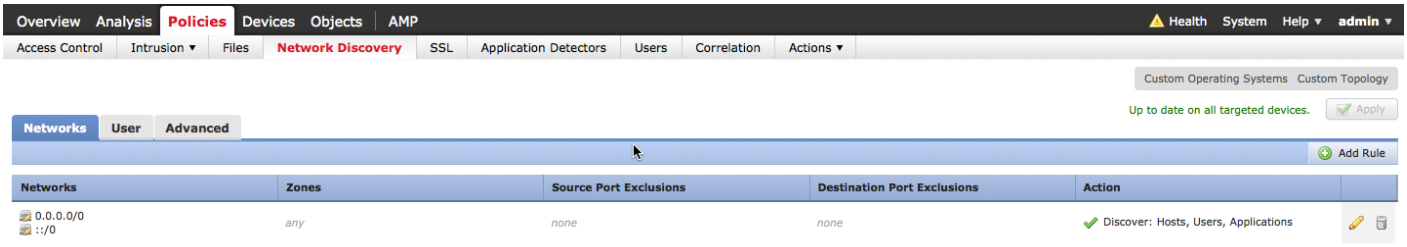
ステップ 4　LDAP 接続をアクティブにします。下図のボタンをクリックします。



ステップ 5　次の内容が表示されます。

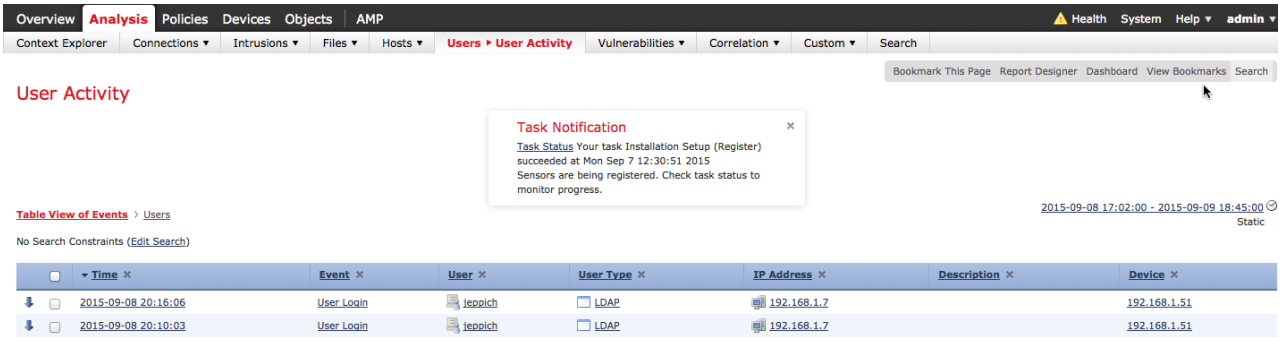


ステップ 6　ホスト、ユーザ、およびアプリケーションのネットワーク検出を有効にします。[ポリシー（Policies）] -> [ネットワーク検出（Network Discovery）] を選択し、鉛筆アイコンをクリックして、ホスト、ユーザ、およびアプリケーションを選択し、保存します。

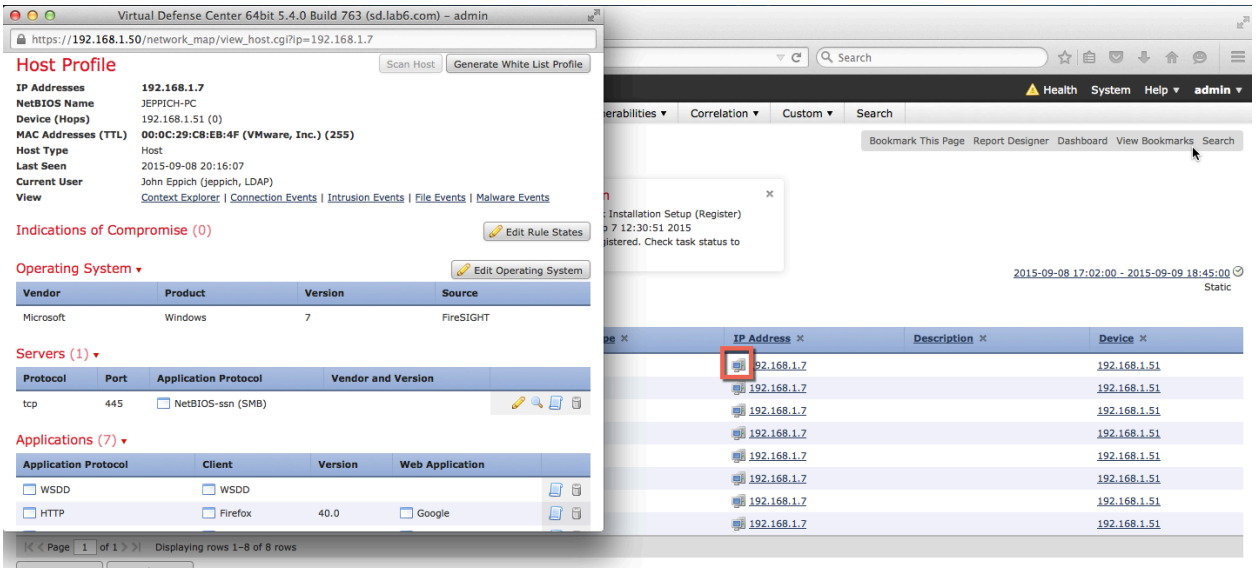


サンプル ユーザ LDAP 情報

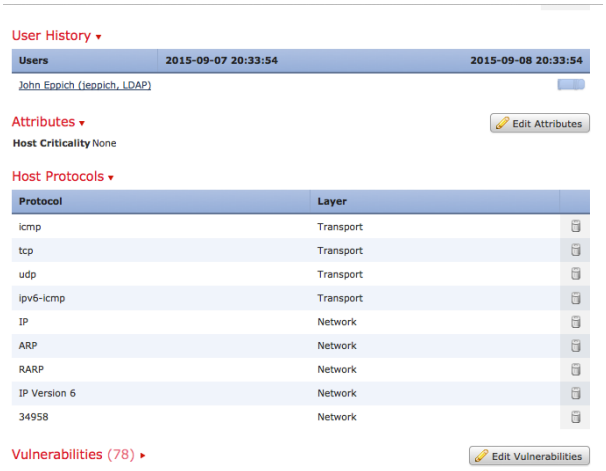
[ユーザアクティビティ(User Activity)] 画面にはエンドユーザ情報が表示されます。



また、下図のように、PC アイコンをクリックすると、IP アドレスに対応する「ホスト プロファイル」が表示されます。



このホスト プロファイルには、ユーザ履歴情報、ホスト プロトコル、および脆弱性情報が含まれます。



pxGrid を使用したスタンドアロン環境の自己署名証明書用の ISE の設定

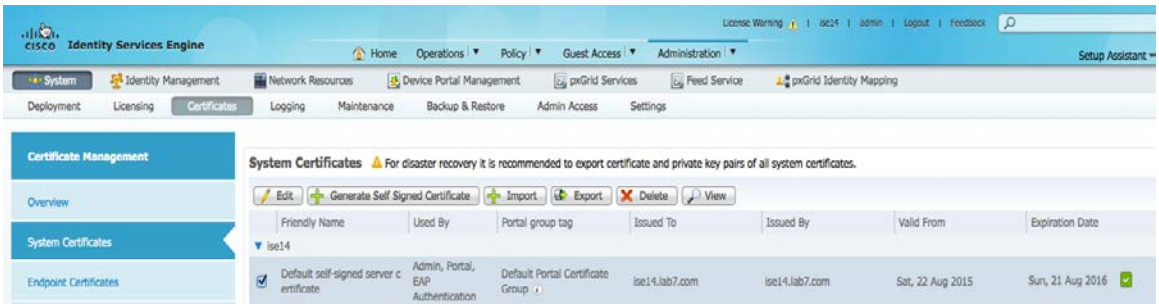
この項では、pxGrid を使用したスタンドアロン環境で、自己署名証明書を使用して ISE を設定する手順を説明します。

ISE 識別自己署名証明書の ISE 信頼証明書ストアへのエクスポート

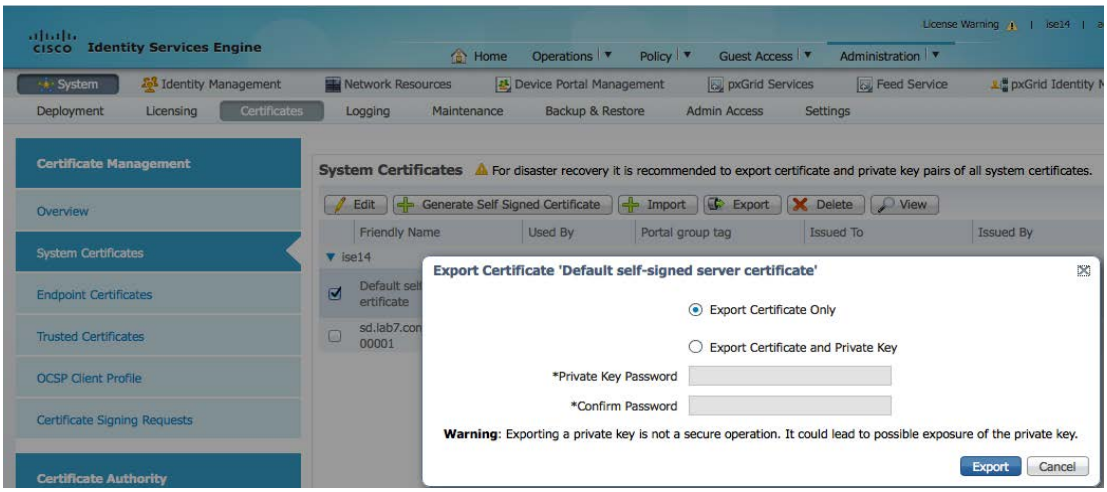
これは ISE が自己署名証明書を信頼するために必要です。

注:これは ISE 2.0 では必要ではない点に注意してください。デフォルトでは、ISE で pxGrid が有効な場合、公開されたノードが表示され、ISE pxGrid ノードへの接続が確立されます。この ISE 識別自己署名証明書が信頼されます。

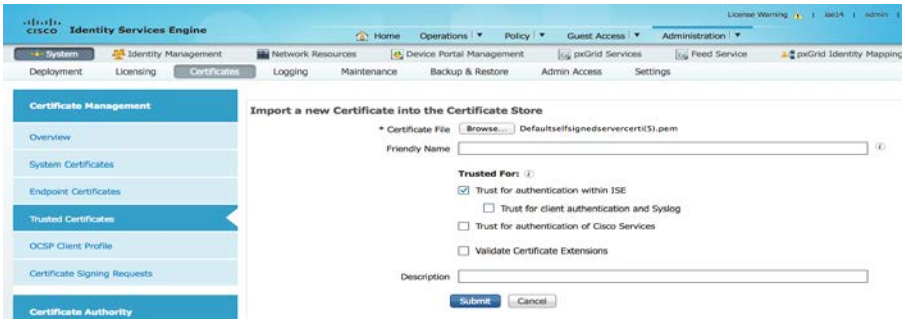
ステップ 1 [管理(Administration)] -> [システム(System)] -> [証明書(Certificates)] -> [システム証明書(System Certificates)] を選択し、ISE 自己署名識別証明書を選択します。



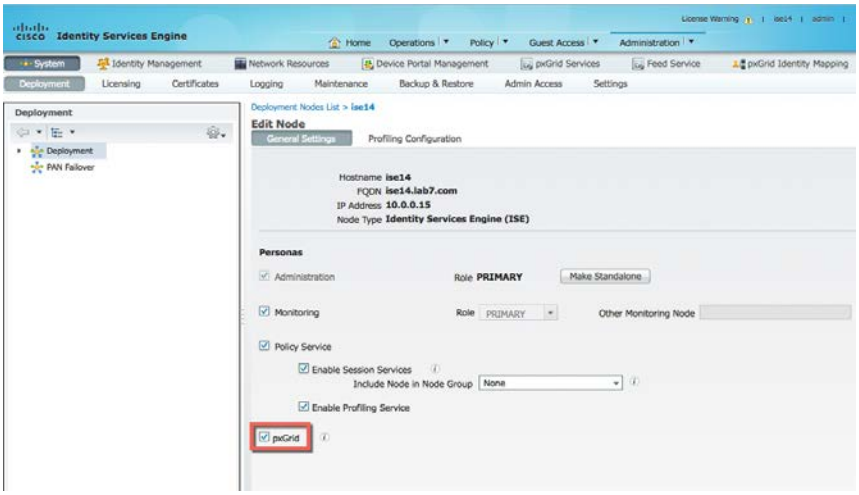
ステップ 2 [証明書のみをエクスポート(Export the certificate only)] を選択し、[エクスポート(Export)] をクリックします。



ステップ 3 ISE 識別自己署名証明書を ISE 信頼ストアにインポートします。
[管理（Administration）] -> [システム（System）] -> [証明書（Certificates）] -> [信頼できる証明書（Trusted Certificates）] -> [インポート（Import）] を選択し、ISE 識別自己署名証明書（PEM）を選択し、[ISE内で認証用に信頼（Trust for authentication within ISE）] をオンにして、[送信（Submit）] を選択します。

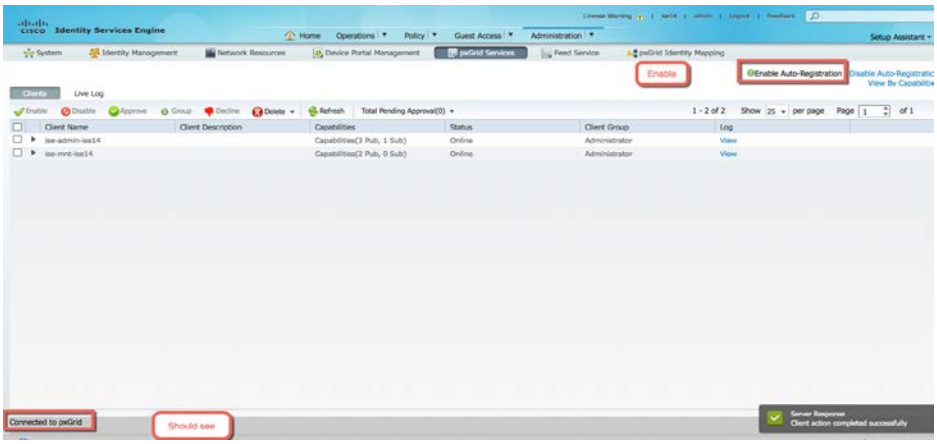


ステップ 4 ISE ノードで pxGrid を有効にします。
[管理（Administration）] -> [システム（System）] -> [導入（Deployment）] を選択し、ノードを選択して、[pxGrid] をオンにし、保存します。



ステップ 5 pxGrid サービスが実行されていることを確認します。
[管理（Administration）] -> [pxGridサービス（pxGrid Services）] を選択して、[自動登録の有効化（Enable Auto Registration）] を [有効（Enable）] にします。

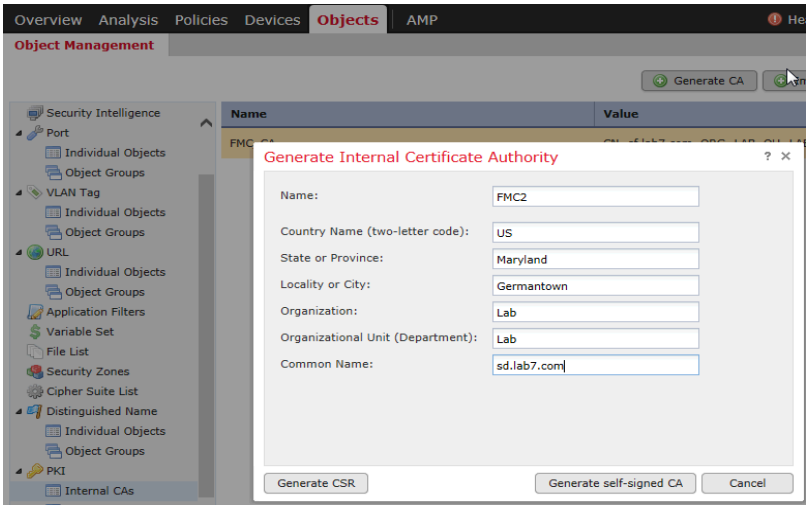
注：接続が表示されるまでに数秒かかる場合があります。



自己署名証明書用の FireSIGHT Management Center の設定

この項では、ISE pxGrid ノード操作で自己署名証明書を使用するために、FireSIGHT Management Center（FMC）を設定します。FireSIGHT Management Center に内部 FMC 認証局が作成され、ISE 証明書システム ストアに対して公開/秘密キー ペアがエクスポートおよびインポートされます。内部 FMC 公開証明書は ISE 証明書信頼システム ストアにエクスポートされます。ISE 識別自己署名公開証明書は FireSIGHT Management Center 信頼 CA ストアにインポートされます。

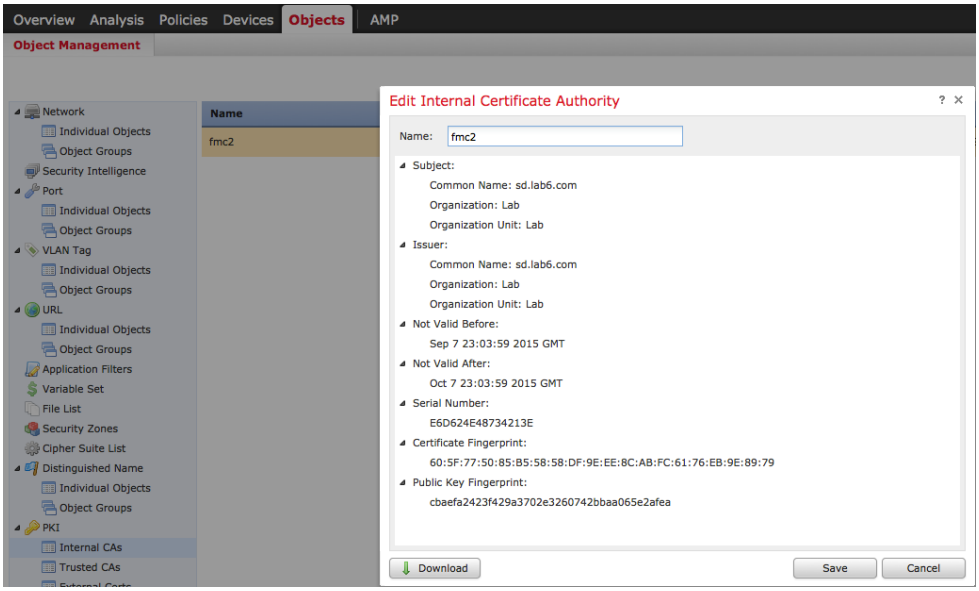
ステップ 1　[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [PKI] -> [内部CA（Internal CAs）] -> [CAの生成（Generate CA）] を選択し、下図のように証明書情報を入力します。
この例では、内部 CA に FMC2 という名前を指定しています。



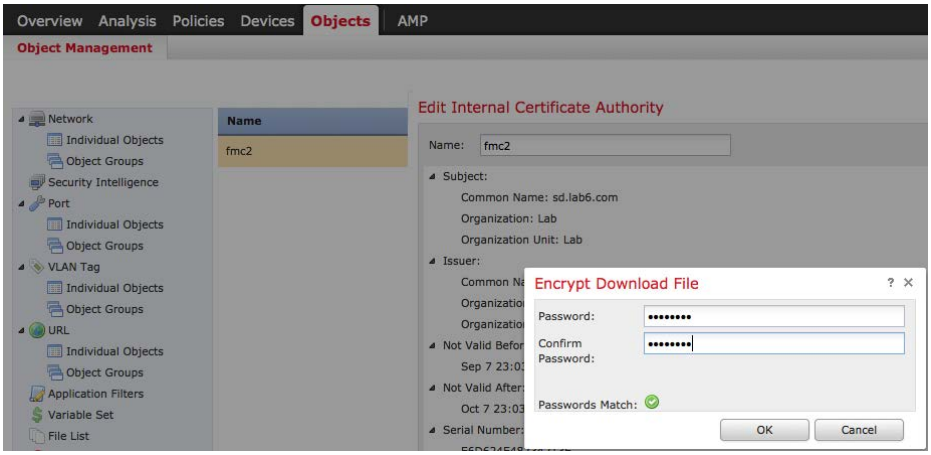
ステップ 2　[自己署名CAの生成（Generate self-signed CA）] をクリックします。

ステップ 3　CA 証明書ファイルをダウンロードします。下図の鉛筆アイコンをクリックします。

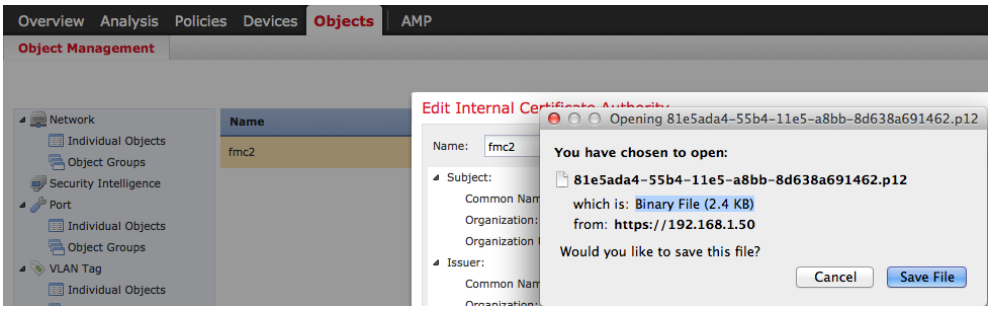
ステップ 4　[ダウンロード（Download）] を選択します。



ステップ 5　暗号化パスワードを入力し、[OK] をクリックします。この例では、cisco123 を使用しています。

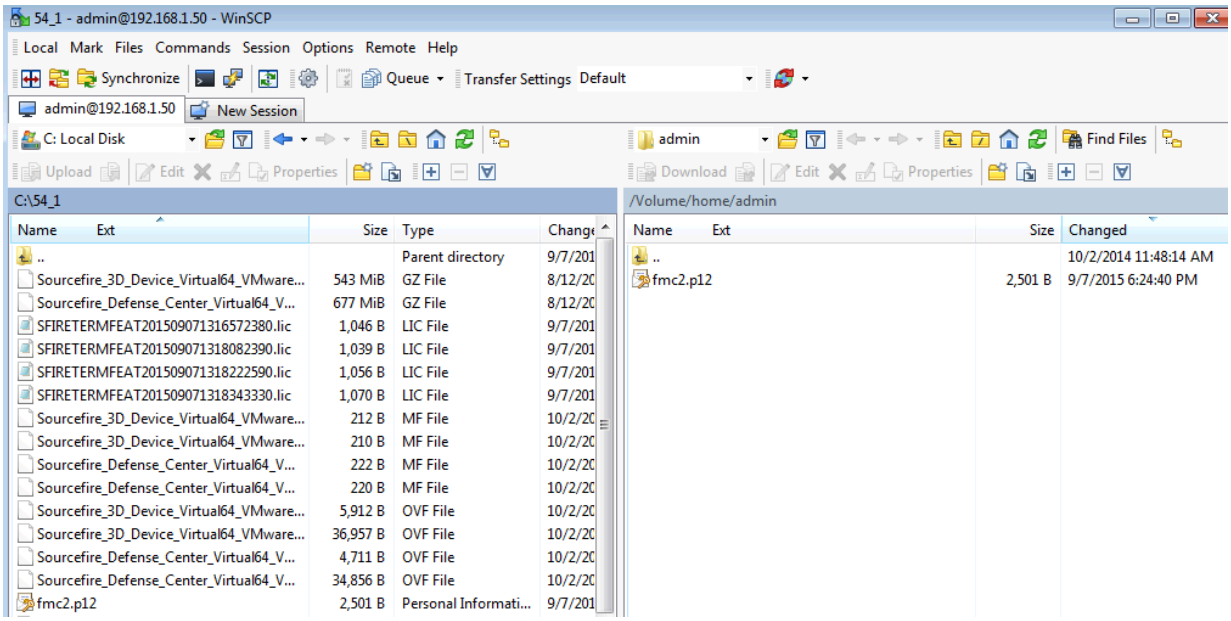


ステップ 6　.p12 ファイルをローカルに保存します。



ステップ 7　使用しやすいように .p12 ファイル名を変更します。この例では、fmc2.p12 が名前を変更したファイルです。

ステップ 8 WinSCP または別の方法を使用して、FireSIGHT Management Console にファイルをアップロードします。



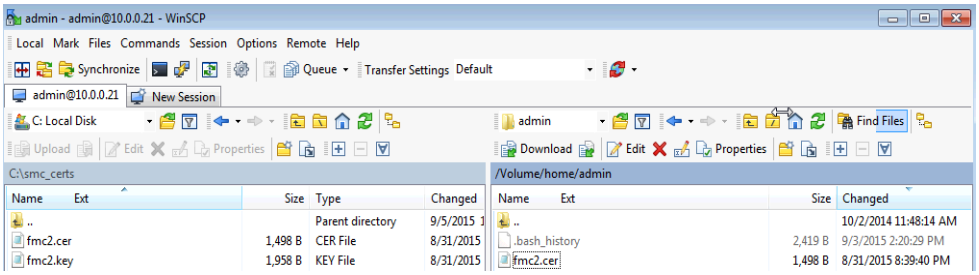
ステップ 9 FireSIGHT Management Console に SSH で接続します。

ステップ 10 次のコマンドを入力して、.p12 ファイルを CER および KEY ファイルに変換します。

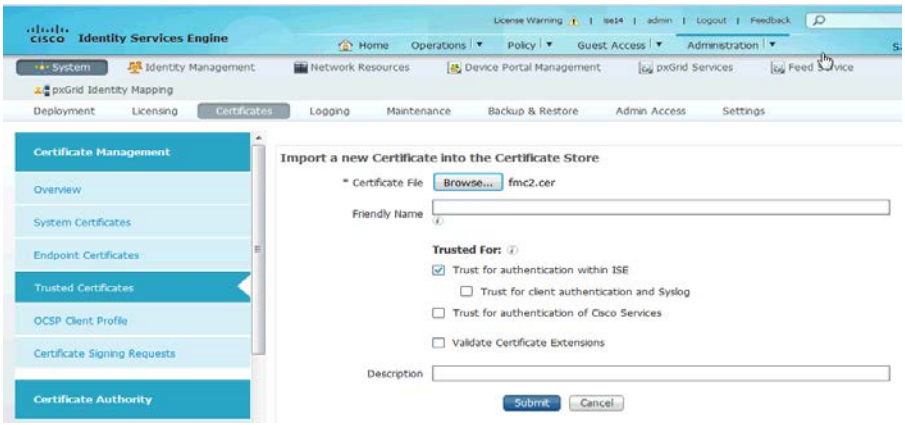
注:CER および KEY ファイル名は任意です。元の .p12 ファイルは fmc2.p12 に名前を変更してあります。

```
sudo openssl pkcs12 -nokeys -clcerts -in fmc2.p12 -out fmc2.cer
Enter Import Password:
MAC verified OK
admin@sd:~$



sudo openssl pkcs12 -nocerts -in fmc2.p12 -out fmc2.key
Enter Import Password:
MAC verified OK
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
admin@sd:~$
```

ステップ 11 WinSCP を使用して、fmc2.cer および fmc2.key ファイルを FireSIGHT Management Center からローカル PC にコピーしました。



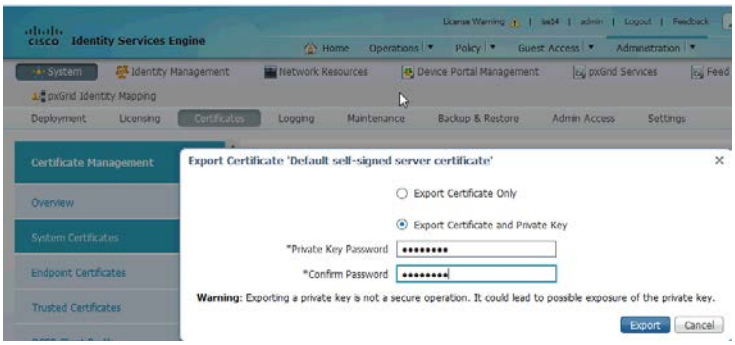
ステップ 12 FireSIGHT Management 内部 CA 公開証明書は ISE 証明書信頼ストアにエクスポートされました。[管理（Administration）] -> [システム（System）] -> [証明書（Certificates）] -> [信頼できる証明書（Trusted Certificates）] で [参照（Browse）] を選択し、**fmc2.cer** をアップロードします。



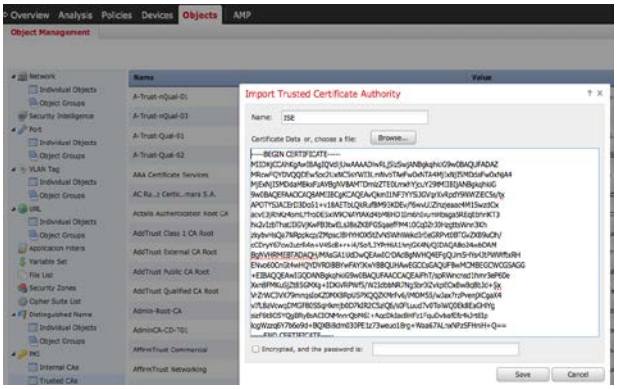
ステップ 13 [ISE内認証の信頼（Trust for authentication within ISE）] をオンにし、[送信（Submit）] をクリックします。

ステップ 14 ISE 信頼証明書ストアから、ISE 識別自己署名公開証明書と秘密キーの両方をエクスポートします。ISE 識別自己署名公開証明書のみを FireSIGHT Management 信頼 CA ストアにエクスポートする必要があります。FireSIGHT Management Console はこれを信頼できる証明書として認識します。[管理（Administration）] -> [システム（System）] -> [証明書（Certificates）] -> [証明書管理（Certificate Management）] -> [信頼できる証明書（Trusted Certificates）] を選択し、ISE 証明書を選択して、公開キーと秘密キーの両方をエクスポートし、パスワードを指定します。

注：この手順は、ISE 2.0 でも同じです。

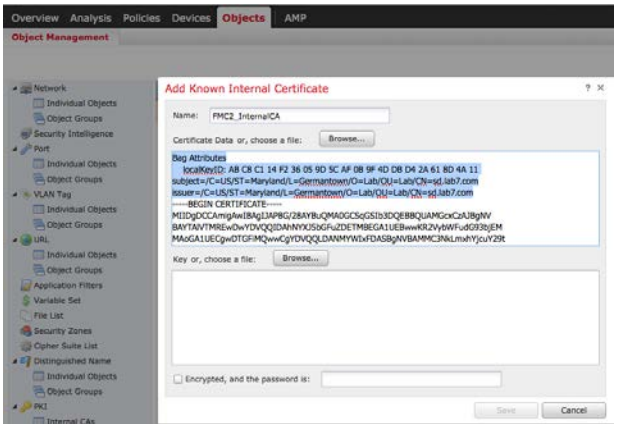


ステップ 15 ISE 自己署名識別証明書を FireSIGHT Management 信頼 CA ストアにインポートします。[オブジェクト（Objects）] -> [オブジェクト管理（Object Management）] -> [PKI] -> [信頼できるCA（Trusted CAs）] -> [信頼できるCAの追加（Add Trusted CA）] を選択し、名前を入力して、保存します。

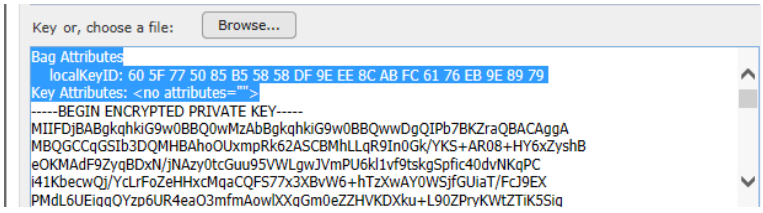


ステップ 16　FireSIGHT Management 内部 CA の公開/秘密キー ペアを FireSIGHT Management Center の内部証明書ストアにインポートします。
[オブジェクト（Objects）] -> [オブジェクト管理（Object Management）] -> [PKI] -> [内部証明書（Internal Certs）] -> [内部証明書の追加（Add Internal Cert）] を選択します。
秘密キーについても同じ手順に従います。

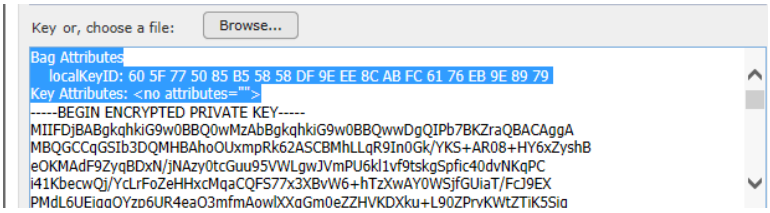
注:----Begin Certificates が始まるまでの Bag 属性を削除してください。



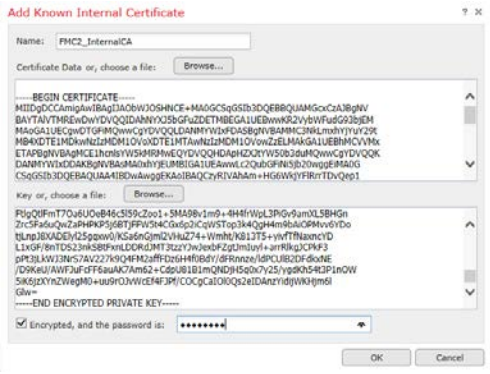
ステップ 17　「---Begin…」の前のキー ファイルの Bag 属性を削除します。



ステップ 18　</no> も削除し、暗号化パスワードを入力します。



ステップ 19　次のように表示されるので、[OK] をクリックして完了します。



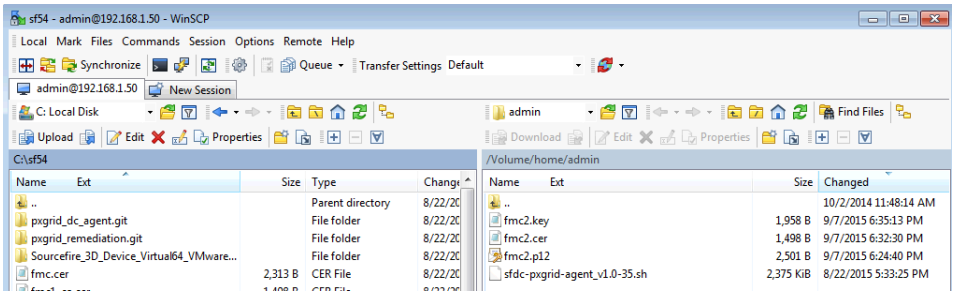
自己署名証明書を使用する pxGrid エージェントの設定

pxGrid エージェントは FireSIGHT Management Center と ISE pxGrid ノード間の証明書の設定と通信を行います。ISE pxGrid ノードの IP アドレスが必要です。FireSIGHT Management Center の公開証明書とキー ファイルは、次のステップに必要です。

FireSIGHT Management Center の公開証明書はホスト証明書として機能します。ISE 識別自己署名証明書は CA 証明書として機能します。

FireSIGHT Management Center の秘密キー ファイルはホスト キーです。キーのパスワードも必要です。

ステップ 1　WinSCP または 別の SCP/SFTP クライアントを使用して、pxGrid エージェントを FireSIGHT Management Console にアップロードします。

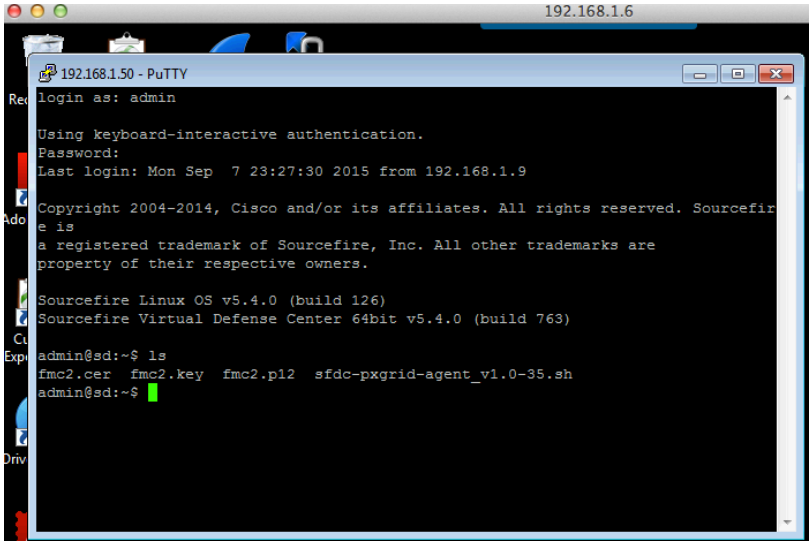


ステップ 2　WinSCP またはその他の方法を使用して、FireSIGHT 内部 CA 公開証明書、内部 CA キーを FireSIGHT MC の /Volume/home/admin へアップロードします。

注：構文の大文字と小文字は区別されます。

ステップ 3　FireSIGHT Management Center に SSH で接続して、次のように入力します。

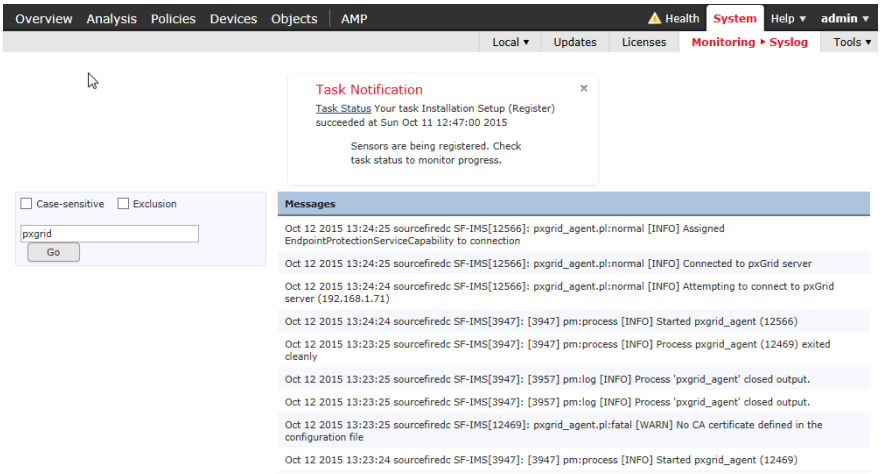
```
sudo bash sfdc-pxgrid_agent_v1.0.35.sh
```



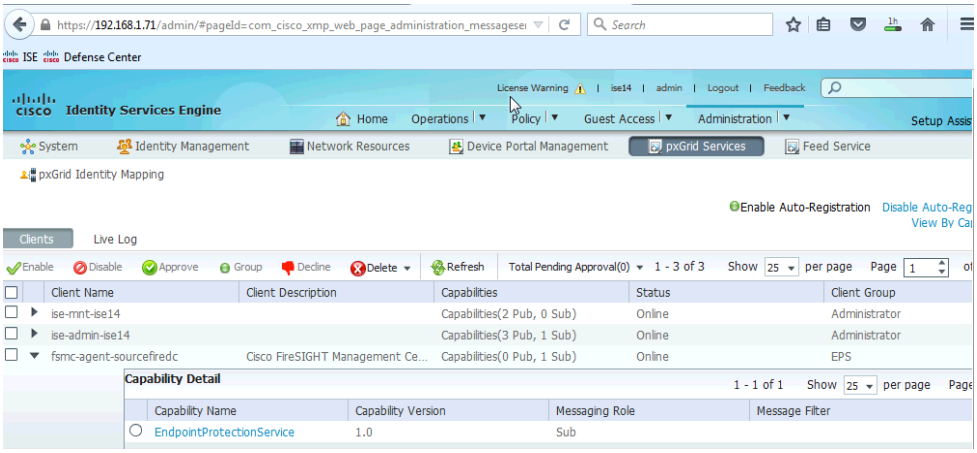
サンプル スクリプトについては、以下を参照してください。

```
Verifying archive integrity... All good.
Uncompressing Cisco pxGrid Agent Installer......
Installing the agent...
Installing the pxGrid libraries and Perl module...
Setting up the agent to be managed by PM...
Installation done!

Configuring pxGrid...

Below you will be asked a series of questions relating to your pxGrid install
and the files supporting it. Health alerts WILL be generated by PM until the
configuration is completed, however. The answers to these questions will
populate the /etc/sf/pxgrid/pxgrid.conf configuration file, which can be
manually modified later at any time. A configuration example is provided in the
same directory with the filename pxgrid.conf.example.


To get this all to work, the agent will need to connect to a pxGrid server.
This is typically your Cisco Identity Services Engine instance, which must also
have the pxGrid service enabled.

What is the IP address of your pxGrid server
> 192.168.1.71

Every agent connecting to pxGrid must have a unique host certificate which will
be used to identify the agent host. Associated key and CA certs must also be
provided.

What is the full path and filename to the host certificate?
> /Volume/home/admin/fmc2.cer
What is the full path and filename to the host key?
> /Volume/home/admin/fmc2.key
What is the host key password?
> cisco123
What is the full path and filename to the CA certificate?
> /Volume/home/admin/ise14lab.pem

Configuration witten to /etc/sf/pxgrid/pxgrid.conf
```

ステップ 4 [システム（System）] -> [モニタリング（Monitoring）] -> [Syslog（Syslog）] を選択し、FireSIGHT Management Center が ISE pxGrid ノードをクライアントとして正常に登録し、EPS トピックにサブスクライブしたことを確認します。



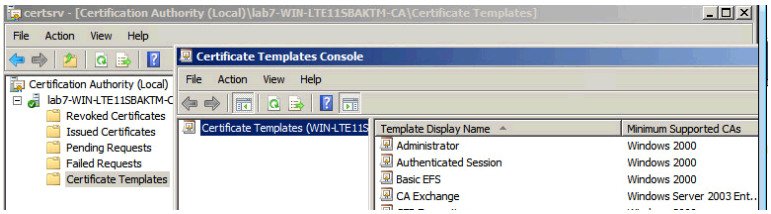
ステップ 5 ISEで表示するには、[管理（Administration）] -> [pxGridサービス（pxGrid Services）] を選択します。FireSIGHT Management Console は ISE pxGrid ノードの EndpointProtectionService 機能に登録されている点に注意してください。



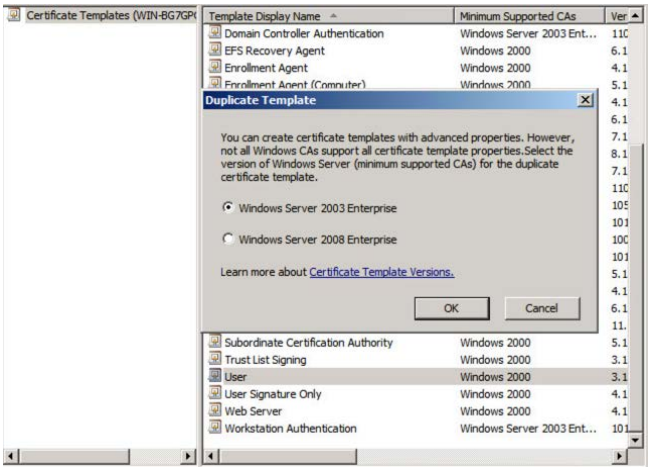
CA 署名操作用にカスタマイズされた pxGrid テンプレート

pxGrid クライアント、FireSIGHT Management Center、および ISE pxGrid ノード間の pxGrid 操作には、クライアント認証とサーバ認証の両方の Enhanced Key Usage（EKU）を持つ、カスタマイズされた pxGrid テンプレートが必要です。これは、FireSIGHT Management Center と ISE pxGrid のノードの両方が同じ CA によって署名された認証局（CA）署名環境で必要です。

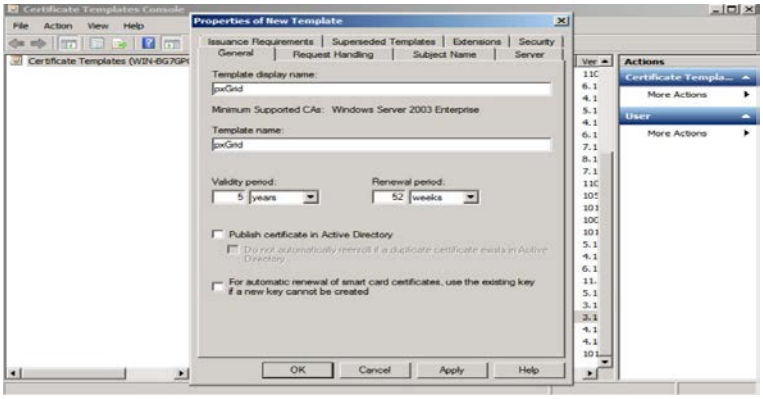
ステップ 1　[管理ツール（Administrative Tools）] -> [証明機関（Certificate Authority）] を選択し、CA サーバの横の [+] をクリックして、ドロップダウン リストから [証明書テンプレート（Certificate Templates）] を右クリックして、[管理（Manage）] を選択します。



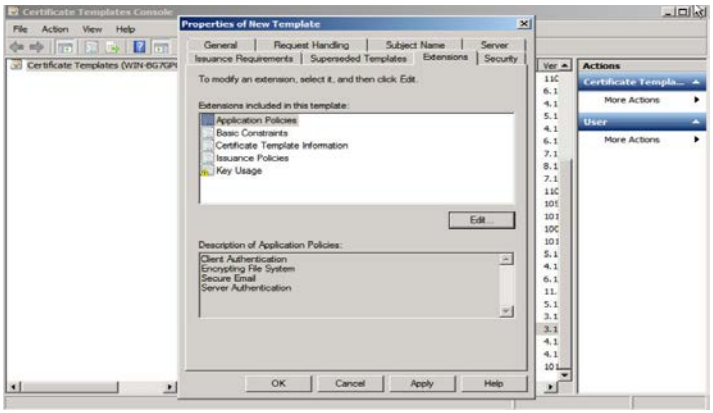
ステップ 2　右クリックして、[ユーザテンプレートの複製（Duplicate User template）] を選択し、[Windows 2003 Enterprise] を選択して、[OK] をクリックします。



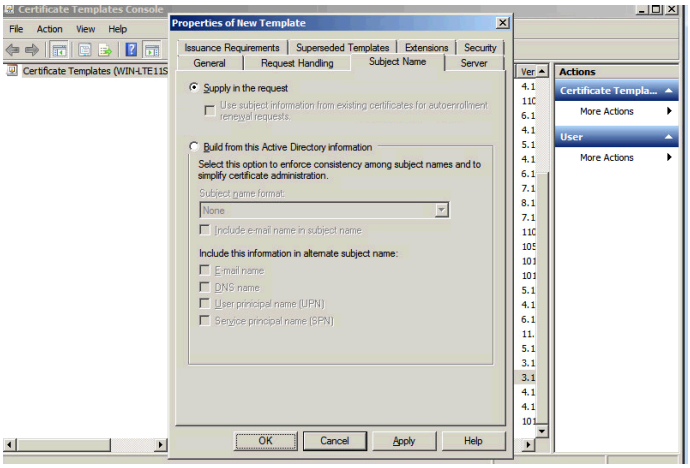
ステップ 3　証明書テンプレートの名前を入力し、[Active Directory の証明書を発行する（Publish certificate in Active Directory）] をオフにして、有効期間および更新期間を指定します。



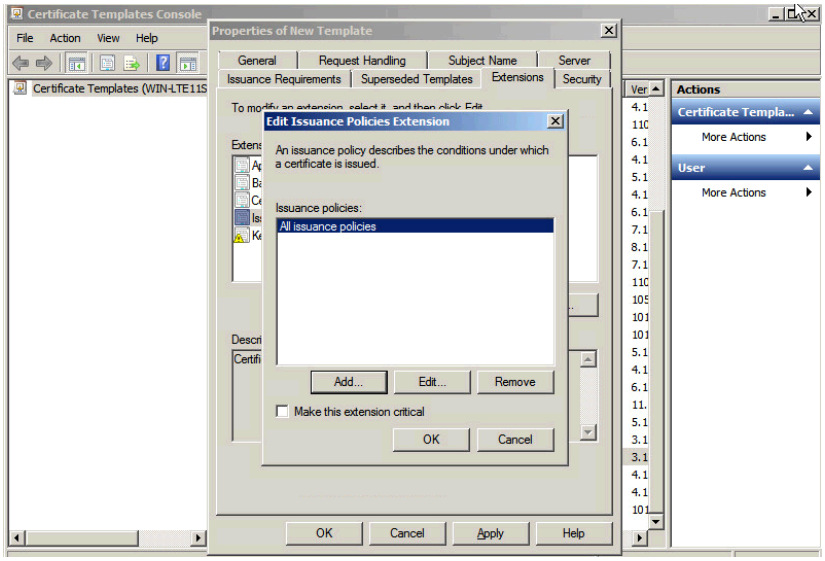
ステップ 4 [拡張(Extensions)] -> [追加(Add)] -> [サーバ認証(Server Authentication)] -> [OK] -> [適用(Apply)] の順にクリックします。



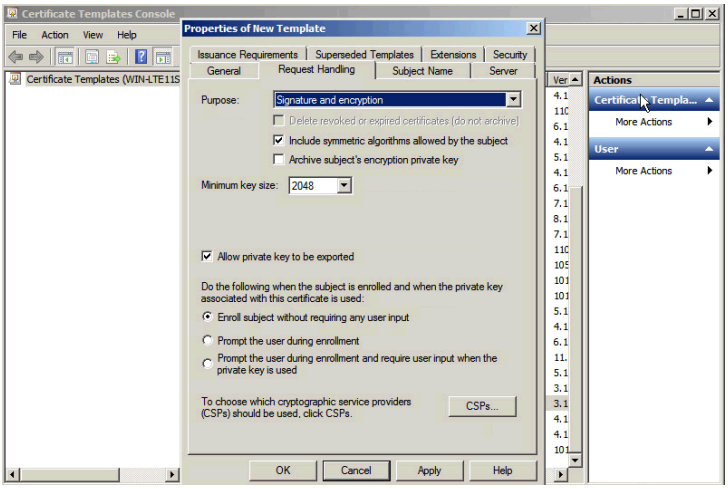
ステップ 5 [サブジェクト名(Subject name)] をクリックして、[要求に含まれる(Supply in request)] をオンにします。



ステップ 6　[拡張（Extensions）] -> [発行ポリシー（Issuance Policies）] -> [編集（Edit）] -> [すべての発行ポリシー（All Issuance Policies）] の順にクリックします。

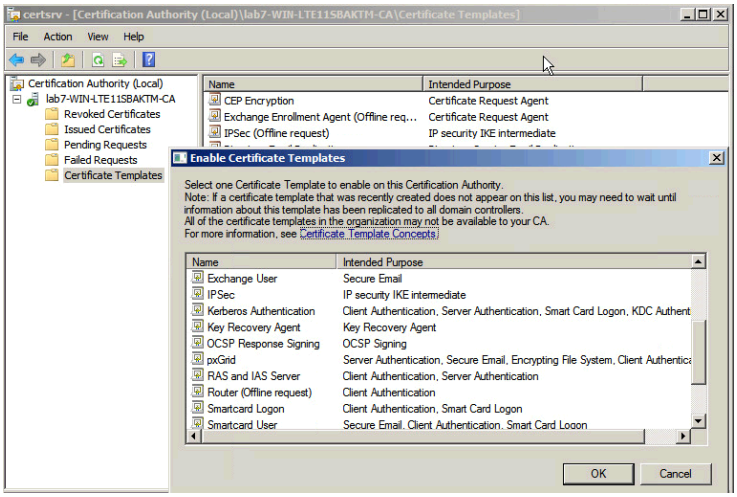


ステップ 7　要求処理をデフォルトのままにします。

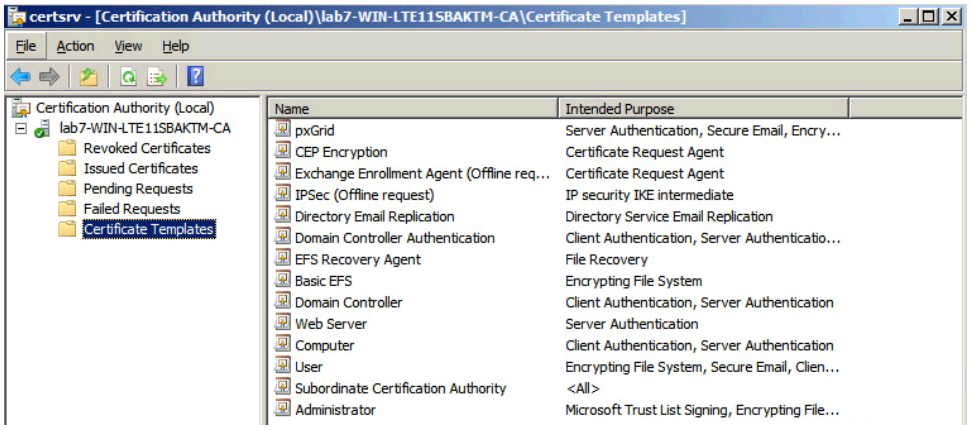


ステップ 8　右クリックして、[証明書テンプレート（Certificate templates）] をクリックします。

ステップ 9　発行する [新規テンプレート（New Template）] を選択し、[pxGrid] を選択します。



ステップ 10　pxGrid のテンプレートが表示されます。



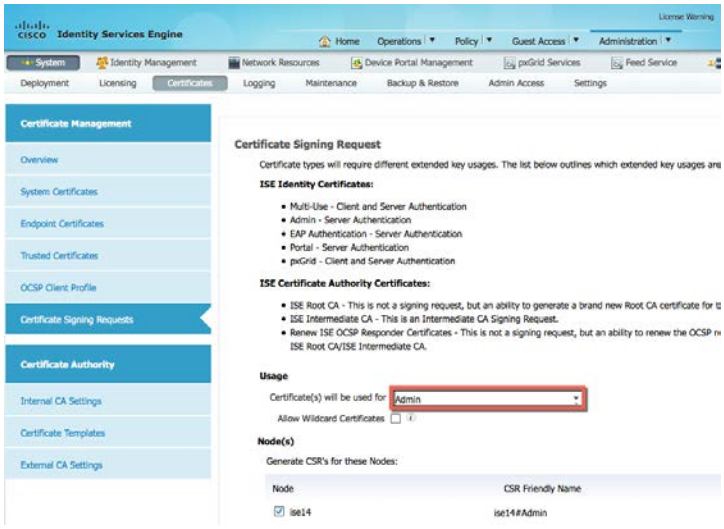
pxGrid を使用したスタンドアロン環境の CA 署名証明書用の ISE の設定

この項では、認証局（CA）によって署名された環境用に ISE pxGrid ノードを設定します。最初に、「pxGrid」CSR 要求が ISE ノードから生成され、pxGrid のカスタマイズされたテンプレートを使用して、CA サーバによって署名されます。証明書は最初の ISE CSR 要求にバインドされます。

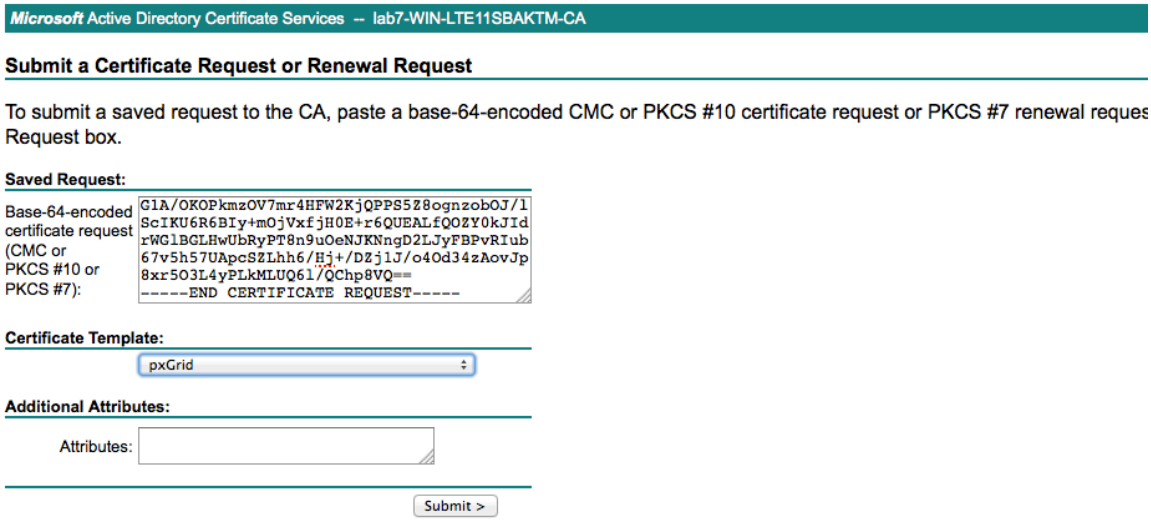
CA ルート証明書は ISE 証明書信頼ストアにインポートされます。ISE ID 識別証明書は ISE 証明書システム ストアにエクスポートされます。ISE ノードは pxGrid 操作用に有効化されます。

ステップ 1　ISE pxGrid ノードになる ISE ノードの CSR 要求を生成します。
[管理（Administration）] -> [システム（System）] -> [証明書（Certificates）] -> [証明書署名要求（Certificate Signing Requests）] -> [生成（Generate）] を選択します。

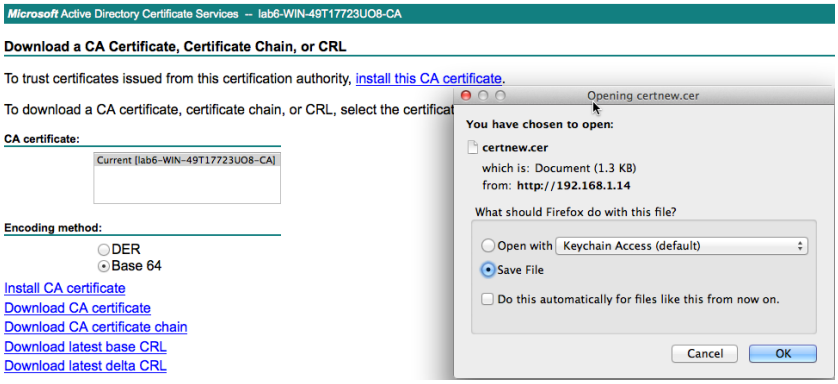
注：証明書用途は、テンプレートが pxGrid のカスタマイズされたものである限り、管理、多目的、または pxGrid のいずれかにすることができます。



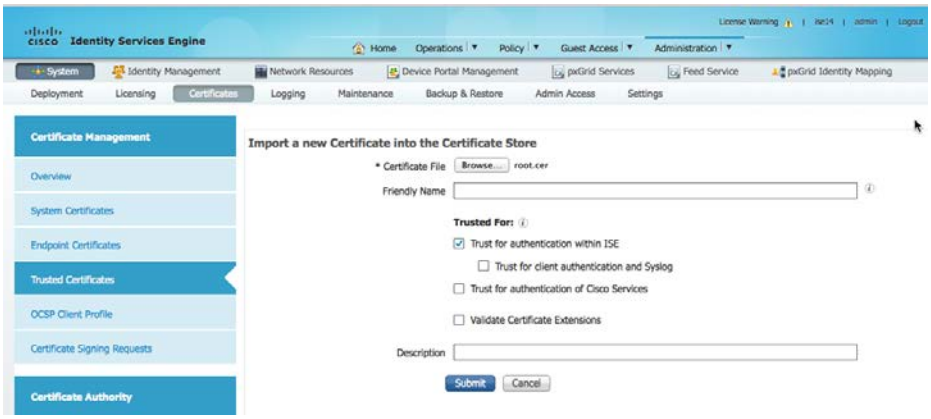
ステップ 2　[証明書の要求（Request a certificate）] -> [証明書の要求の詳細設定（Advanced Certificate request）] を選択し、CSR 情報をコピーして貼り付け、カスタマイズされた pxGrid テンプレートを選択して、[送信（Submit）] をクリックします。



ステップ 3 Base 64 符号化形式の CA ルートをダウンロードします。

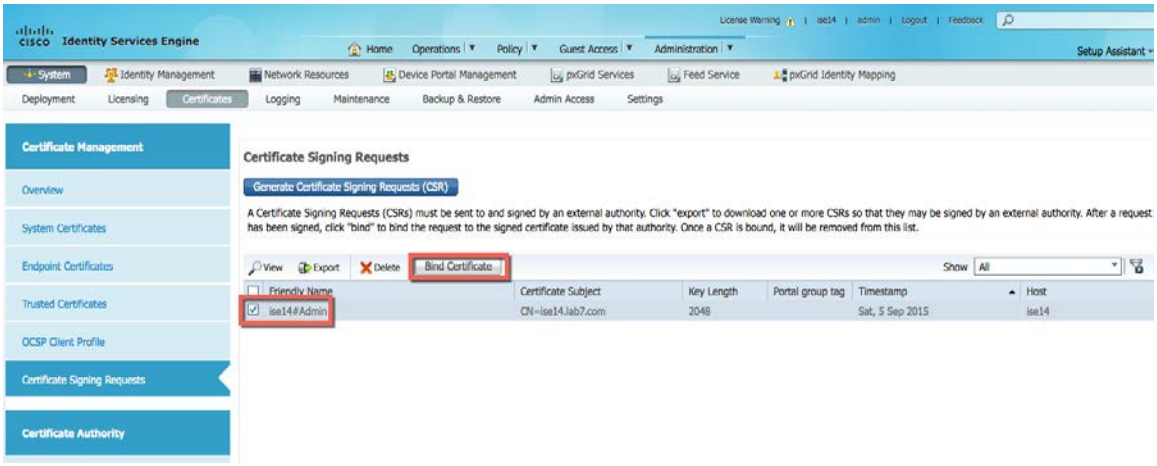


ステップ 4 CA ルートを ISE 証明書信頼システム ストアにアップロードします。
[管理（Administration）] -> [システム（System）] -> [証明書（Certificates）] -> [信頼できる証明書（Trusted Certificates）] を選択し、CA ルート証明書をアップロードします。

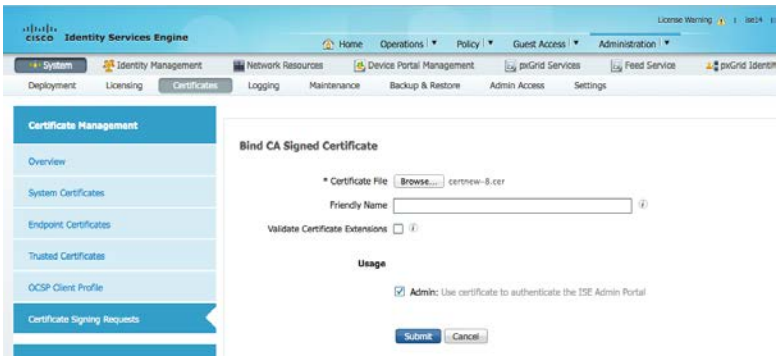


ステップ 5 [ISE内認証の信頼（Trust for authentication within ISE）] を有効にし、[送信（Submit）] をクリックします。

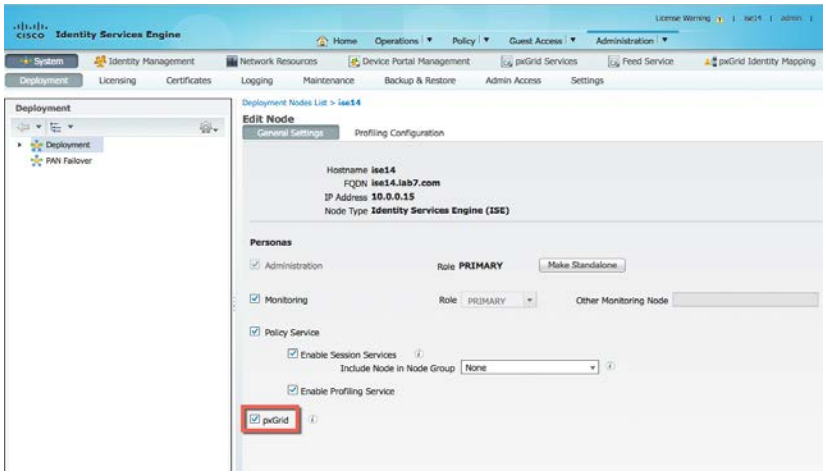
ステップ 6　ISE pxGrid ノード証明書を ISE 証明書システム ストアにアップロードします。[管理（Administration）] -> [システム（System）] -> [証明書署名の要求（Certificate Signing Requests）] を選択し、証明書を CSR 要求にバインドします。



ステップ 7　**ISE pxGrid ノード証明書を参照およびアップロードし、送信します。**

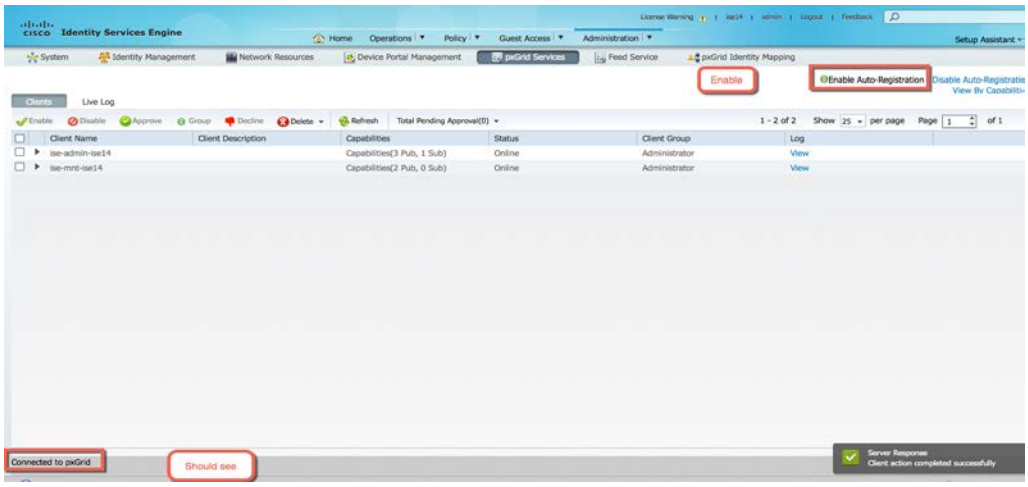


ステップ 8　ISE ノードで pxGrid を有効にします。[管理（Administration）] -> [システム（System）] -> [導入（Deployment）] を選択し、ISE ノードを強調表示して、pxGrid ペルソナを有効にします。



ステップ 9 pxGrid サービスが実行されていることを確認し、[自動登録の有効化（Enable Auto Registration）] を選択します。
[管理（Administration）] > [pxGridサービス（pxGrid services）] を選択します。

注: pxGrid サービスは表示に数秒かかる場合があります。



CA 署名証明書用の FireSIGHT Management Center の設定

この項では、認証局（CA）署名証明書の操作用に、FireSIGHT Management Center（FMC）を設定します。FireSIGHT Management Center の秘密キーと CSR 要求は FireSIGHT Management Center コンソール（FMC）から作成します。CA サーバは CSR 要求に署名し、カスタマイズされた pxGrid テンプレートを使用して、FMC 識別証明書を提供します。

FMC 証明書と FMC キーは両方とも FMC 内部証明書ストアにアップロードされます。CA ルート証明書は FMC 信頼 CA ストアにアップロードされます。

ステップ 1　FireSIGHT 秘密キーを生成します。

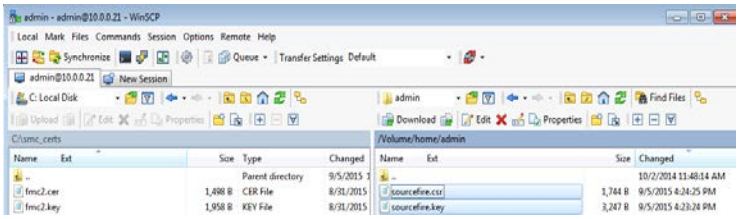
注：ここで、パスワードは pxGrid エージェント設定で定義されます。

```
openssl genrsa -des3 -out sourcefire.key 4096
```

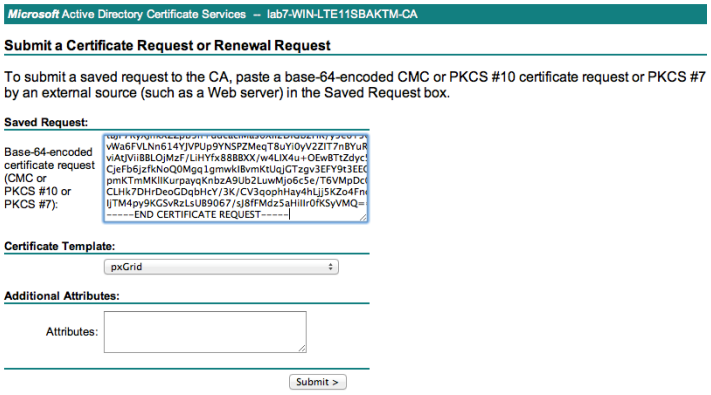
ステップ 2　CSR 要求を生成します。

```
openssl req -new -key sourcefire.key -out sourcefire.csr
```

ステップ 3　WinSCP を使用して、ファイルを FireSIGHT Management Center（FMC）からローカルの PC にコピーします。

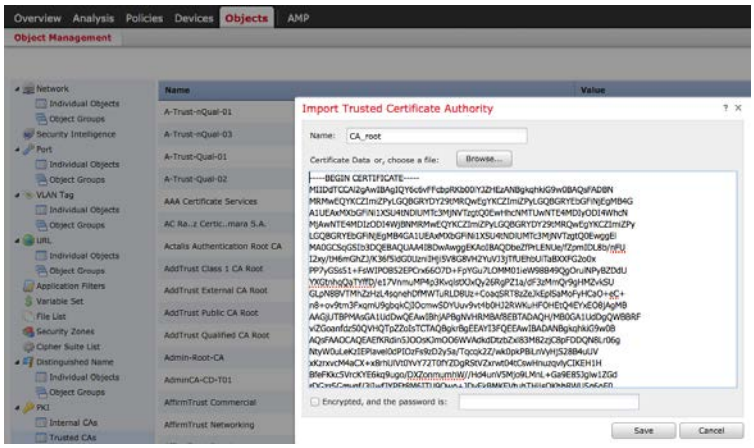


ステップ 4　カスタマイズされた pxGrid テンプレートを使用し、[証明書の要求（Request a certificate）] -> [詳細ユーザ要求（Advanced User request）] を選択し、FMC CSR 要求をコピーして貼り付け、送信します。Base 64 符号化形式の証明書をダウンロードします。

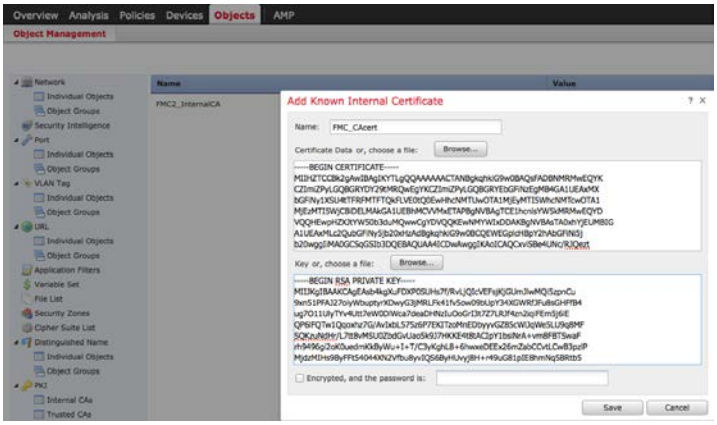


ステップ 5 Base 64 符号化形式の CA ルート証明書をダウンロードします。

ステップ 6 CA ルート証明書を FireSIGHT Management 信頼 CA ストアにアップロードします。
[オブジェクト（Objects）] -> [オブジェクト管理（Object Management）] -> [PKI] -> [信頼できるCA（Trusted CAs）] -> [信頼できるCAの追加（Add Trusted CA）] を選択し、名前を入力して、ルート CA をアップロードし、保存します。



ステップ 7 FireSIGHT Management Center 公開証明書と秘密キーを FMC 内部証明書ストアにアップロードします。
[オブジェクト（Objects）] -> [オブジェクト管理（Object Management）] -> [PKI] -> [内部証明書（Internal Certs）] を選択し、Sourcefire CER ファイルと Sourcefire KEY ファイルを追加して、保存します。



CA 署名証明書を使用する pxGrid エージェントの設定

pxGrid エージェントは FireSIGHT Management Center と ISE pxGrid ノード間の証明書の設定と通信を行います。ISE pxGrid ノードの IP アドレスが必要です。FireSIGHT Management Center の公開証明書とキー ファイルが必要です。

FireSIGHT Management Center の公開証明書はホスト証明書として機能します。CA ルート証明書は CA 証明書として機能します。

FireSIGHT キー ファイルはホスト キーです。キーのパスワードも必要です。

ステップ 1 WinSCP を使用して、pxGrid エージェントを FireSIGHT Management Console にアップロードします。

ステップ 2 WinSCP またはその他の方法を使用して、FireSIGHT 公開証明書、FireSIGHT CA キー、および CA ルート証明書を FireSIGHT MC /Volume/home/admin へアップロードします。

注:構文の大文字と小文字は区別されます。

ステップ 3 FireSIGHT Management Center に SSH で接続して、次のように入力します。

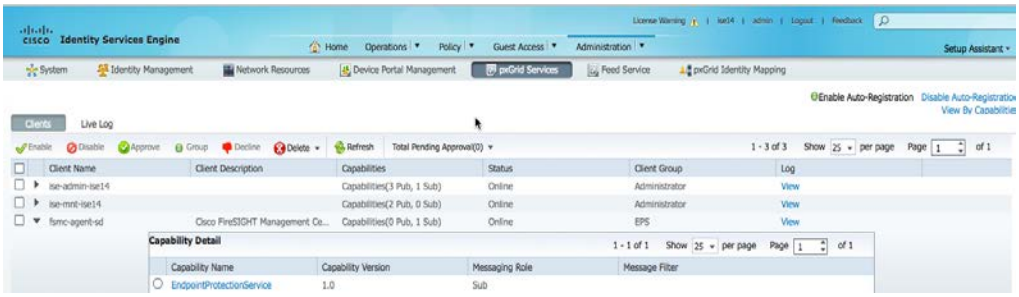
```
sudo bash sfdc-pxgrid_agent_v1.0.35.sh
```

サンプル スクリプトについては、以下を参照してください。

```
Verifying archive integrity... All good.
Uncompressing Cisco pxGrid Agent Installer......
Installing the agent...
Installing the pxGrid libraries and Perl module...
Setting up the agent to be managed by PM...
Installation done!

Configuring pxGrid...

Below you will be asked a series of questions relating to your pxGrid install
and the files supporting it. Health alerts WILL be generated by PM until the
configuration is completed, however. The answers to these questions will
populate the /etc/sf/pxgrid/pxgrid.conf configuration file, which can be
manually modified later at any time. A configuration example is provided in the
same directory with the filename pxgrid.conf.example.
```

```
To get this all to work, the agent will need to connect to a pxGrid server.
This is typically your Cisco Identity Services Engine instance, which must also
have the pxGrid service enabled.

What is the IP address of your pxGrid server
> 10.0.0.0.15

Every agent connecting to pxGrid must have a unique host certificate which will
be used to identify the agent host. Associated key and CA certs must also be
provided.

What is the full path and filename to the host certificate?
> /Volume/home/admin/sourcefire.cer
What is the full path and filename to the host key?
> /Volume/home/admin/sourcefire.key
What is the host key password?
> cisco123
What is the full path and filename to the CA certificate?
> /Volume/home/admin/root.cer

Configuration witten to /etc/sf/pxgrid
```

ステップ 4 FireSIGHT Management Center は pxGrid クライアントとして正常に登録され、EPS 公開済みトピックにサブスクライブされました。
[管理（Administration）] > [pxGridサービス（pxGrid Services）] を選択します。



FireSIGHT pxGrid 修復モジュール

この項では、pxGrid 軽減修復モジュールを FireSIGHT Management Center にアップロードします。pxGrid インスタンスを作成し、修復タイプを定義します。これらの修復タイプは、それぞれの相関ポリシーへの応答として割り当てられるときに pxGrid ANC 機能を提供します。

これらの修復のタイプは次のとおりです。

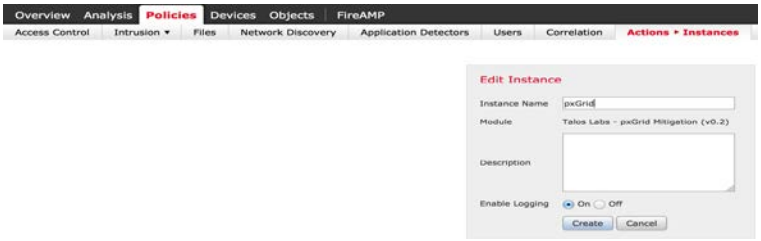
- **検疫** - 送信元 IP アドレスに基づいてエンドポイントを検疫します。
- **ポートバウンス** - エンドポイントまたはホスト ポートを一時的にバウンスします。
- **強制終了** - エンドユーザ セッションを強制終了します。
- **シャットダウン** - ホスト ポートのシャットダウンを開始します。これにより、スイッチ ポートの設定に「shutdown」コマンドが挿入されします。
- **再認証** - エンドユーザを再認証します。
- **検疫解除** - エンドポイントの検疫を解除します。

FireSIGHT pxGrid 修復モジュールのアップロード

ステップ 1 pxGrid 修復モジュールを FireSIGHT Management Center にアップロードします。[ポリシー（Policies）] -> [アクション（Actions）] -> [修復（Remediations）] -> [モジュール（Modules）] -> [新規モジュールのインストール（Install a new module）] を選択し、モジュール ファイル pxGrid_Mitigation_Remediation_v1.0.tgz を参照して、アップロードします。

新しいインスタンスの作成

ステップ 1 新しい pxGrid インスタンスを作成します。[ポリシー（Policies）] -> [アクション（Actions）] -> [修復（Remediations）] -> [インスタンス（Instances）] -> [新規インスタンスの追加（Add a new Instance）] -> [モジュールタイプ（Module type）] -> [Talos Labs-pxGrid軽減（Talos Labs-pxGrid mitigation）] -> [追加（Add）] を選択し、[インスタンス名（Instance Name）] を **pxGrid** として [作成（Create）] を選択します。



FireSIGHT pxGrid 軽減タイプの作成

これらの修復のタイプは、エンドポイントの修復アクションを呼び出す相関ルールに対する応答として割り当てられる pxGrid ANC の軽減アクションを定義します。

注:選択するには虫めがねをクリックします。

検疫

軽減ソースに基づいて検疫の軽減アクションを作成します。

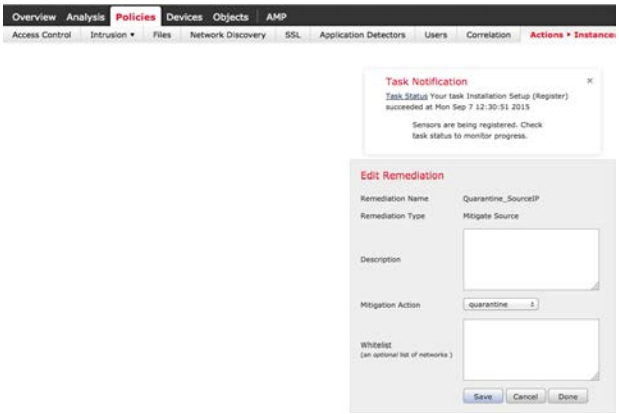
ステップ 1 [ポリシー(Policies)] -> [アクション(Actions)] -> [修復(Remediations)] -> [モジュール(Modules)] -> [Talos Labs- pxGrid軽減(Talos Labs- pxGrid Mitigation)] を選択し、設定済みインスタンスの pxGrid を選択します。

ステップ 2 「虫めがね」-> [軽減ソースに基づいて新しい修復タイプを追加(Add a new remediation type based on Mitigate Source)] をクリックします。

ステップ 3 修復名に **Quarantine_SourceIP** と入力します。

ステップ 4 軽減アクションには、ドロップダウン メニューから [検疫(quarantine)] を選択します。

ステップ 5 [保存(Save)] をクリックします。



ポートバウンス

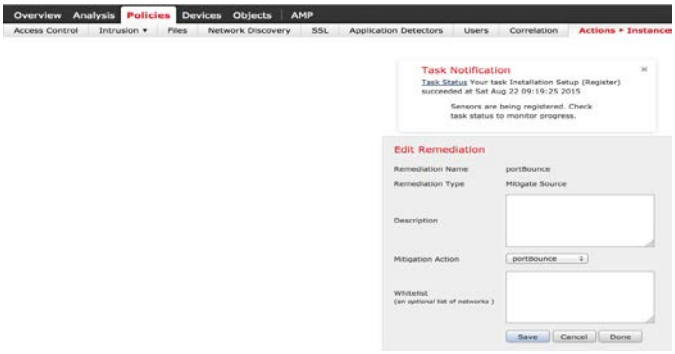
軽減ソースに基づいてポートバウンスの軽減アクションを作成します。

ステップ 1 [ポリシー(Policies)] -> [アクション(Actions)] -> [インスタンス(Instances)] を選択し、設定済みインスタンスの [pxGrid] の横の虫めがねをクリックします。

ステップ 2 ドロップダウンから [軽減ソース(Mitigate Source)] を選択し、[追加(Add)] をクリックします。

ステップ 3 修復名に **portBounce** と入力します。

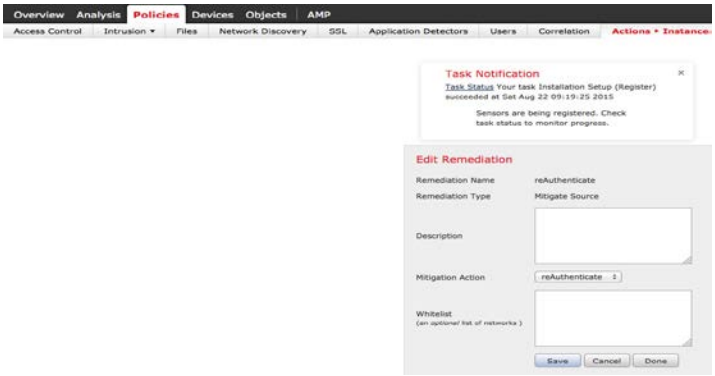
ステップ 4 軽減アクションには、ドロップダウン メニューから [ポートバウンス(portBounce)] を選択します。
ステップ 5 [保存(Save)] をクリックします。



再認証

軽減ソースに基づいて再認証の軽減アクションを作成します。

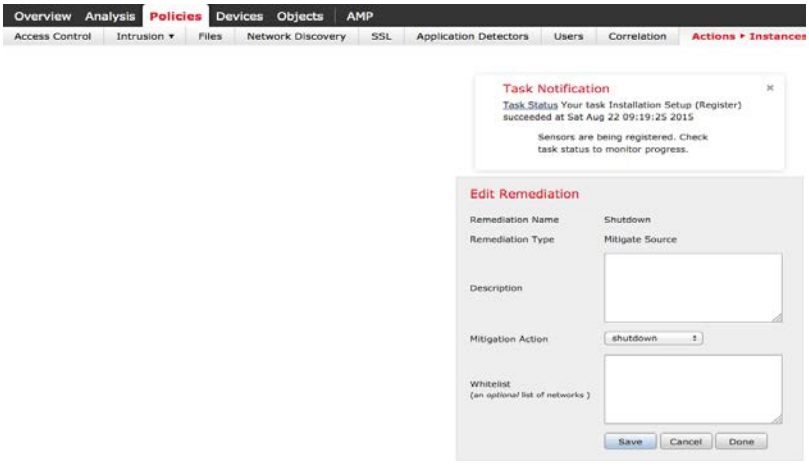
ステップ 1 [ポリシー(Policies)] -> [アクション(Actions)] -> [インスタンス(Instances)] を選択し、設定済みインスタンスの [pxGrid] の横の虫めがねをクリックします。
ステップ 2 ドロップダウンから [軽減ソース(Mitigate Source)] を選択し、[追加(Add)] をクリックします。
ステップ 3 修復名に **reAuthenticate** と入力します。
ステップ 4 軽減アクションには、ドロップダウン メニューから [再認証(reAuthenticate)] を選択します。
ステップ 5 [保存(Save)] をクリックします。



シャットダウン

軽減ソースに基づいてシャットダウン軽減アクションを作成します。

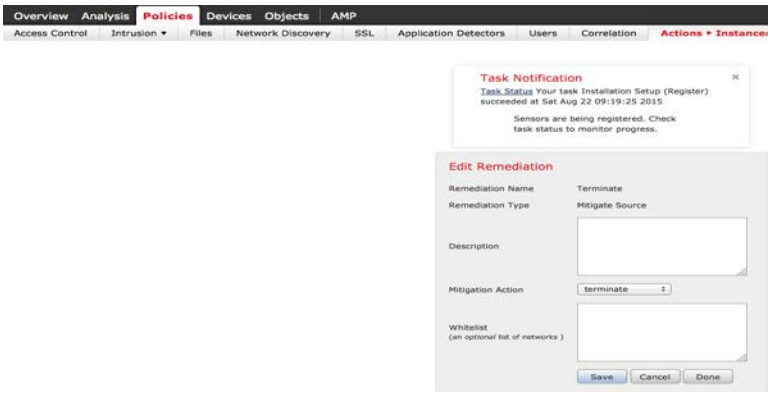
ステップ 1 [ポリシー(Policies)] -> [アクション(Actions)] -> [インスタンス(Instances)] を選択し、設定済みインスタンスの [pxGrid] の横の虫めがねをクリックします。
ステップ 2 ドロップダウンから [軽減ソース(Mitigate Source)] を選択し、[追加(Add)] をクリックします。
ステップ 3 修復名に **Shutdown** と入力します。
ステップ 4 軽減アクションには、ドロップダウン メニューから [シャットダウン(shutdown)] を選択します。
ステップ 5 [保存(Save)] をクリックします。



強制終了

軽減ソースに基づいて強制終了の軽減アクションを作成します。

ステップ 1 [ポリシー（Policies）] -> [アクション（Actions）] -> [インスタンス（Instances）] を選択し、設定済みインスタンスの [pxGrid] の横の虫めがねをクリックします。
ステップ 2 ドロップダウンから [軽減ソース（Mitigate Source）] を選択し、[追加（Add）] をクリックします。
ステップ 3 修復名に **Terminate** と入力します。
ステップ 4 軽減アクションには、ドロップダウン メニューから [強制終了（terminate）] を選択します。
ステップ 5 [保存（Save）] をクリックします。

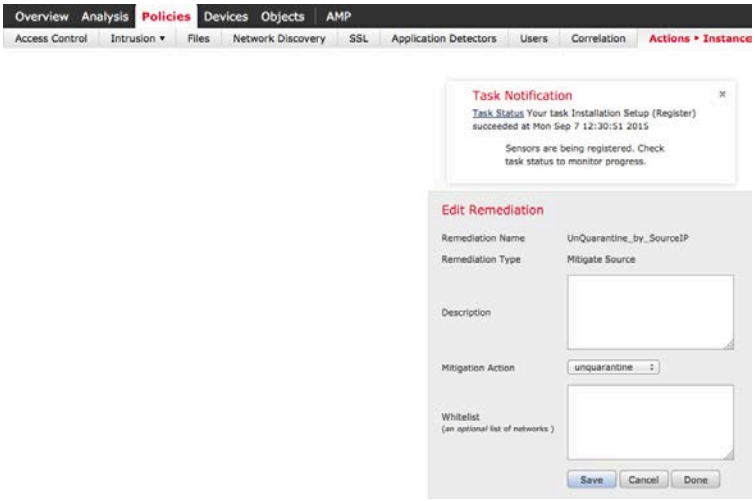


検疫解除

軽減ソースに基づいて検疫解除の軽減アクションを作成します。

ステップ 1 [ポリシー（Policies）] -> [アクション（Actions）] -> [インスタンス（Instances）] を選択し、設定済みインスタンスの [pxGrid] の横の虫めがねをクリックします。
ステップ 2 ドロップダウンから [軽減ソース（Mitigate Source）] を選択し、[追加（Add）] をクリックします。
ステップ 3 修復名に **UnQuarantine_SourceIP** と入力します。

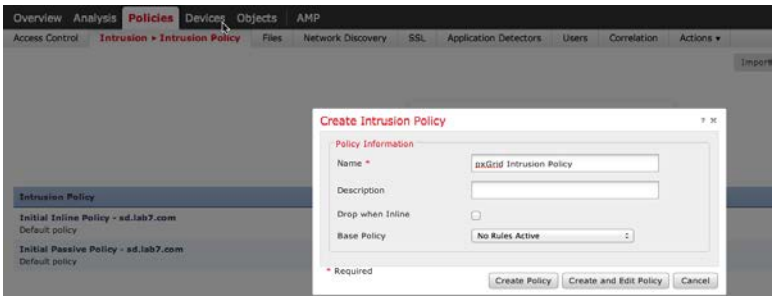
ステップ 4 軽減アクションには、ドロップダウン メニューから [検疫解除（unquarantine）] を選択します。
ステップ 5 [保存（Save）] をクリックします。



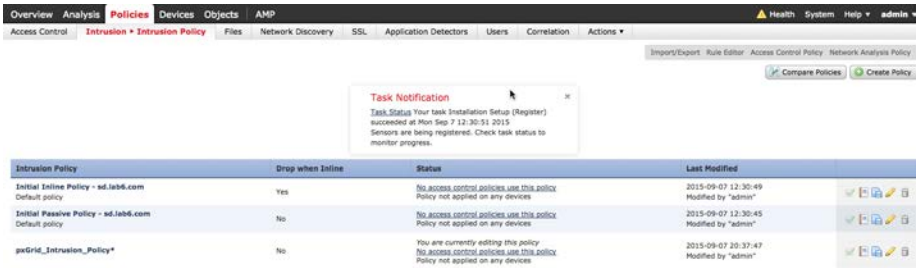
FireSIGHT pxGrid 侵入ポリシー

この項では、pxGrid 侵入ポリシーを作成し、FireSIGHT センサーに導入します。このポリシーは「SERVER IIS CMD.EXE アクセス」ルールを含み、エンドユーザがブラウザに www.yahoo.com/cmd.exe と入力すると、相関ポリシーに基づいて侵入イベントが生成されます。ただし、検疫解除相関ポリシーは例外です。

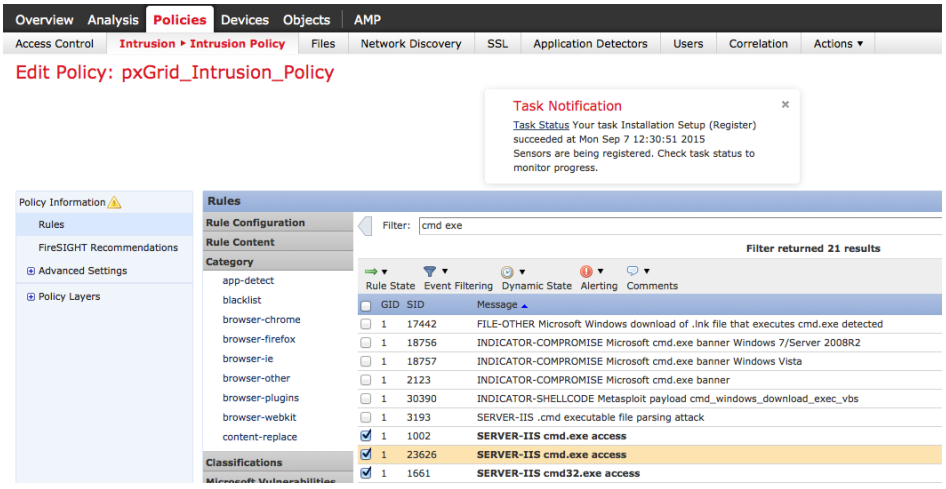
ステップ 1 [ポリシー（Policies）] -> [侵入（Intrusion）] -> [侵入ポリシー（Intrusion Policy）] に移動します。
ステップ 2 [ポリシーの作成（Create Policy）] をクリックします。
ステップ 3 新しいポリシーに **pxGrid_Intrusion_Policy** という名前を付けます。
ステップ 4 [ポリシーの作成（Create Policy）] をクリックします。



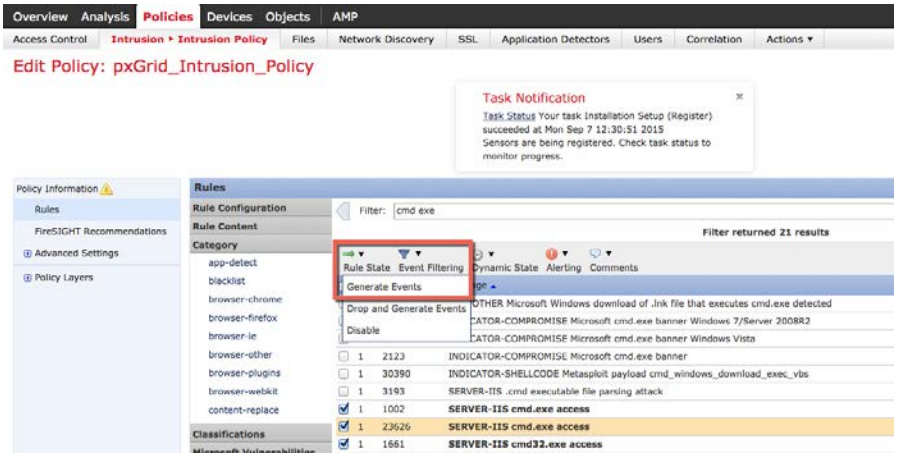
ステップ 5 編集のために [pxGrid_Intrusion_Policy] をクリックします。



ステップ 6 [ルール（Rules）] をクリックし、**cmd.exe** をフィルタ条件にして、以下のルールを選択します。

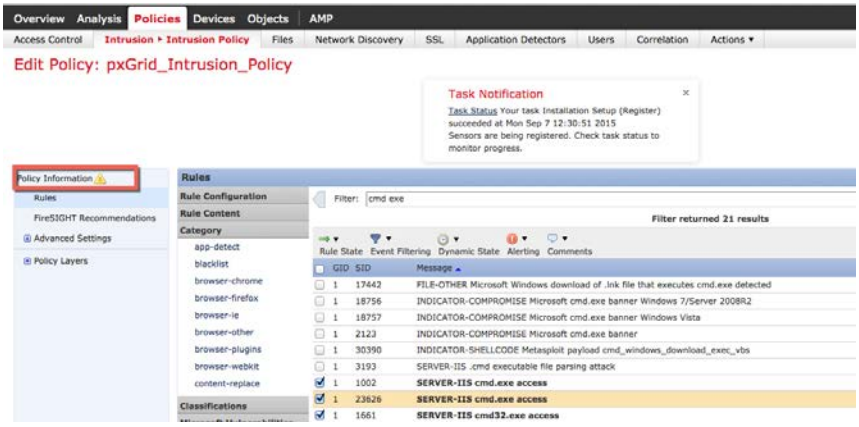


ステップ 7 [ルール状態（Rule State）] > [イベントの生成（Generate Events）] をクリックして、[OK] をクリックします。

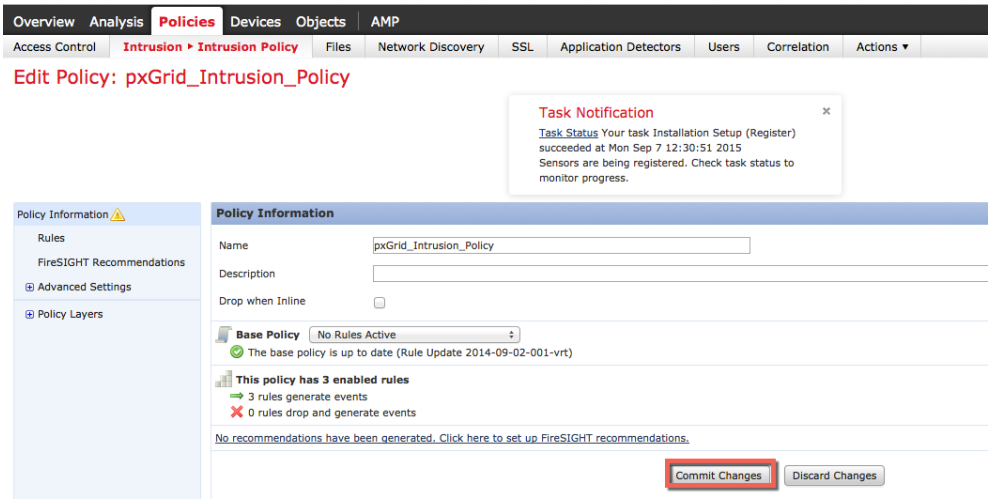


ステップ 8 「3 つのルールに関するルール状態の設定が正常終了した」ことを示す成功メッセージ表示されます。

ステップ 9 [ポリシー情報（Policy Information）] をクリックします。



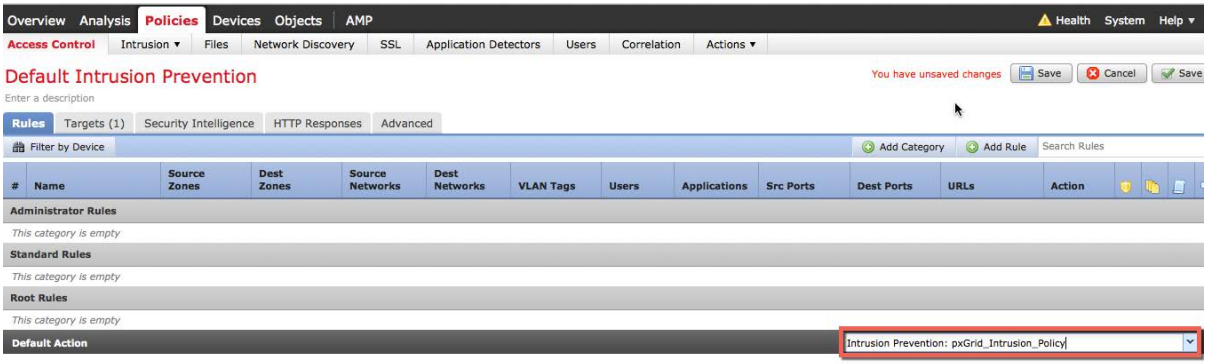
ステップ 10　[変更を確定（Commit Changes）] をクリックします。



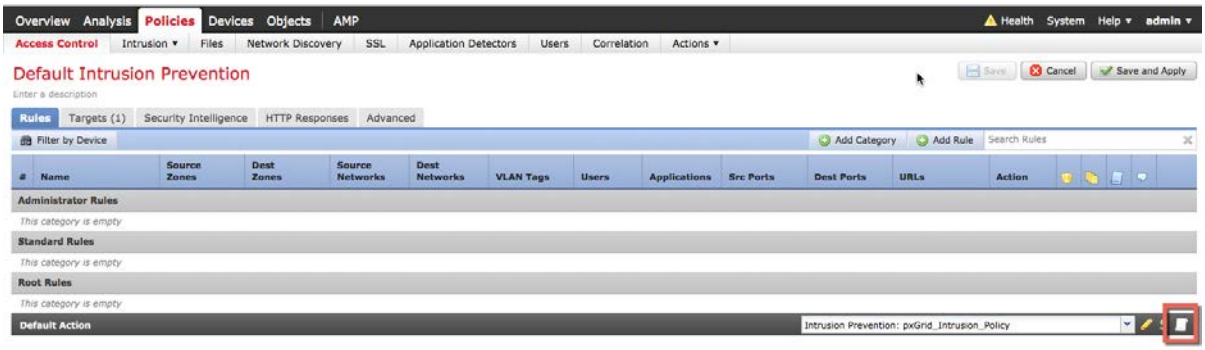
ステップ 11　[OK] をクリックします。

ステップ 12　[ポリシー（Policies）] -> [アクセスコントロールポリシー（Access Control Policies）] -> [デフォルトの侵入防御（Default Intrusion Prevention）] を選択して、編集します。

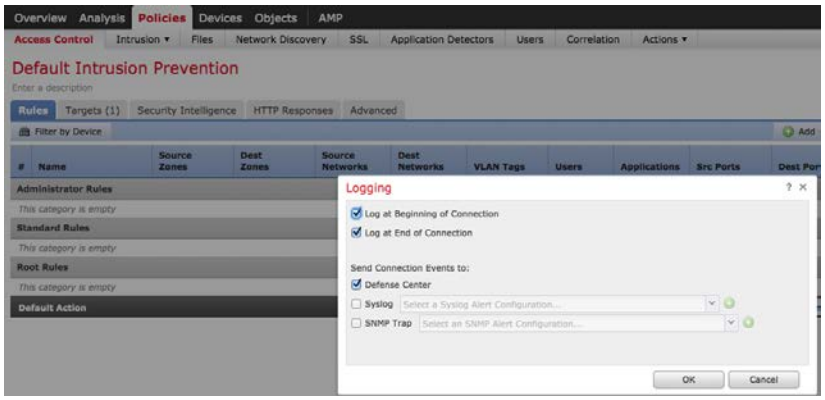
ステップ 13　[デフォルトのアクション（Default actions）] で、ドロップダウンから [pxGrid_Intrusion_Policy] を選択します。



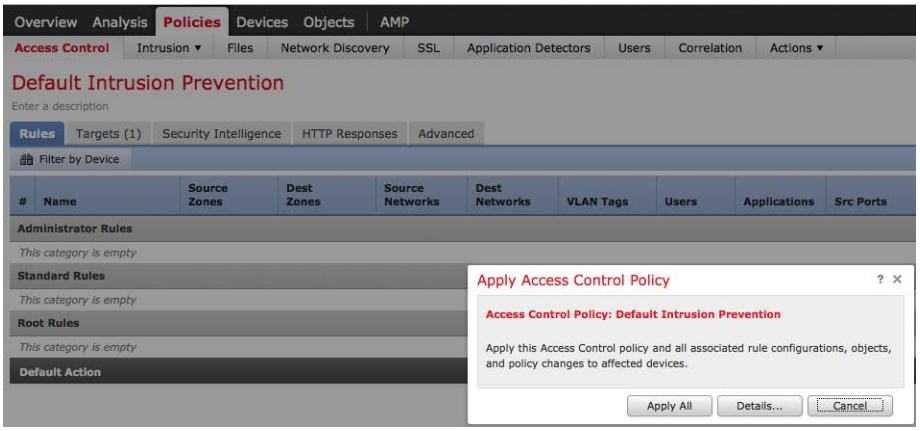
ステップ 14　[保存(Save)] をクリックします。
ステップ 15　テーブルの右下の [ロギング(Logging)] アイコンをクリックします。



ステップ 16　接続の開始時と終了時のロギングを有効にします。宛先として [Defense Center] を選択します。
ステップ 17　[OK] をクリックします。

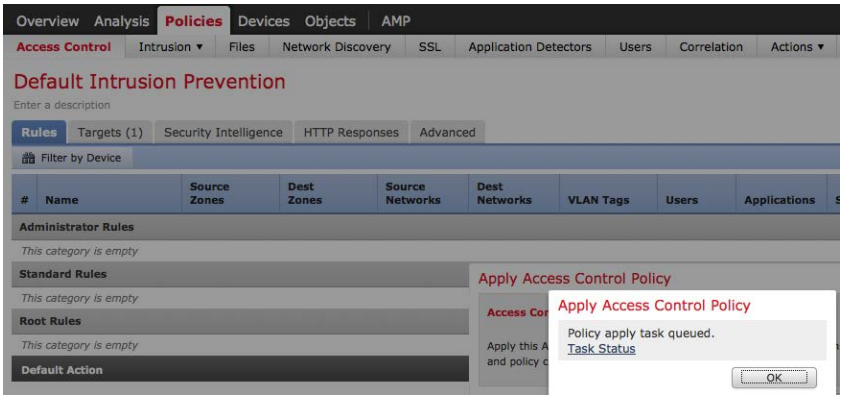


ステップ 18　[保存して適用(Save and Apply)] をクリックします。
ステップ 19　次が表示されます。



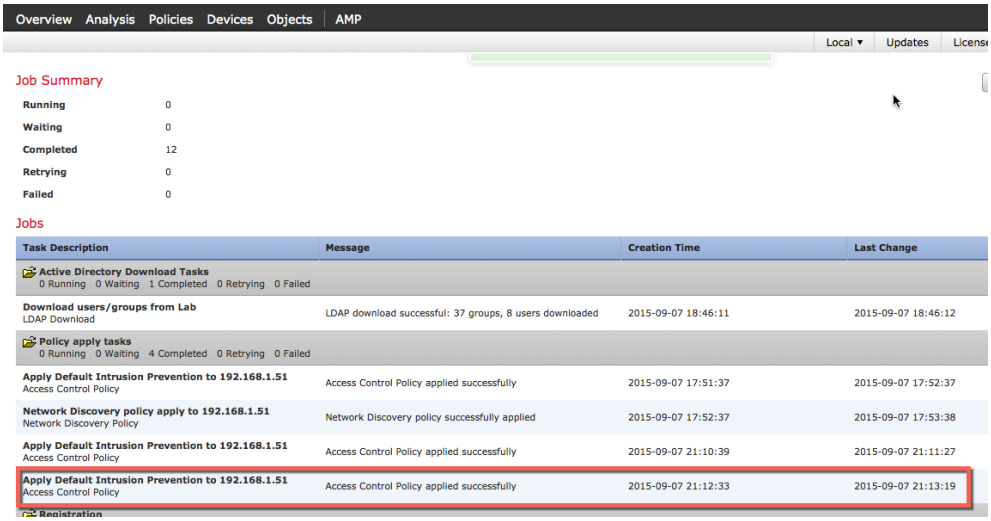
ステップ 20 [すべてを適用（Apply All）] をクリックします。

ステップ 21 タスクがキューに入力されたことが表示されます。



ステップ 22 [OK] をクリックします。

ステップ 23 [システム（System）] -> [モニタリング（Monitoring）] -> [タスクステータス（Task Status）] を選択して結果を表示し、タスクが正常に完了したことを確認します。

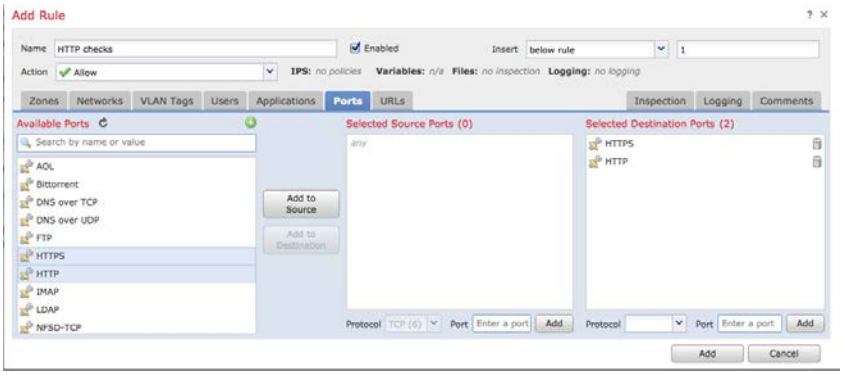


FireSIGHT 接続ルール

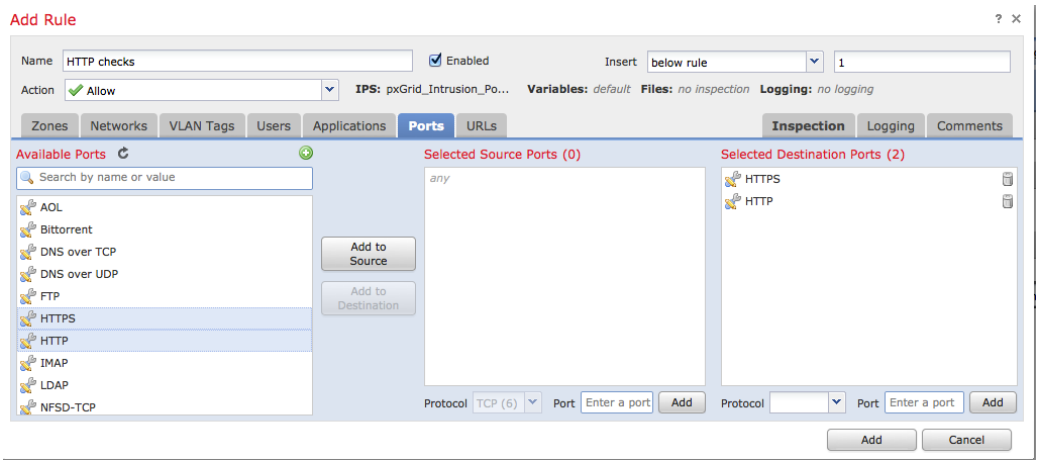
この項では、デフォルト アクセス ポリシーに追加する接続ルールを定義します。このデフォルト アクセス ポリシーには pxGrid 侵入ポリシーも組み込みます。この接続ルールは、HTTP/HTTPS 上の接続イベントをモニタし、これらの接続の詳細を FireSIGHT Management Center のログに記録します。この接続ルールは、UnQuarantine ポリシーによって検疫解除の修復タイプをトリガーする接続イベントをモニタするために使用されます。

ステップ 1　[ポリシー（Policies）] -> [アクセス制御（Access Control）] に移動します。
ステップ 2　鉛筆アイコンをクリックして、[デフォルトの侵入防御（Default Intrusion Prevention）] を編集します。

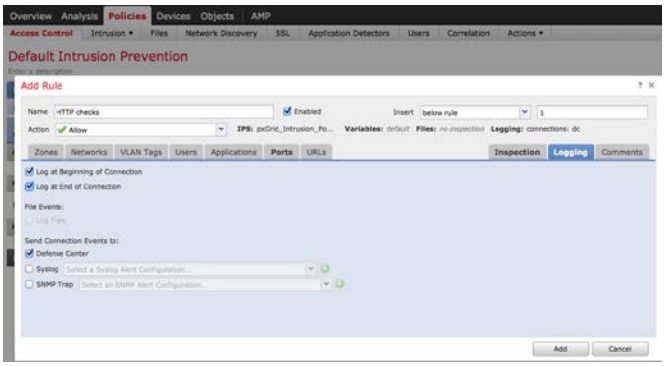
ステップ 3　[ルールの追加（Add Rule）] をクリックします。
ステップ 4　ルールに **HTTP Checks** という名前を付けます。
ステップ 5　[ポート（Ports）] タブを選択します。
ステップ 6　宛先ポートとして、[HTTP] および [HTTPS] を選択します。



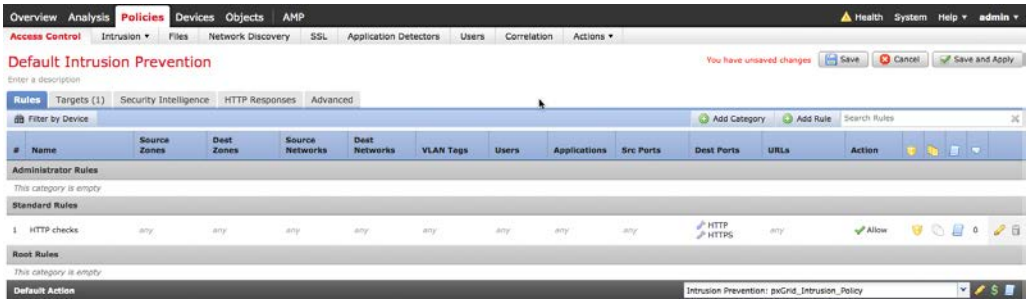
ステップ 7　[IPS] をクリックし、[pxGrid_Intrusion_Policy] を選択します。



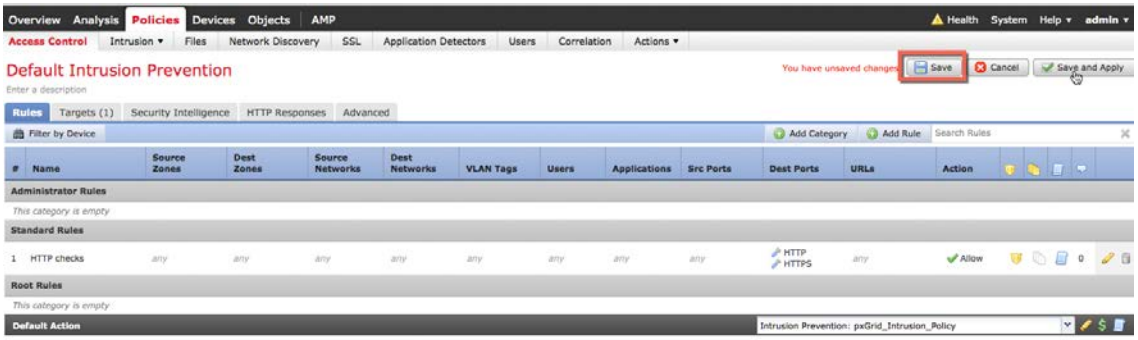
ステップ 8　[Logging（ロギング）] を選択します。



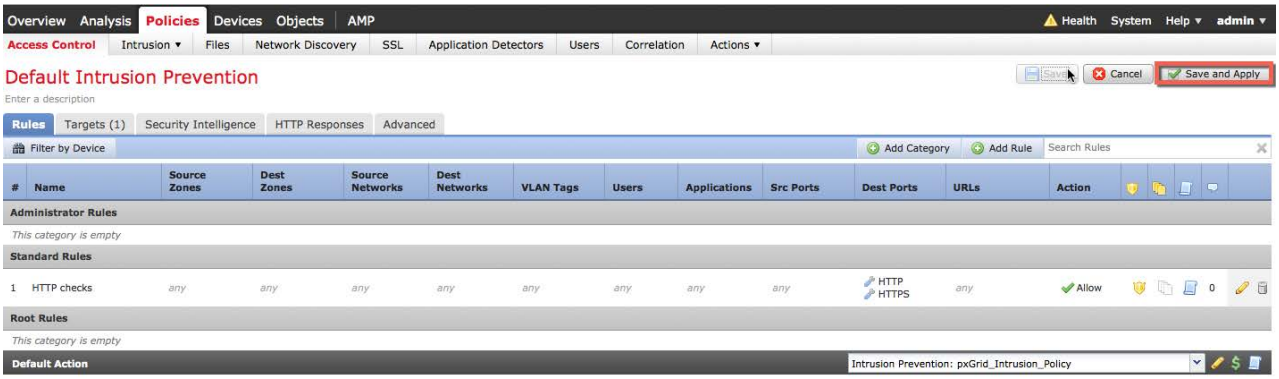
ステップ 9　次が表示されます。



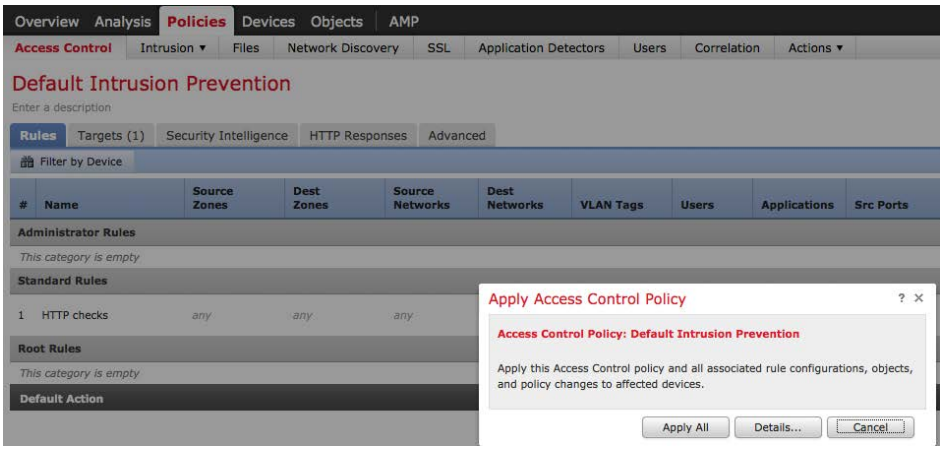
ステップ 10　[Save（保存）] を選択します。



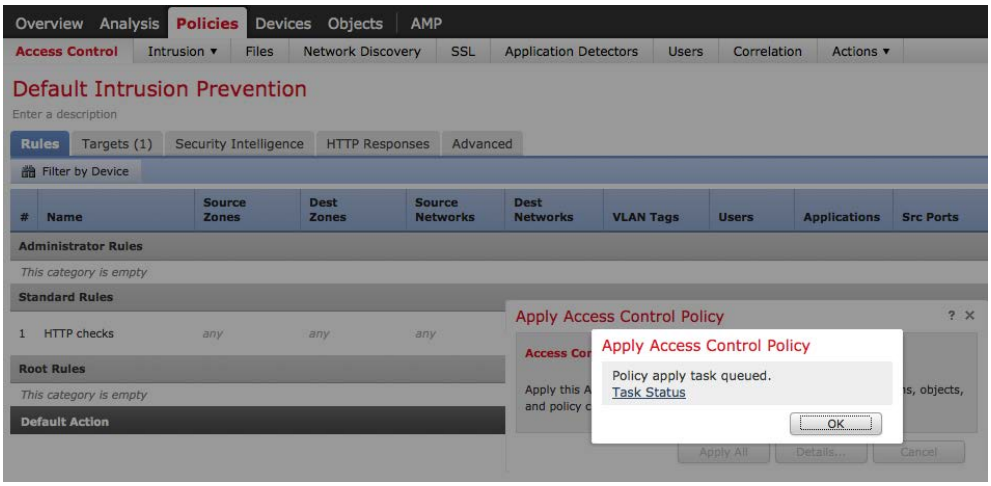
ステップ 11　[保存して適用（Save and Apply）] を選択します。



ステップ 12　[すべてを適用（Apply All）] をクリックします。



ステップ 13　「ポリシー適用タスクがキューに入力されました（Policy apply task queued）」というメッセージを確認して、[OK] をクリックします。



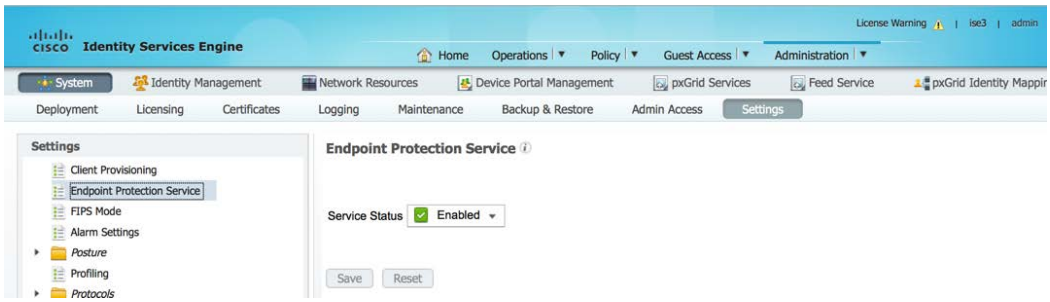
ISE EPS サービスと検疫許可ポリシーの設定

この項では、ISE で EPS を有効にし、ISE で検疫許可ポリシーを作成する手順について示します。ISE 1.4 で、エンドポイント保護サービスは Adaptive Network Control に名前が変更されました。ISE 2.0 では、これはデフォルトで有効になり、管理の下に Adaptive Network Control サービス設定はありません。

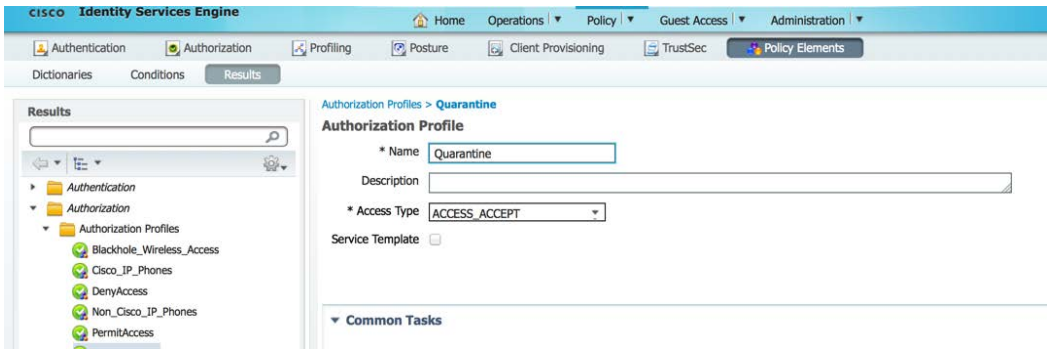
注:ISE 2.0 の Adaptive Network Control ポリシーは、AdaptiveNetworkControl 機能に登録される pxGrid クライアントに依存します。これは、FireSIGHT Management Center にはあてはまりません。FireSIGHT Management Center は EndpointProtectionService 機能に登録され、iSE 許可ポリシーに依存します。ISE 2.0 では、エンドポイントの検疫解除を pxGrid GCL EPS_unquarantine スクリプトを使用して行う必要がある点に注意してください。これは、FireSIGHT Management Center で検疫解除相関ポリシー、非相関ルールを作成し、検疫解除軽減応答を検疫解除相関ポリシーに割り当てることで実行します。

ステップ 1　ISE エンドポイント保護サービスを有効にします。
[管理(Administration)] -> [システム(System)] -> [設定(Settings)] -> [エンドポイント保護サービス(Endpoint Protection Service)] を選択し、[エンドポイント保護サービス(Endpoint Protection Service)] を有効にして、保存します。

注:エンドポイント保護サービスは ISE 2.0 では適用されず、デフォルトで有効になります。

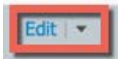


ステップ 2　検疫許可プロファイルを作成します。
[ポリシー(Policy)] -> [ポリシー要素(Policy Elements)] -> [結果(Results)] -> [許可(Authorization)] -> [許可プロファイル(Authorization Profiles)] -> [追加(Add)] を選択し、[名前(Name)] に **Quarantine** と入力して、保存します。



注:この例では、許可状態プロファイルを示すために、アクセス タイプを [ACCESS_ACCEPT] に設定しました。

ステップ 3　検疫許可ポリシーを作成します。

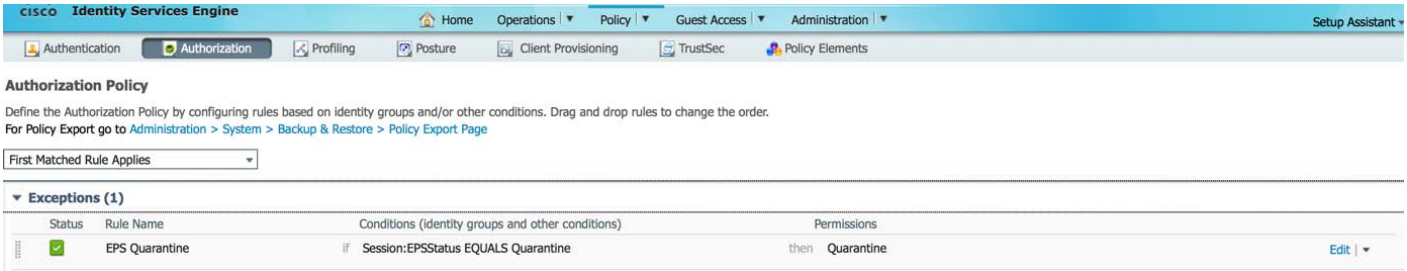
[ポリシー（Policy）] -> [許可（Authorization）] -> [例外（Exceptions）] -> 

-> 

を選択し、次のように入力します。

ルール名：**EPS Quarantine**
新しい条件ルールの作成：[Session:EPSStatus:EQUALS:Quarantine]
標準プロファイル：[検疫（Quarantine）]

[終了（Done）] をクリックします。



ステップ 4　[保存（Save）] をクリックします。

FireSIGHT Management Center 相関ポリシー

この項では、検疫、ポートバウンス、再認証、ポートシャットダウン、強制終了、および検疫解除用に FireSIGHT 相関ポリシーおよびルールを作成します。これらのポリシーにはそれぞれ修復応答を割り当て、エンドポイントでの pxGrid ANC 軽減修復アクションを提供します。

相関ポリシーが作成された後で、ルール モジュールを作成します。相関ポリシーはそれぞれのルール モジュールを追加します。ルール モジュールにはそれぞれ応答が割り当てられます。

たとえば、検疫相関ポリシーを作成します。検疫ルール モジュールが作成され、侵入イベントが発生すると、エンドポイントの送信元 IP アドレスが検疫されます。検疫ルール モジュールに検疫修復タイプ応答が割り当てられます。エンドユーザが pxGrid 侵入ポリシーに違反すると、侵入イベントと相関イベントがトリガーされ、検疫修復タイプ応答に基づいて検疫軽減アクションが起動します。

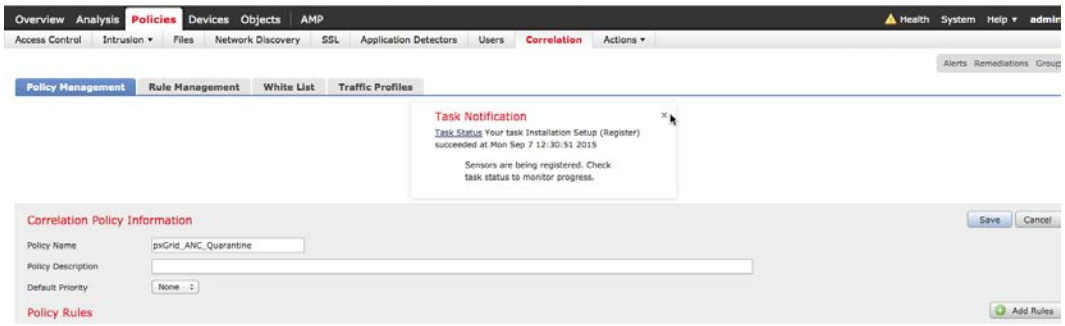
ポートバウンス、再認証、ポートシャットダウン、強制終了のポリシーは同じフローに従います。

検疫解除ポリシーは接続イベントをトリガーする検疫解除ルール モジュールを持ち、エンドポイントが特定の URL サイトにアクセスすると、エンドポイントの送信元 IP アドレスに従って検疫解除されます。

検疫

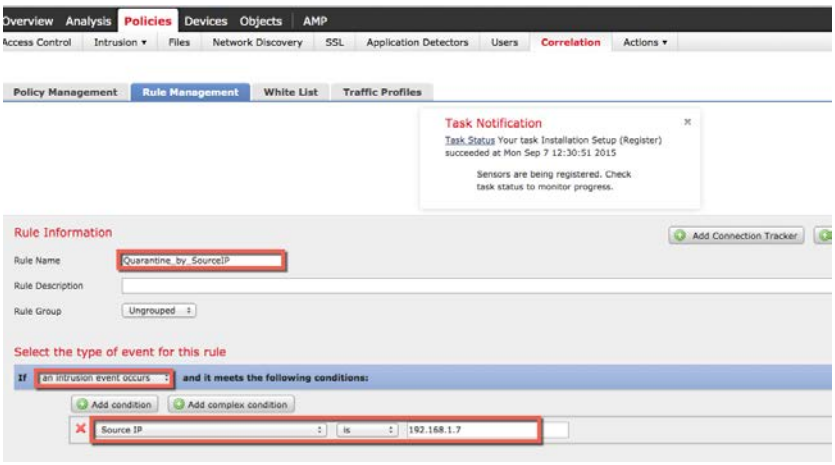
検疫相関ポリシーを作成します。

ステップ 1　[ポリシー（Policies）] -> [相関（Correlation）] -> [ポリシー管理（Policy Management）] -> [ポリシーの作成（Create Policy）] -> [pxGrid_ANC_Quarantine] -> [保存（Save）] を選択します。

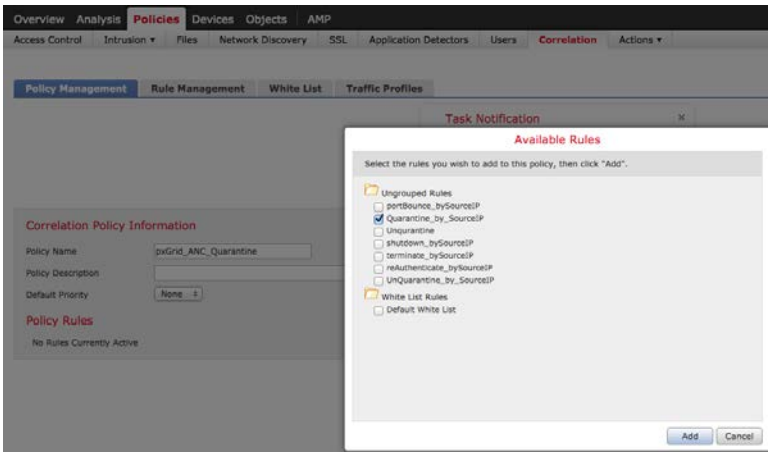


ステップ 2 [ポリシー（Policies）] -> [相関（Correlation）] -> [ルール管理（Rule Management）] -> [ルールの作成（Create Rule）] を選択し、Quarantine_by_SourceIP というルール名を追加し、次のように入力して、[保存（Save）] します。

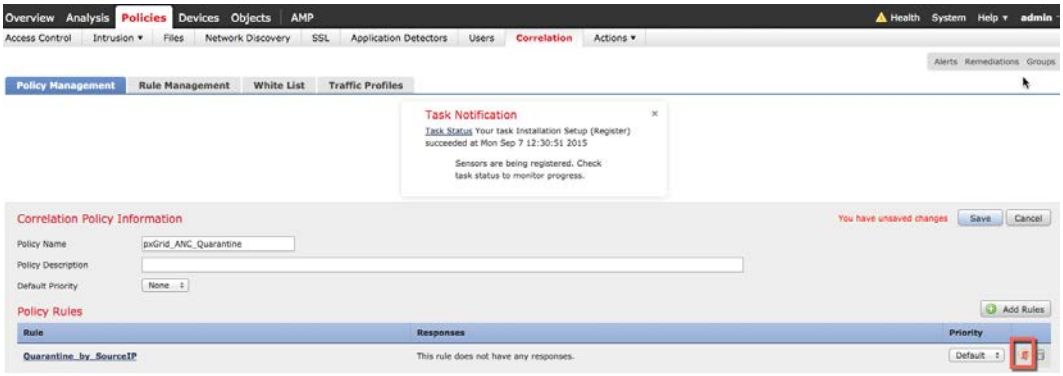
注：このルールでは、送信元 IP アドレスに対する検疫の概念実証を提供します。



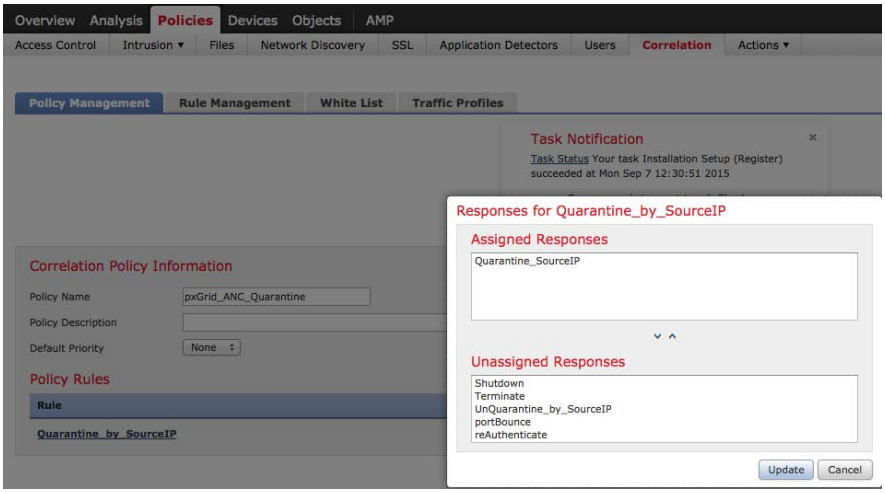
ステップ 3 [ポリシー（Policies）] -> [相関（Correlation）] -> [ポリシー管理（Policy Management）] -> [pxGrid ANC 検疫（pxGrid ANC Quarantine）] > [ルールの追加（Add rules）] -> [pxGrid ANC検疫（pxGrid ANC Quarantine）] -> [追加（Add）] を選択します。



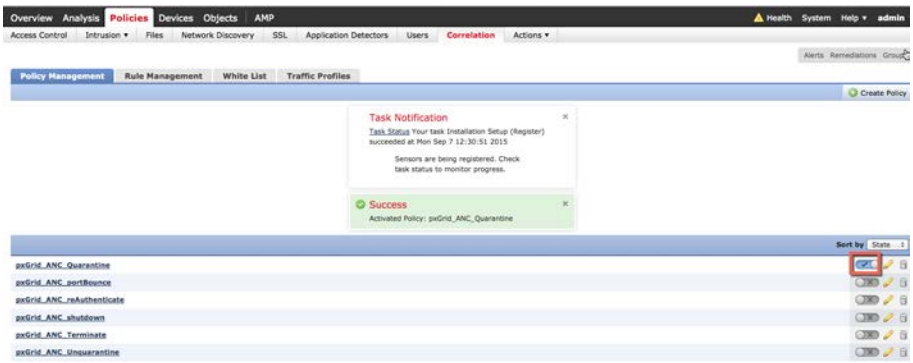
ステップ 4 次に、応答を追加します。[応答（Responses）] タブをクリックします。



ステップ 5 [Quarantine_SourceIP] を [割り当てられた応答（Assigned Responses）] に移動し、[更新（Update）] -> [保存（Save）] を選択します。



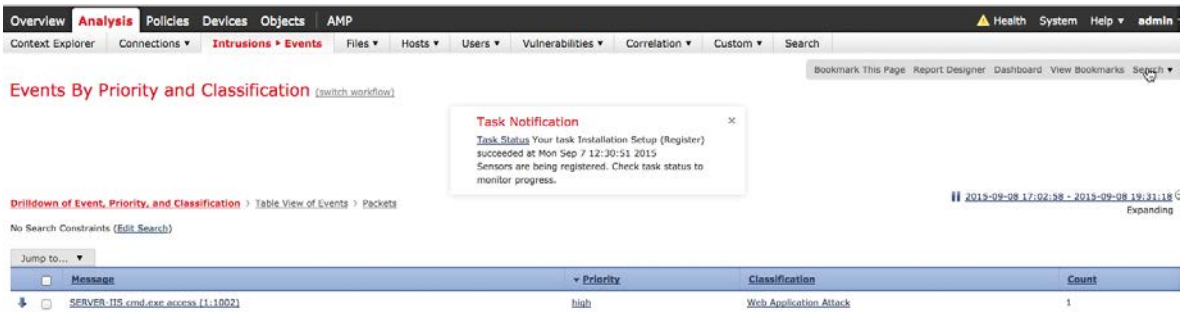
ステップ 6 ボタンをクリックして検疫相関ポリシーをアクティブ化します。



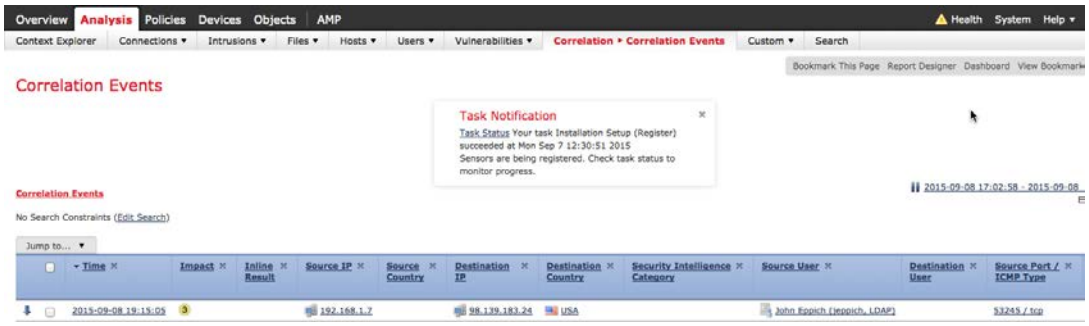
テスト

エンドユーザがブラウザ ウィンドウに www.yahoo.com/cmd.exe と入力すると、FireSIGHT の pxGrid 侵入ポリシーの「SERVER-IIS.cmd.exe アクセス」ルール違反から侵入イベントがトリガーされます。エンドポイントは、相関ポリシーで定義されている検疫ルールに割り当てられた検疫軽減応答に基づいて検疫されます。

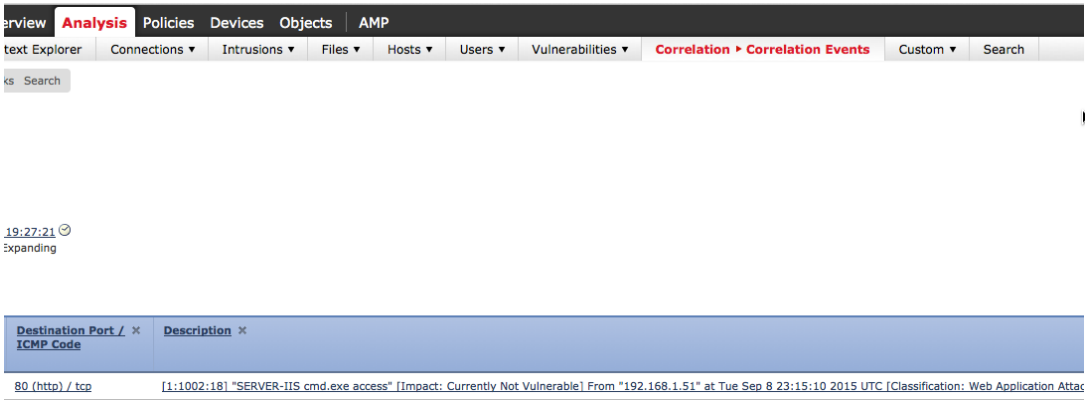
ステップ 1　エンドユーザはブラウザで www.yahoo.com/cmd.exe と入力します。
ステップ 2　これは「Web アプリケーション攻撃」侵入イベントをトリガーします。



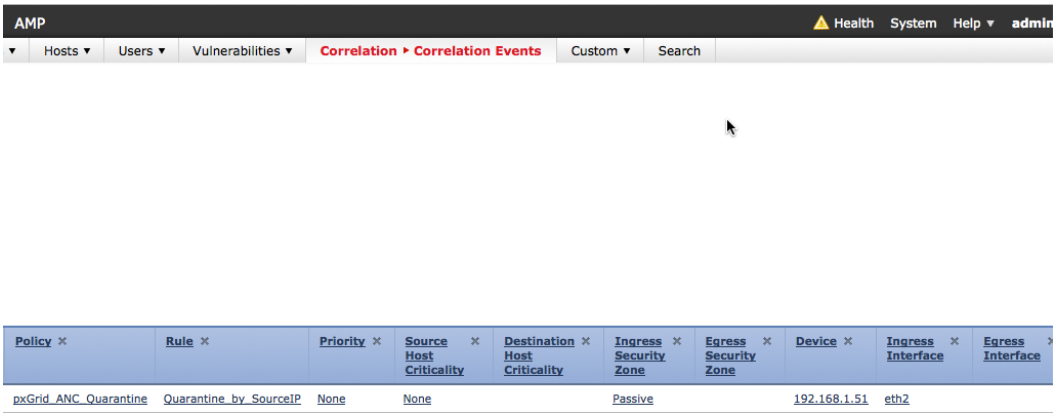
ステップ 3　また、「相関イベント」もトリガーします。
検疫される送信元 IP アドレスと FireSIGHT LDAP/ユーザ認識設定に基づくユーザ情報に注意してください。



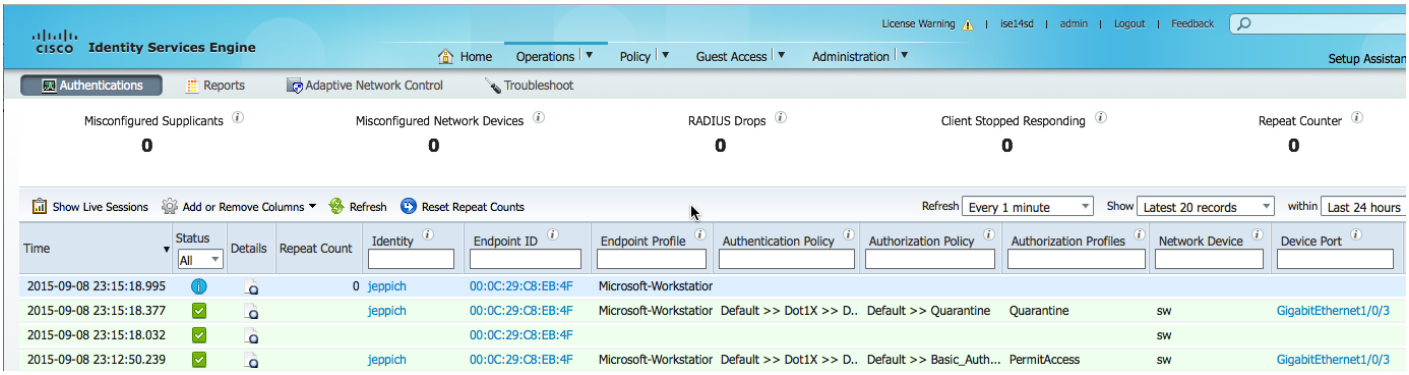
ステップ 4　同じイベントの作業を続けます。
pxGrid_Intrusion_Policy ルールに含まれている宛先ポートとルール違反に注意してください。



ステップ 5　同じイベントの作業を続けます。
割り当てられた検疫軽減応答をトリガーした相関ポリシーおよび相関ルールに注意してください。



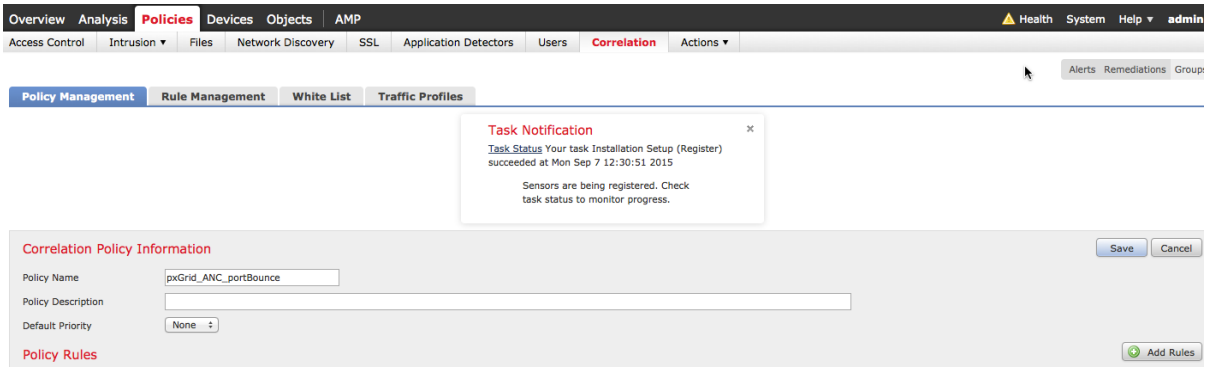
ステップ 6　ISE の応答を表示するには、[運用（Operations）] -> [認証（Authentications）] を選択します。



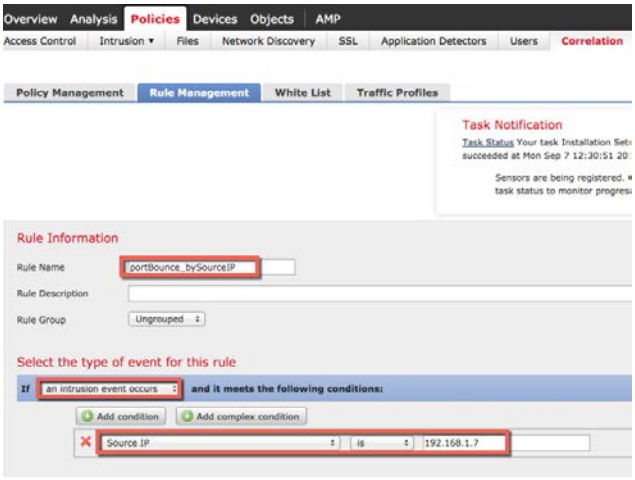
ポートバウンス

ポートバウンス相関ポリシーを作成します。

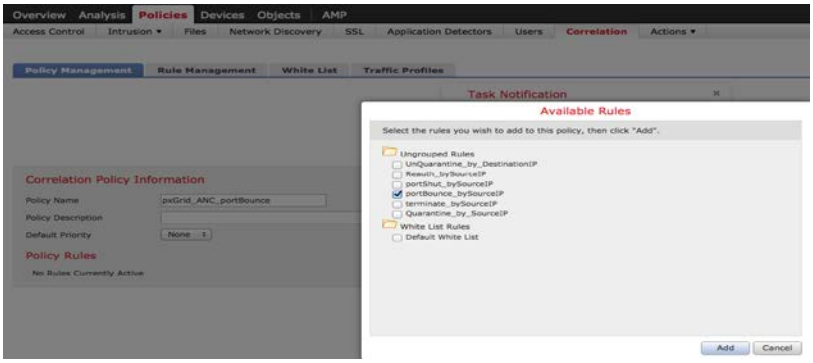
ステップ 1　[ポリシー（Policies）] -> [相関（Correlation）] -> [ポリシー管理（Policy Management）] -> [ポリシーの作成（Create Policy）] -> [pxGrid ANC portBounce（pxGrid ANC ポートバウンス）] -> [保存（Save）] を選択します。



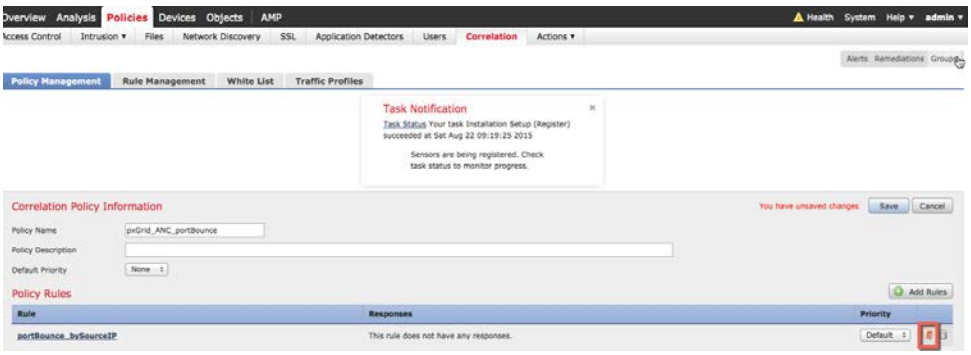
ステップ 2 [ポリシー（Policies）] -> [相関（Correlation）] -> [ルール管理（Rule Management）] -> [ルールの作成（Create Rule）] を選択し、**portBounce_by_SourceIP** というルール名を追加し、次のように入力して、保存します。



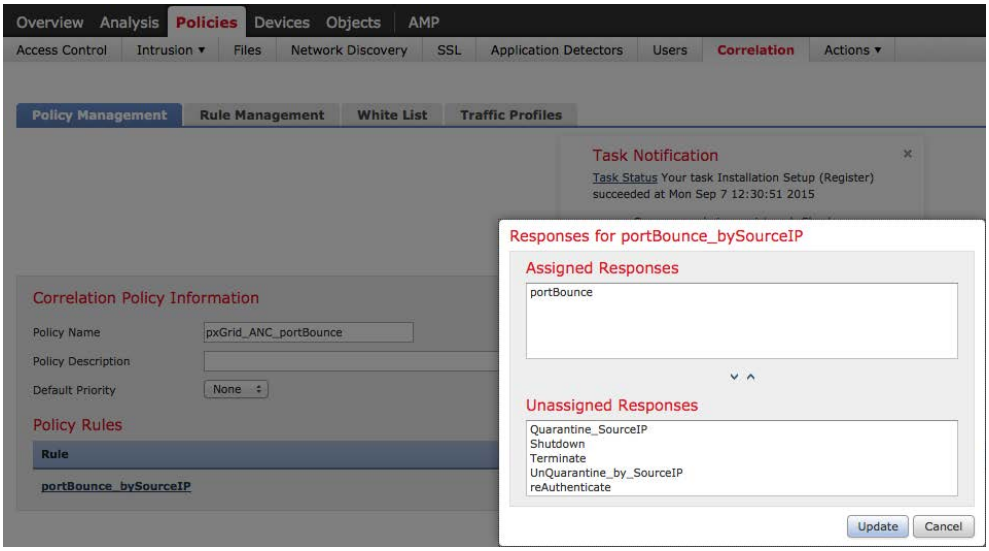
ステップ 3 [ポリシー（Policies）] -> [相関（Correlation）] -> [ポリシー管理（Policy Management）] -> [pxGrid ANC portBounce（pxGrid ANC ポートバウンス）] > [ルールの追加（Add rules）] -> [portBounce_by_SourceIP] を選択して、ルールを追加します。



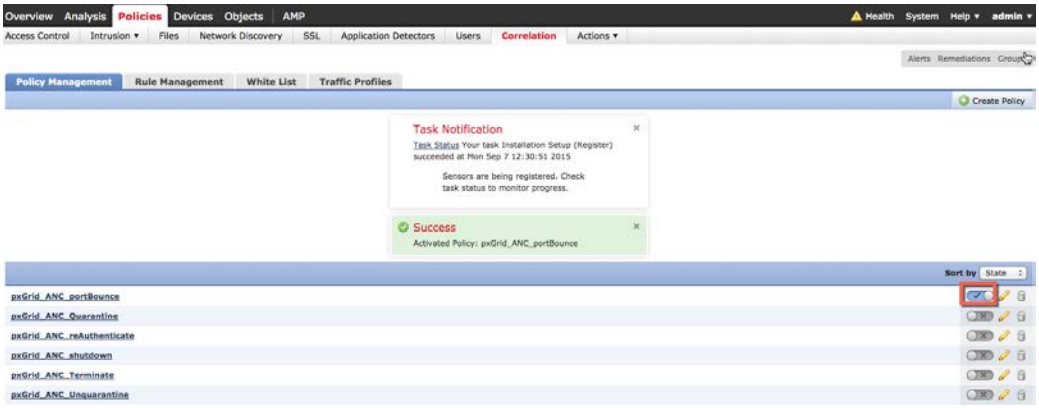
ステップ 4 次に、応答を追加します。[応答（Responses）] タブをクリックします。



ステップ 5 [ポリシー（Policies）] -> [相関（Correlation）] -> [portBounce_by_SourceIP] を選択し、[ポートバウンス（portBounce）] を [割り当てられた応答（Assigned Responses）] に移動し、[更新（Update）] -> [保存（Save）] を選択します。



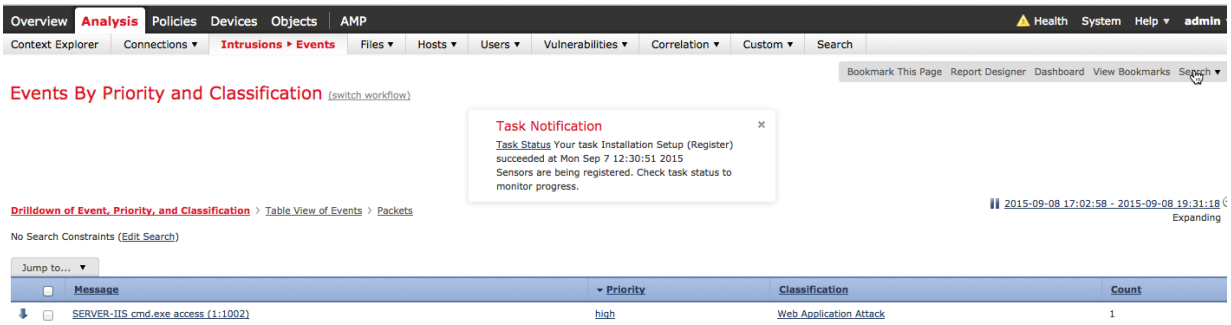
ステップ 6 強制終了ポリシーをアクティブ化し、その下のボタンをクリックして、ポリシーを有効にします。



テスト

エンドユーザがブラウザ ウィンドウに www.yahoo.com/cmd.exe と入力すると、FireSIGHT の pxGrid 侵入ポリシーの「SERVER-IIS.cmd.exe アクセス」ルール違反から侵入イベントがトリガーされます。エンドポイントを含むポートは、相関ポリシーで定義されているルールに割り当てられたポートバウンス軽減応答に基づいてバウンスされます。

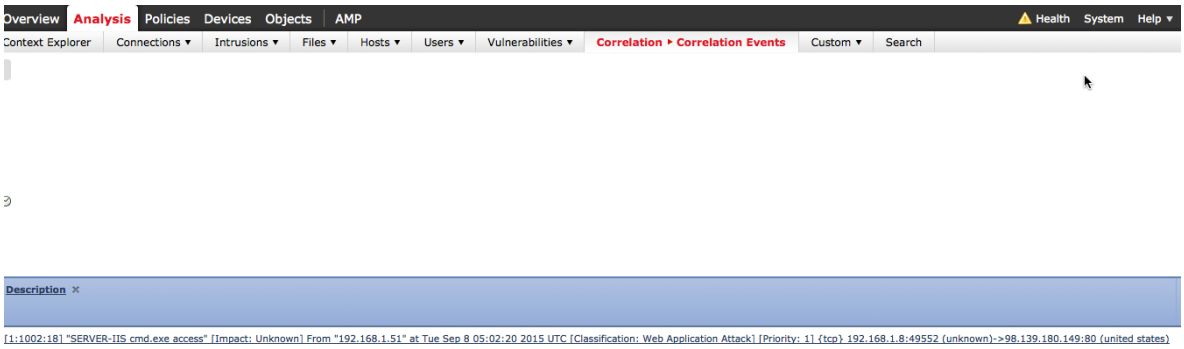
ステップ 1 エンドユーザはブラウザで www.yahoo.com/cmd.exe と入力します。
ステップ 2 これは「Web アプリケーション攻撃」侵入イベントをトリガーします。



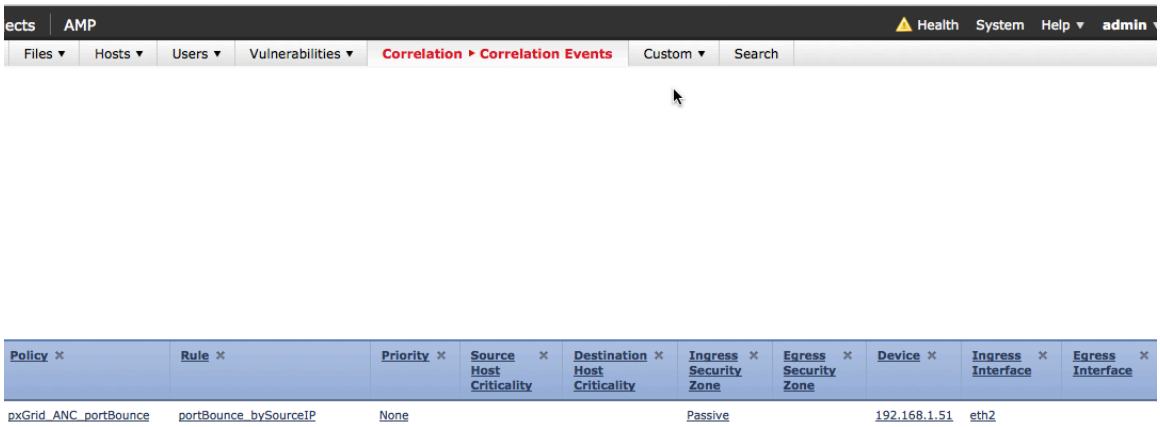
ステップ 3 また、「相関イベント」もトリガーします。
ポートは送信元 IP アドレスに属するホストに対してバウンスされます。

注: ネットワーク検出のホストおよびユーザが有効になっていないため、ユーザ情報はありません。

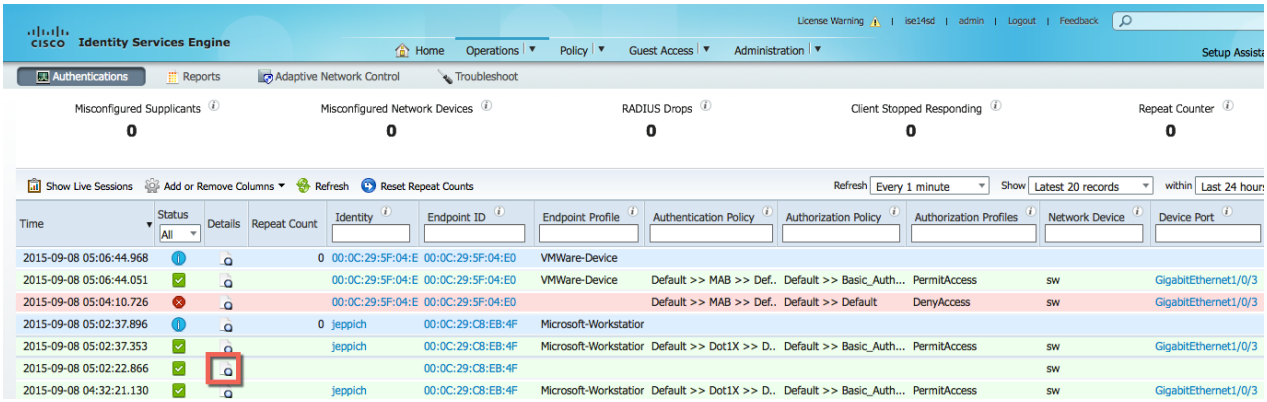
ステップ 4 同じイベントの作業を続けます。
pxGrid_Intrusion_Policy ルールに含まれているルール違反に注意してください。



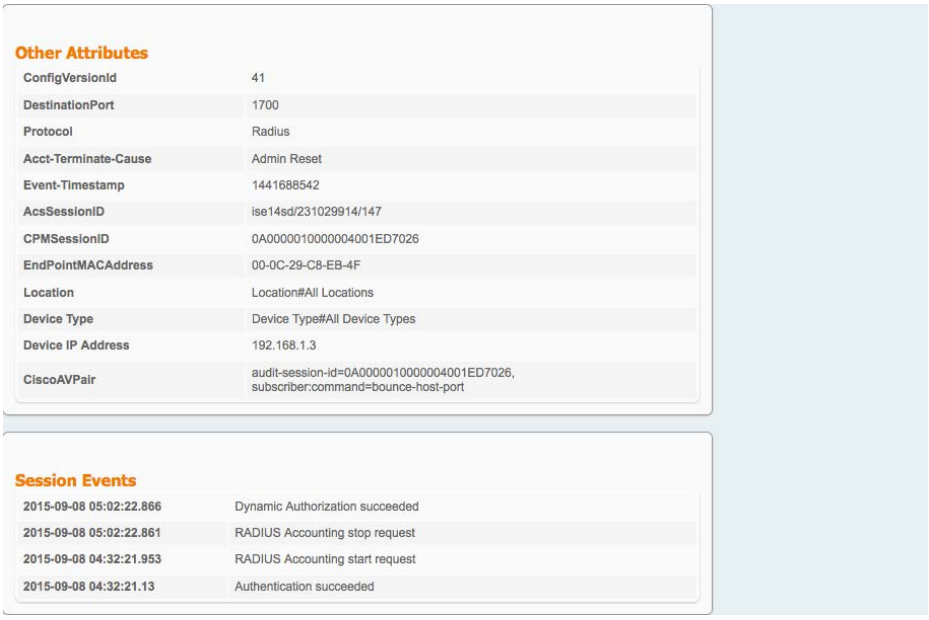
ステップ 5 同じイベントの作業を続けます。
割り当てられたポートバウンス軽減応答をトリガーした相関ポリシーおよび相関ルールに注意してください。



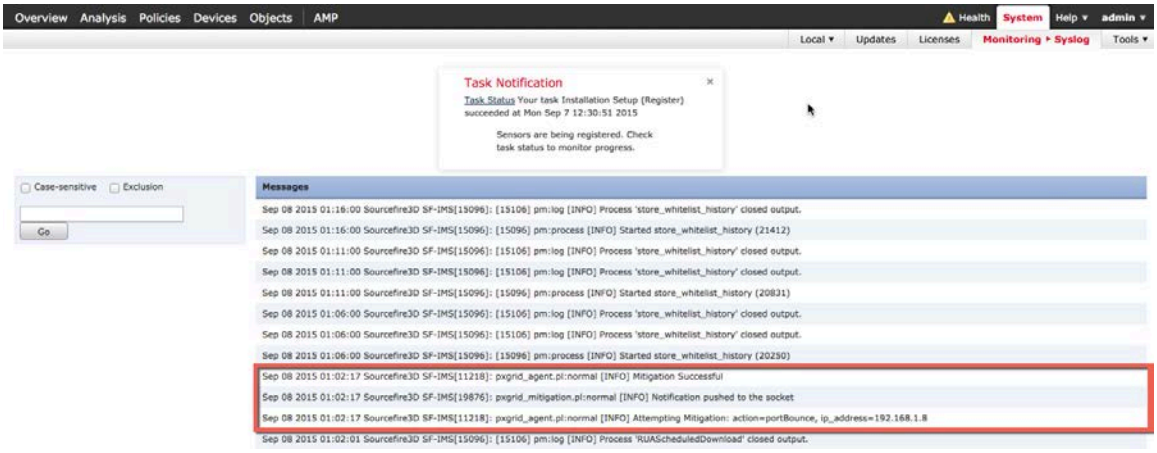
ステップ 6　　ISE の応答を表示するには、[運用（Operations）] - [認証（Authentications）] を選択します。



ステップ 7　　詳細ボタンを選択すると、ポートが CiscoAVpair 属性に基づいてバウンスされることがわかります。



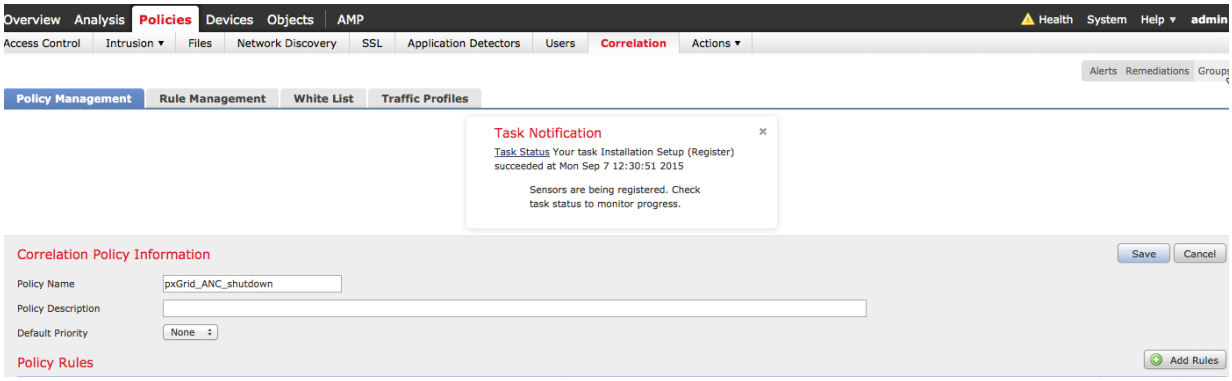
ステップ 8 また、FireSIGHT Management Center syslog イベントを表示して、ポートバウンス軽減アクションが成功したことを確認できます。



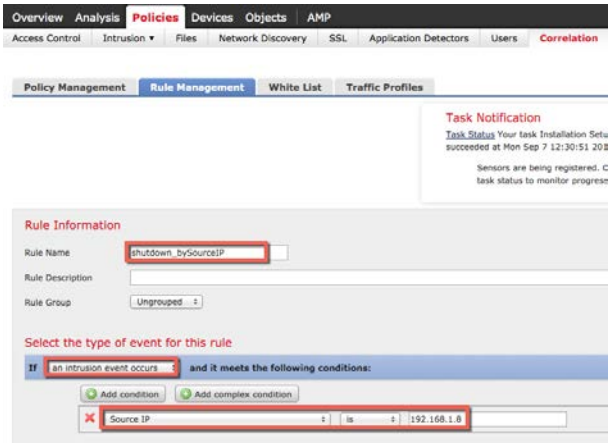
ポートシャットダウン

ポートシャットダウン相関ポリシーを作成します。

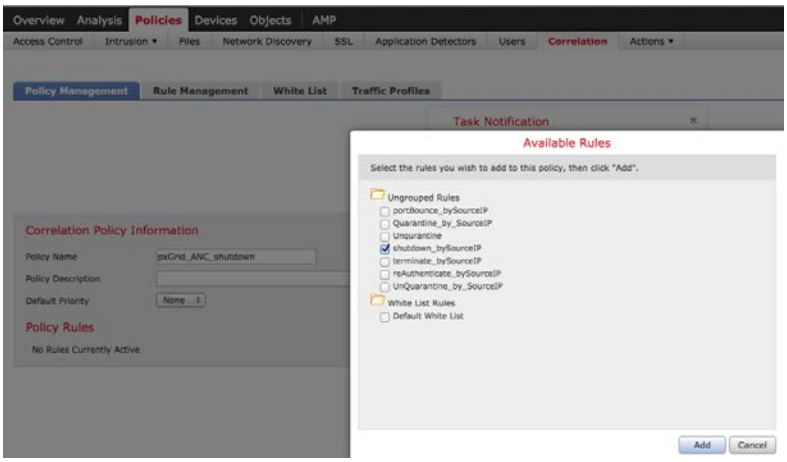
ステップ 1 [ポリシー（Policies）] -> [相関（Correlation）] -> [ポリシー管理（Policy Management）] -> [ポリシーの作成（Create Policy）] -> [pxGrid_ANC_shutdown] -> [保存（Save）] を選択します。



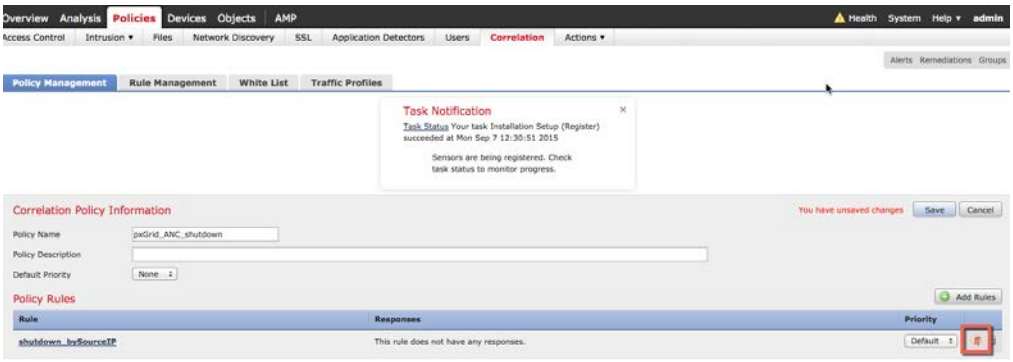
ステップ 2 [ポリシー（Policies）] -> [相関（Correlation）] -> [ルール管理（Rule Management）] -> [ルールの作成（Create Rule）] を選択し、shutdown_by_SourceIP というルール名を追加し、次のように入力して、保存します。



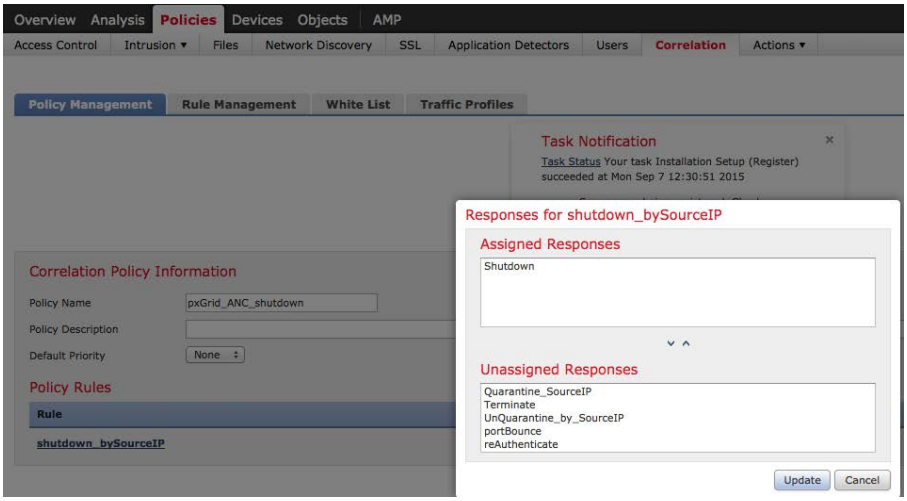
ステップ 3 [ポリシー（Policies）] -> [相関（Correlation）] -> [ポリシー管理（Policy Management）] -> [pxGrid_ANC_shutdown] > [ルールの追加（Add rules）] -> [shutdown_bySourceIP] を選択して、ルールを追加します。



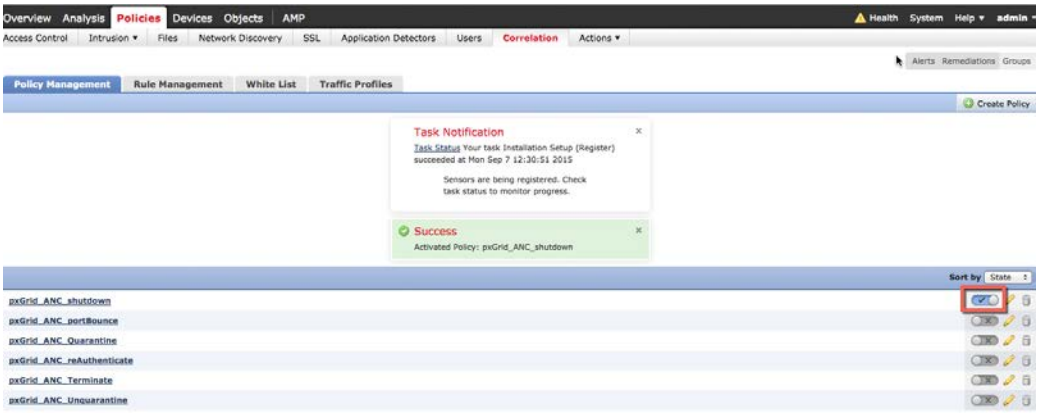
ステップ 4 次に、応答を追加します。[応答（Responses）] タブをクリックします。



ステップ 5 [ポリシー（Policies）] -> [相関（Correlation）] -> [pxGrid_ANC_shutdown] を選択し、[シャットダウン（Shutdown）] を [割り当てられた応答（Assigned Responses）] に移動し、[更新（Update）] -> [保存（Save）] を選択します。



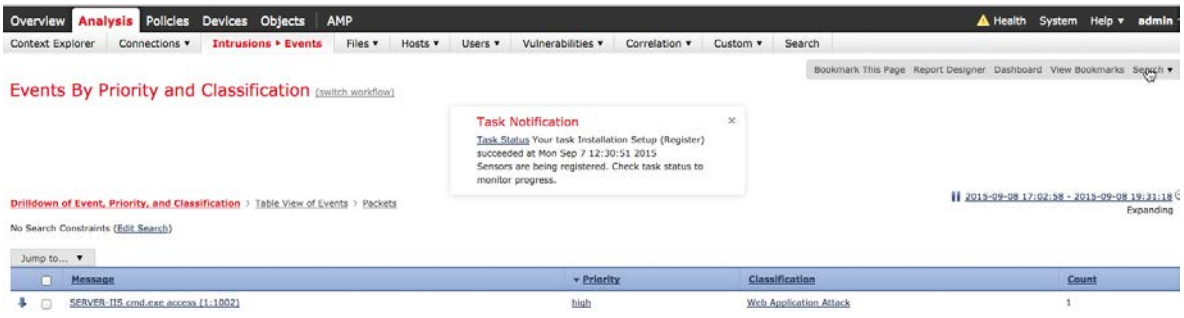
ステップ 6　　強制終了ポリシーをアクティブ化し、その下のボタンをクリックして、ポリシーを有効にします。



テスト

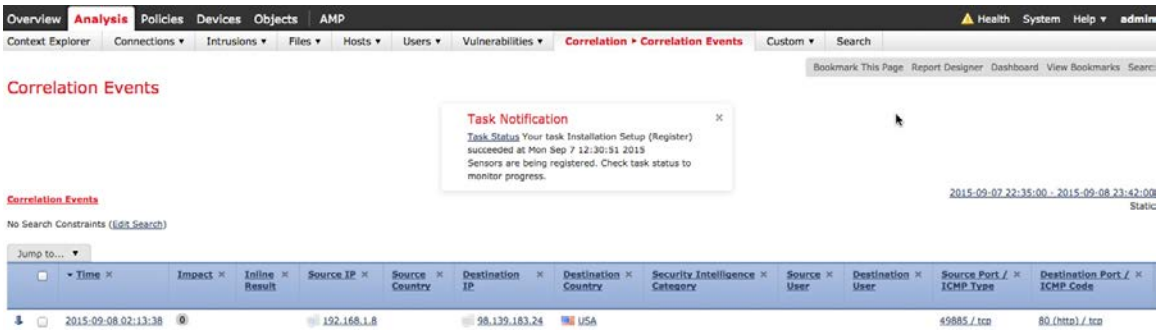
エンドユーザがブラウザ ウィンドウに www.yahoo.com/cmd.exe と入力すると、FireSIGHT の pxGrid 侵入ポリシーの「SERVER-IIS.cmd.exe アクセス」ルール違反から侵入イベントがトリガーされます。エンドポイントのポートは相関ポリシーで定義したルールに割り当てられたシャットダウン軽減応答に基づいて遮断されます。

ステップ 1　　エンドユーザはブラウザで www.yahoo.com/cmd.exe と入力します。
ステップ 2　　これは「Web アプリケーション攻撃」侵入イベントをトリガーします。

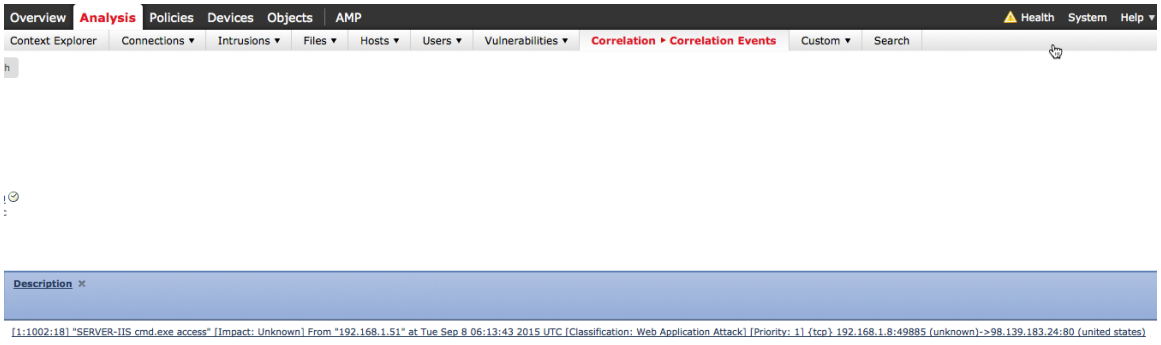


ステップ 3　また、「相関イベント」もトリガーします。
送信元 IP アドレスに属するホストのポートがシャットダウンされることに注意してください。

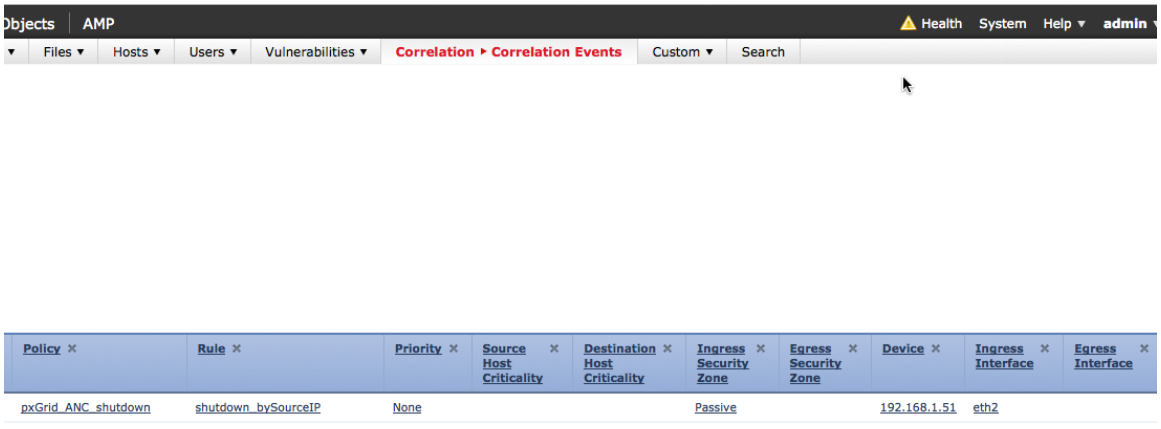
注：ネットワーク検出のホストおよびユーザが有効になっていないため、ユーザ情報はありません。



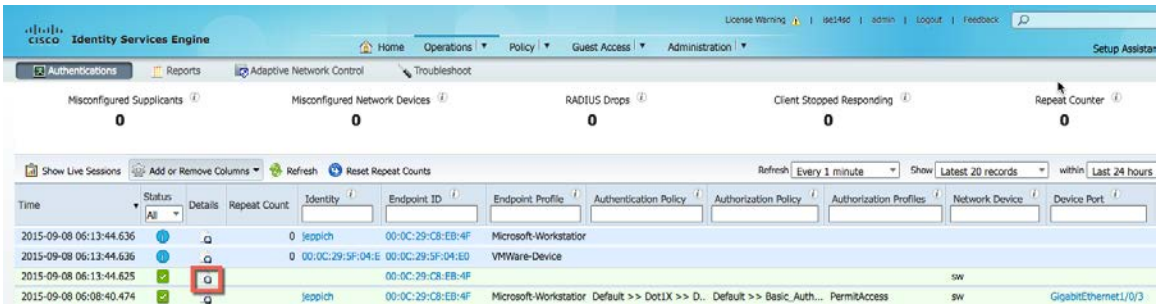
ステップ 4　同じイベントの作業を続けます。
pxGrid_Intrusion_Policy ルールに含まれているルール違反に注意してください。



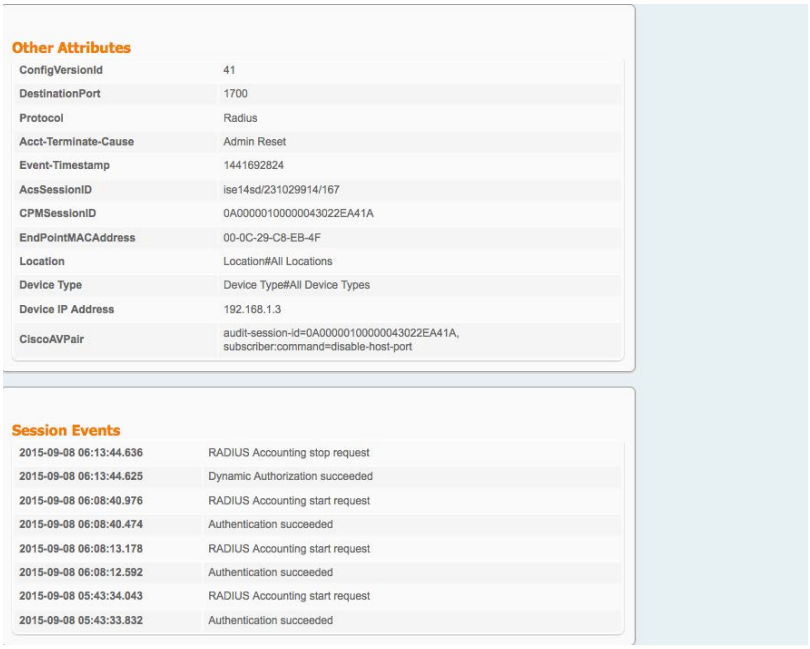
ステップ 5　同じイベントの作業を続けます。
割り当てられたポートシャットダウン軽減応答をトリガーした相関ポリシーおよび相関ルールに注意してください。



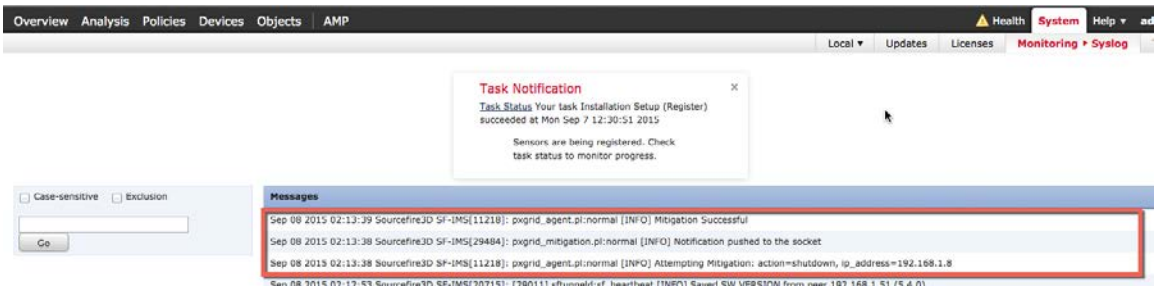
ステップ 6 ISE の応答を表示するには、[運用（Operations）] -> [認証（Authentications）] を選択します。



ステップ 7 詳細ボタンを選択すると、ポートが CiscoAVpair 属性に基づいて無効化されることがわかります。



ステップ 8 また、FireSIGHT Management Center syslog イベントを表示して、ポート シャットダウン軽減アクションが成功したことを確認できます。



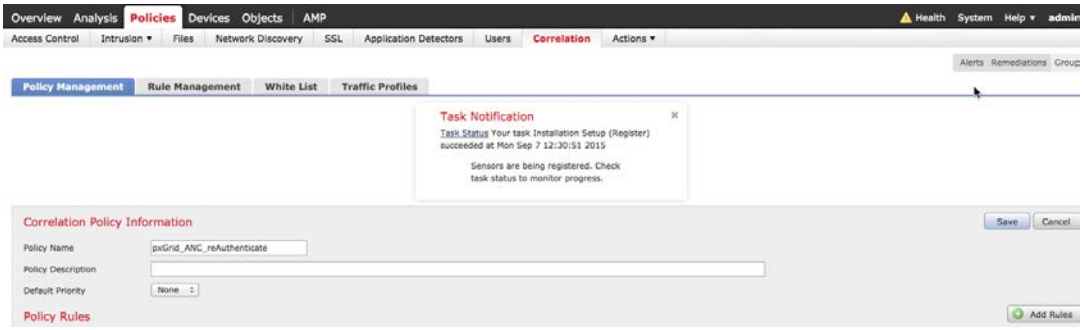
ステップ 9　　また、スイッチで、ポートの「shutdown」を確認できます。

```
interface GigabitEthernet1/0/3
 description internal LAN
 switchport mode access
 shutdown
 authentication host-mode multi-auth
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 authentication fallback mab
 mab
```

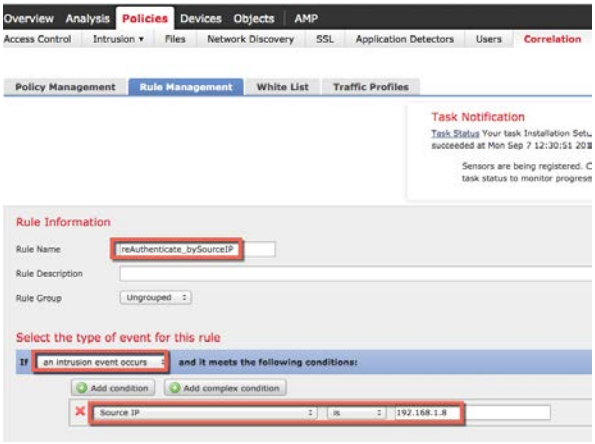
再認証

再認証ポリシーを作成します。

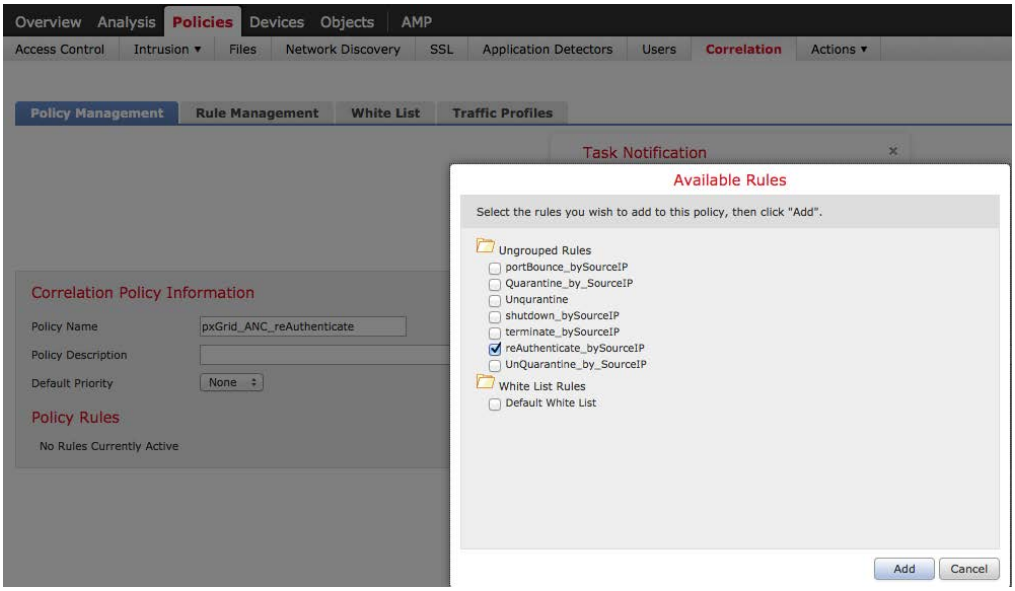
ステップ 1　　[ポリシー（Policies）] -> [相関（Correlation）] -> [ポリシー管理（Policy Management）] -> [ポリシーの作成（Create Policy）] -> [pxGrid ANC 再認証（pxGrid ANC reAuthenticate）] -> [保存（Save）] を選択します。



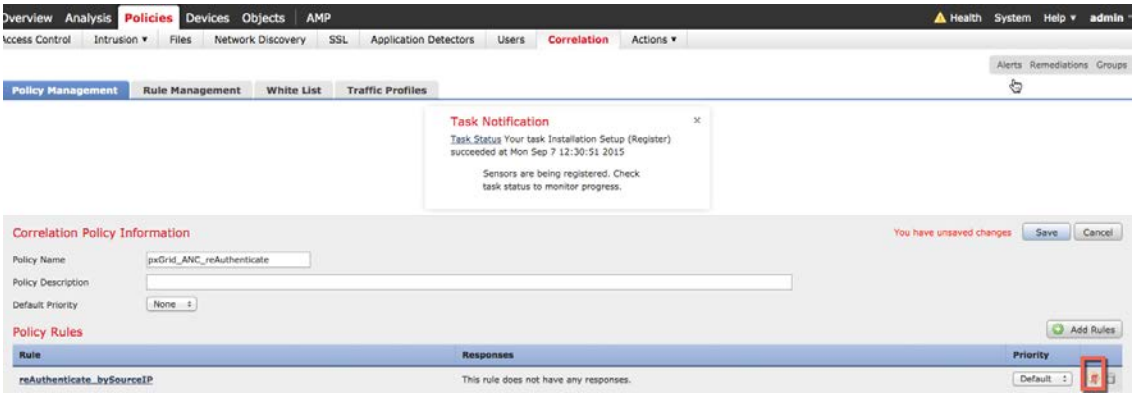
ステップ 2　　[ポリシー（Policies）] -> [相関（Correlation）] -> [ルール管理（Rule Management）] -> [ルールの作成（Create Rule）] を選択し、**reAuthenticate_bySourceIP** というルール名を追加し、次のように入力して、保存します。



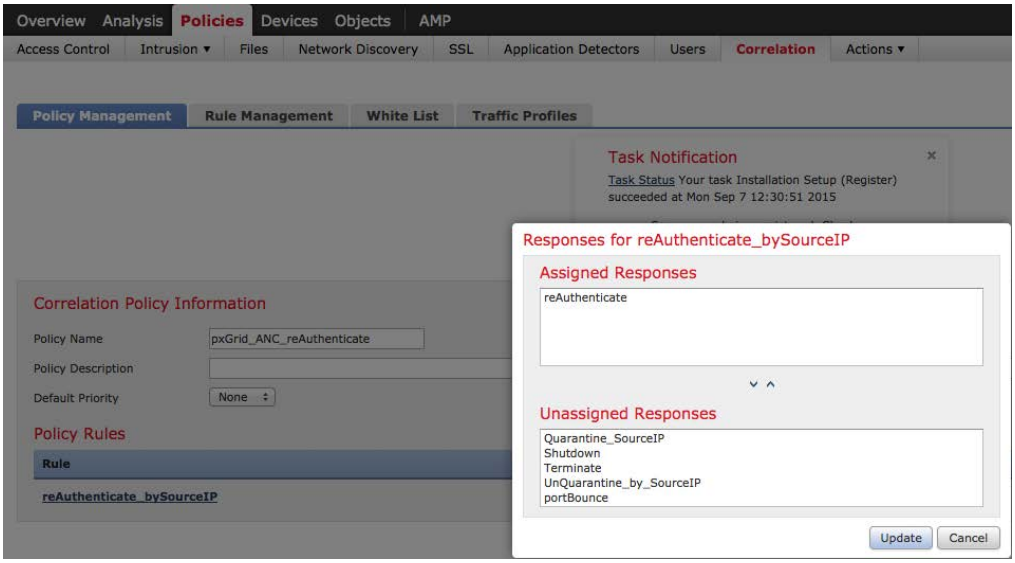
ステップ 3 [ポリシー（Policies）] -> [相関（Correlation）] -> [ポリシー管理（Policy Management）] -> [pxGrid_ANC_reAuthenticate] -> [ルールの追加（Add rules）] -> [reAuthenticate_bySourceIP] を選択して、ルールを追加します。



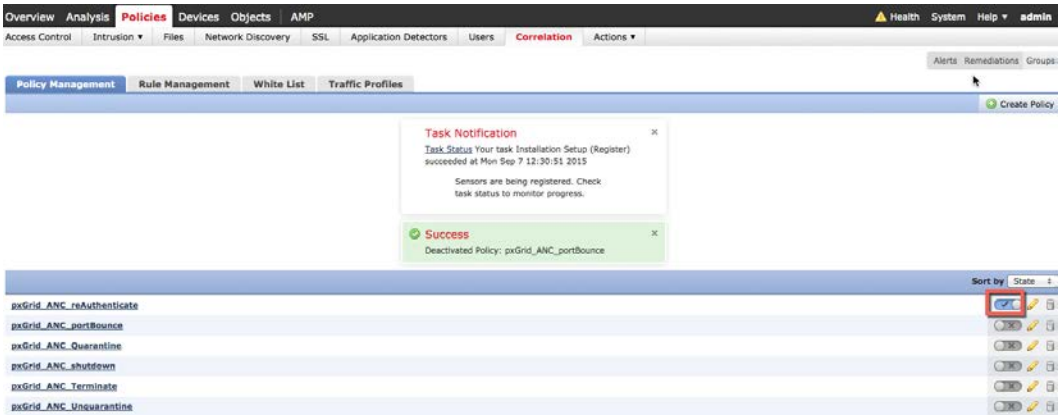
ステップ 4 次に、応答を追加します。[応答（Responses）] タブをクリックします。



ステップ 5 [ポリシー（Policies）] -> [相関（Correlation）] -> [pxGrid_ANC_reAuthenticate] を選択し、[再認証（reAuthenticate）] を [割り当てられた応答（Assigned Responses）] に移動し、[更新（Update）] -> [保存（Save）] を選択します。



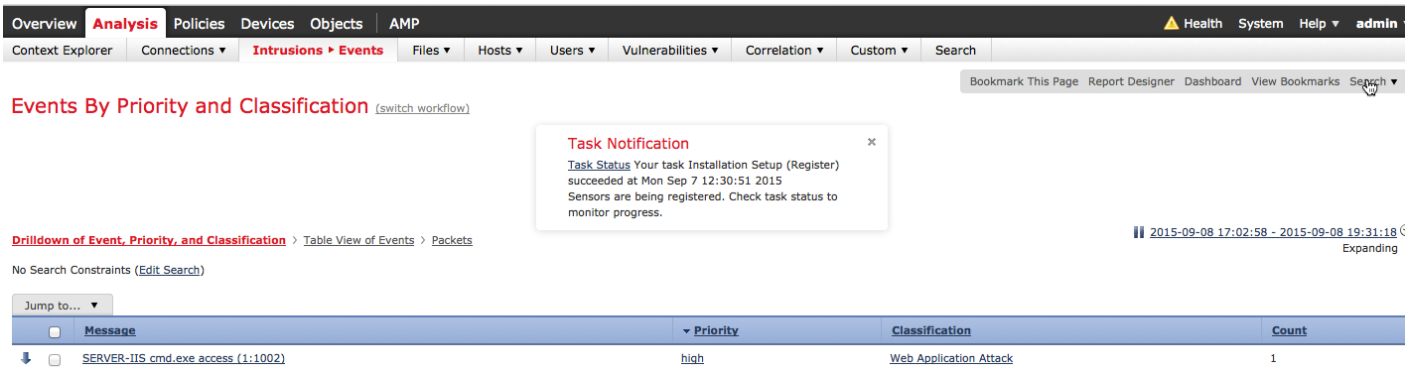
ステップ 6　　強制終了ポリシーをアクティブ化し、その下のボタンをクリックして、ポリシーを有効にします。



テスト

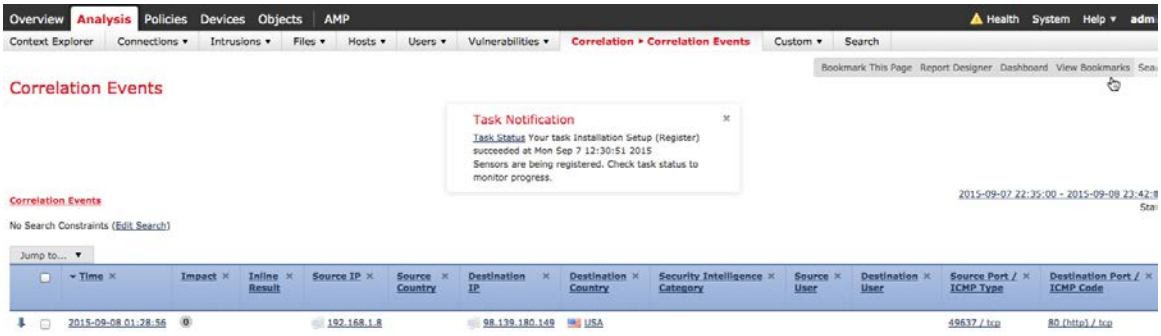
エンドユーザがブラウザ ウィンドウに www.yahoo.com/cmd.exe と入力すると、FireSIGHT の pxGrid 侵入ポリシーの「SERVER-IIS.cmd.exe アクセス」ルール違反から侵入イベントがトリガーされます。エンドポイントは、相関ポリシーで定義されているルールに割り当てられた再認証軽減応答に基づいて再認証されます。

ステップ 1　　エンドユーザはブラウザで www.yahoo.com/cmd.exe と入力します。
ステップ 2　　これは「Web アプリケーション攻撃」侵入イベントをトリガーします。

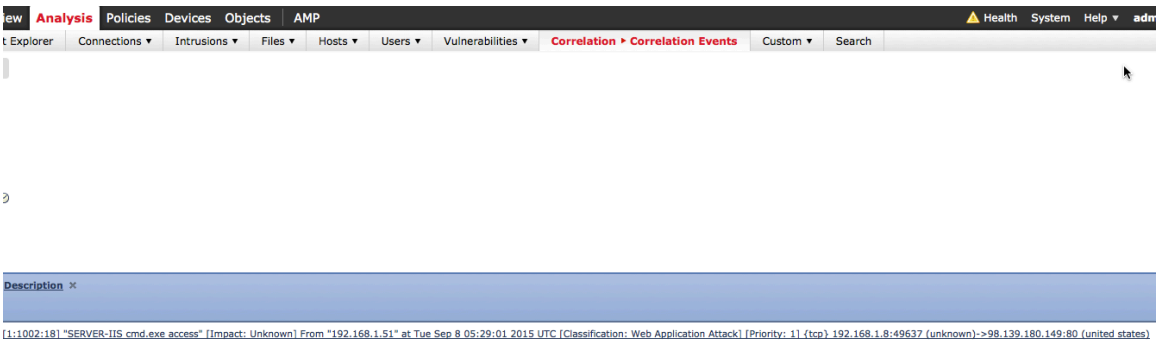


ステップ 3 また、「相関イベント」もトリガーします。
送信元 IP アドレスに属するエンドユーザが再認証されることに注意してください。

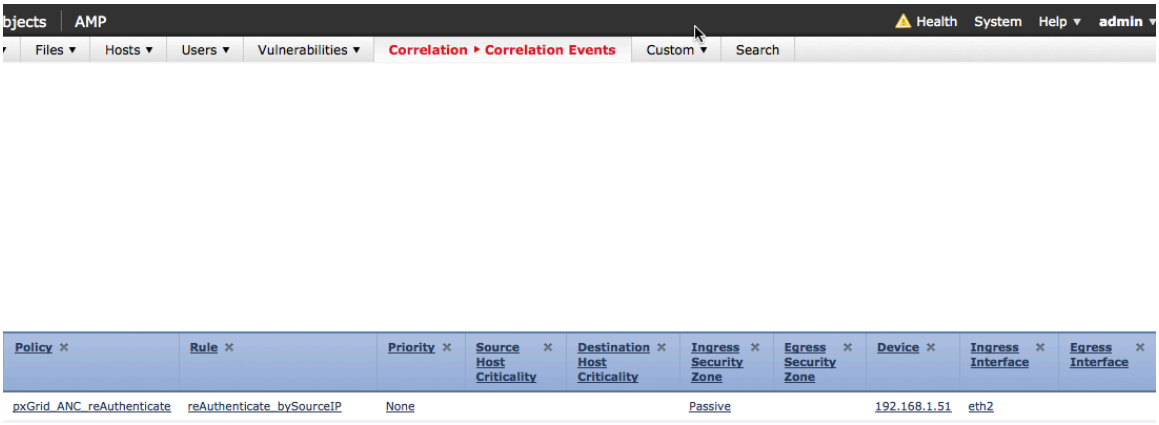
注：ネットワーク検出のホストおよびユーザが有効になっていないため、ユーザ情報はありません。



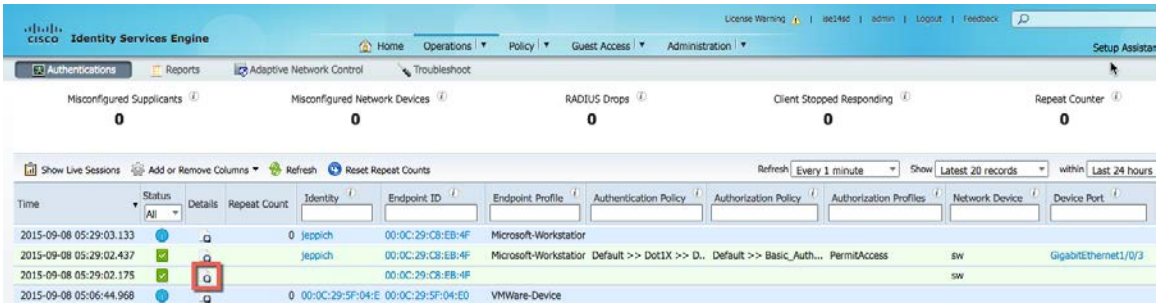
ステップ 4 同じイベントの作業を続けます。
pxGrid_Intrusion_Policy ルールに含まれているルール違反に注意してください。



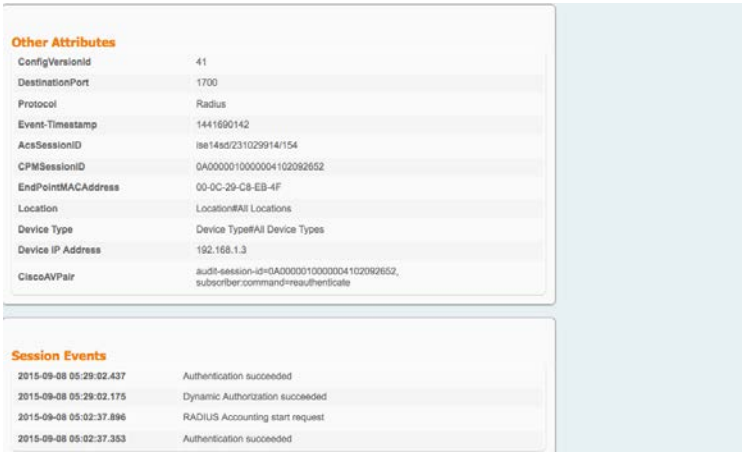
ステップ 5 同じイベントの作業を続けます。
割り当てられたポート再認証軽減応答をトリガーした相関ポリシーおよび相関ルールに注意してください。



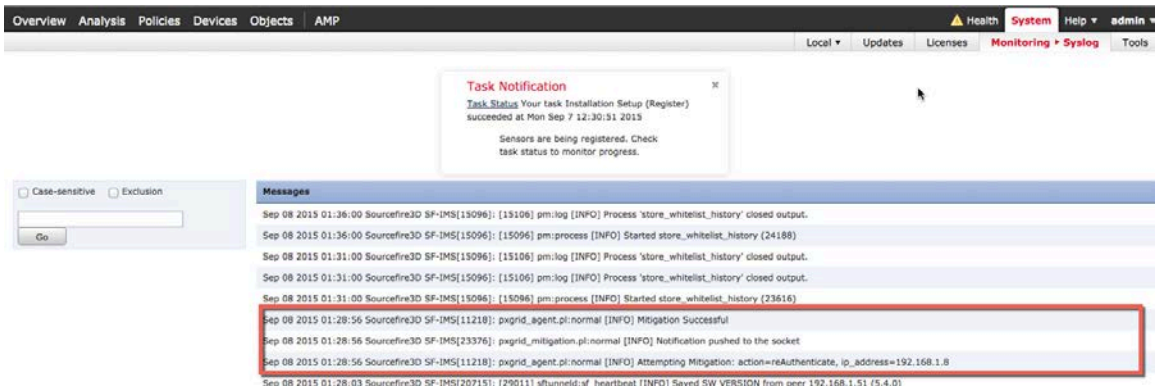
ステップ 6　ISE の応答を表示するには、[運用（Operations）] -> [認証（Authentications）] を選択します。



ステップ 7　詳細ボタンを選択すると、ポートが CiscoAVpair 属性に基づいて無効化されることがわかります。



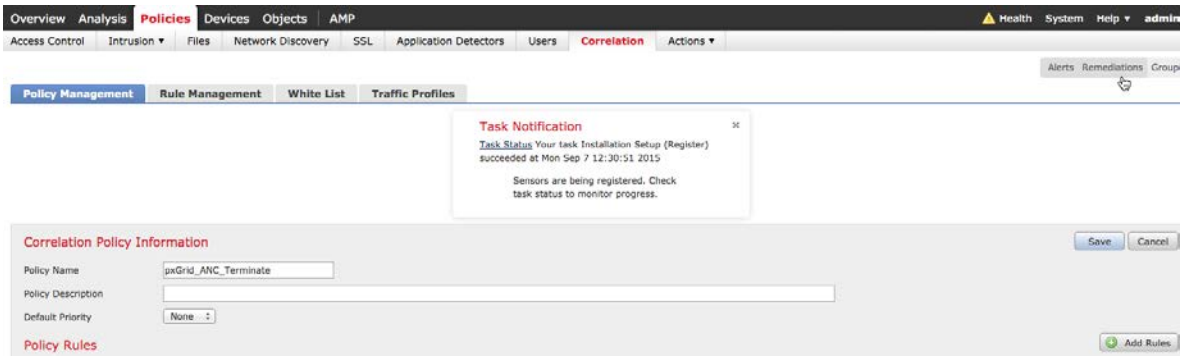
ステップ 8 また、FireSIGHT Management Center syslog イベントを表示して、再認証軽減アクションが成功したことを確認できます。



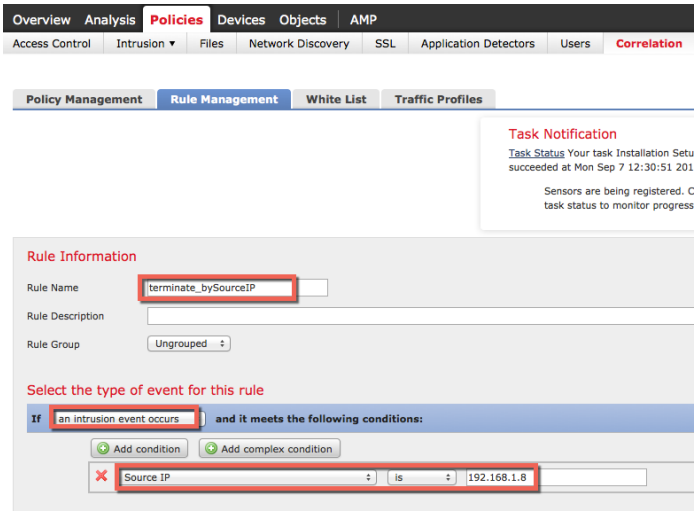
強制終了

強制終了相関ポリシーを作成します。

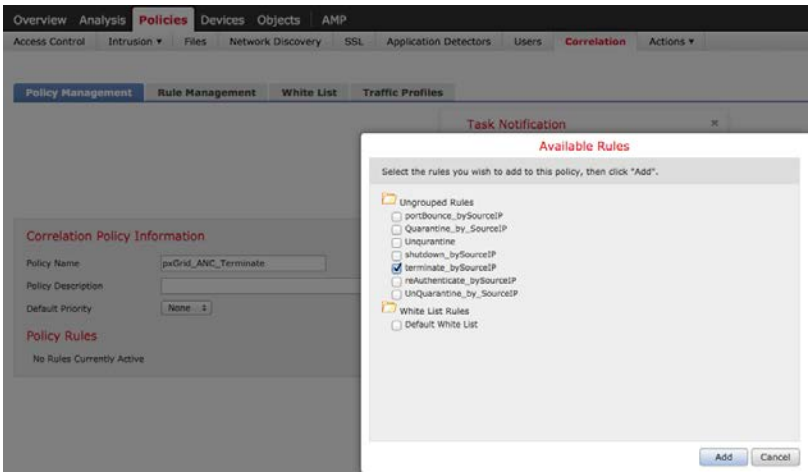
ステップ 1 [ポリシー（Policies）] -> [相関（Correlation）] -> [ポリシー管理（Policy Management）] -> [ポリシーの作成（Create Policy）] -> [pxGrid ANC 強制終了（pxGrid ANC Terminate）] -> [保存（Save）] を選択します。



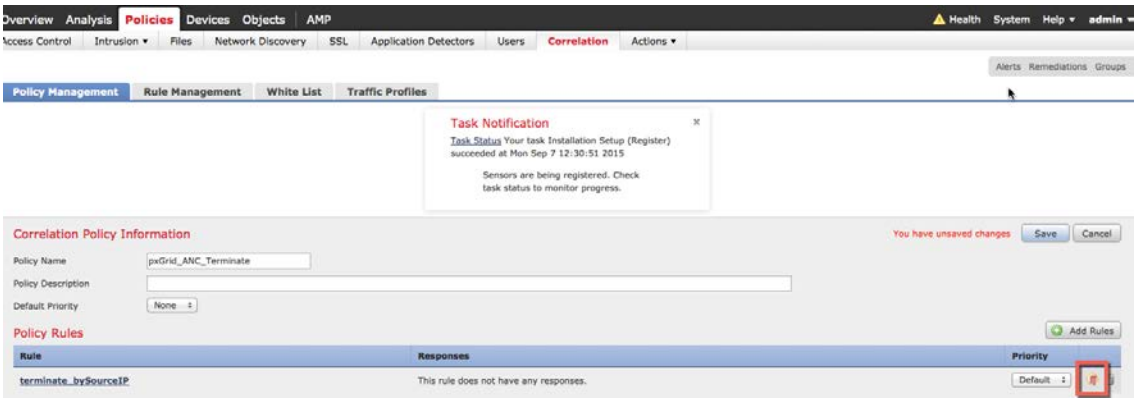
ステップ 2 [ポリシー（Policies）] -> [相関（Correlation）] -> [ルール管理（Rule Management）] -> [ルールの作成（Create Rule）] を選択し、**Terminate_by_SourceIP** というルール名を追加し、次のように入力して、保存します。



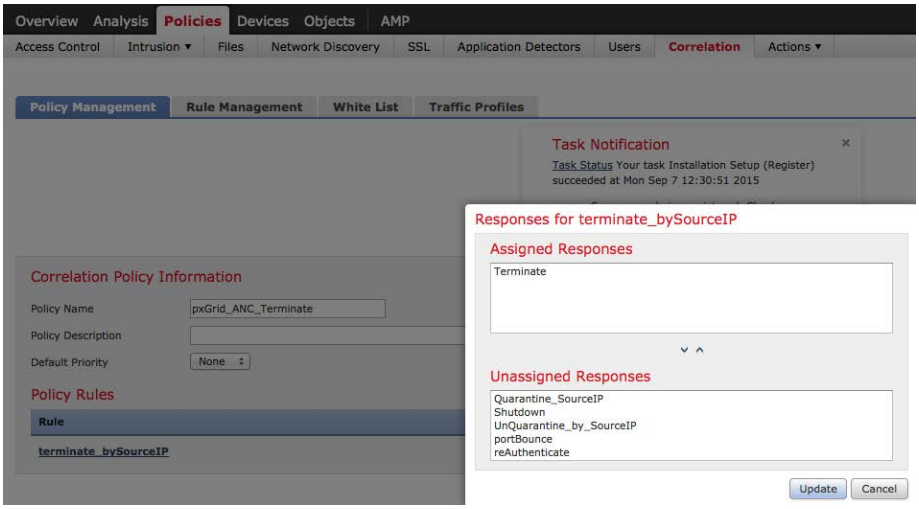
ステップ 3 [ポリシー（Policies）] -> [相関（Correlation）] -> [ポリシー管理（Policy Management）] -> [pxGrid ANC 強制終了（pxGrid ANC Terminate）] > [ルールの追加（Add rule）] -> [Terminate_by_SourceIP] を選択して、ルールを追加します。



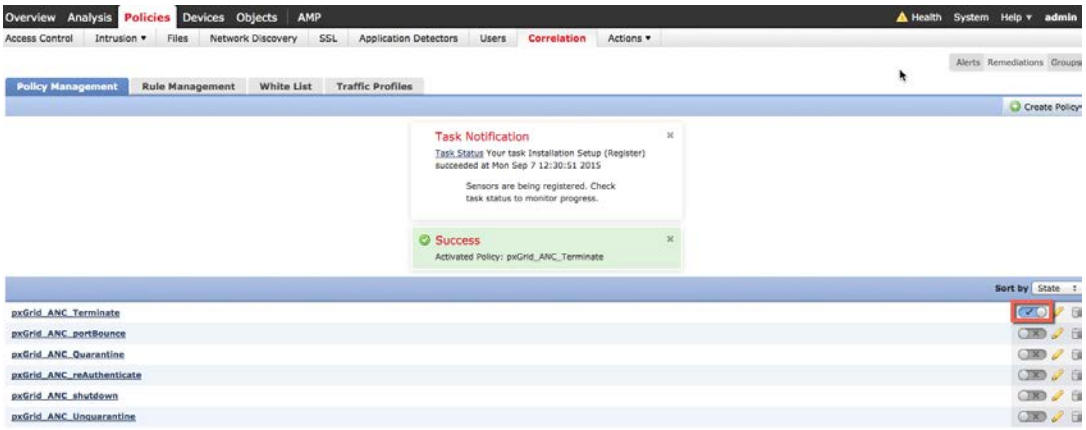
ステップ 4 次に、応答を追加します。[応答（Responses）] タブをクリックします。



ステップ 5 [ポリシー（Policies）] -> [相関（Correlation）] -> [pxGrid_ANC_Terminate] を選択し、[強制終了（Terminate）] を [割り当てられた応答（Assigned Responses）] に移動し、[更新（Update）] -> [保存（Save）] を選択します。



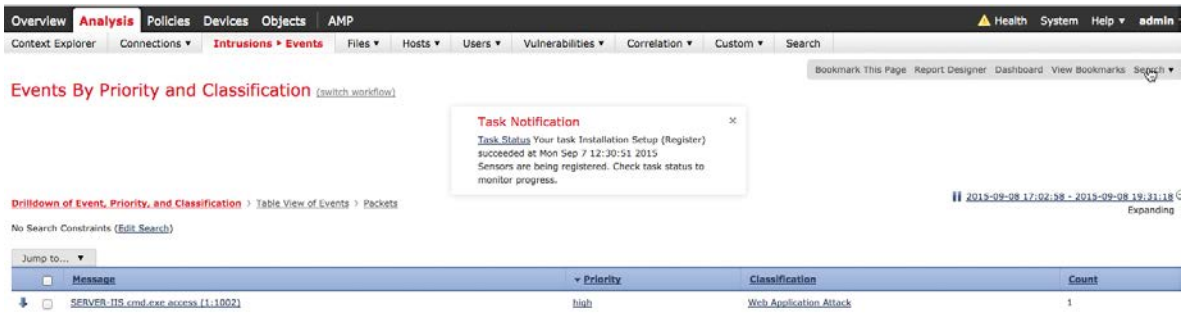
ステップ 6 強制終了ポリシーをアクティブ化し、その下のボタンをクリックして、ポリシーを有効にします。



テスト

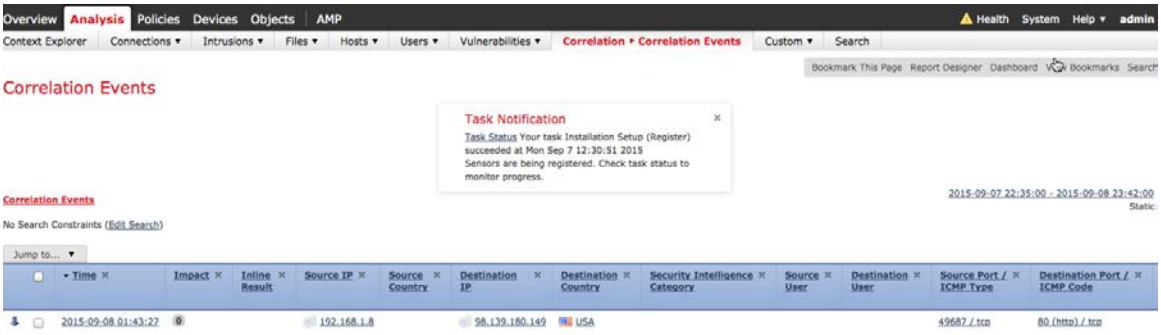
エンドユーザがブラウザ ウィンドウに www.yahoo.com/cmd.exe と入力すると、FireSIGHT の pxGrid 侵入ポリシーの「SERVER-IIS.cmd.exe アクセス」ルール違反から侵入イベントがトリガーされます。エンド ユーザのセッションは、相関ポリシーで定義されているルールに割り当てられた強制終了軽減応答に基づいて終了します。

ステップ 1 エンドユーザはブラウザで www.yahoo.com/cmd.exe と入力します。
ステップ 2 これは「Web アプリケーション攻撃」侵入イベントをトリガーします。

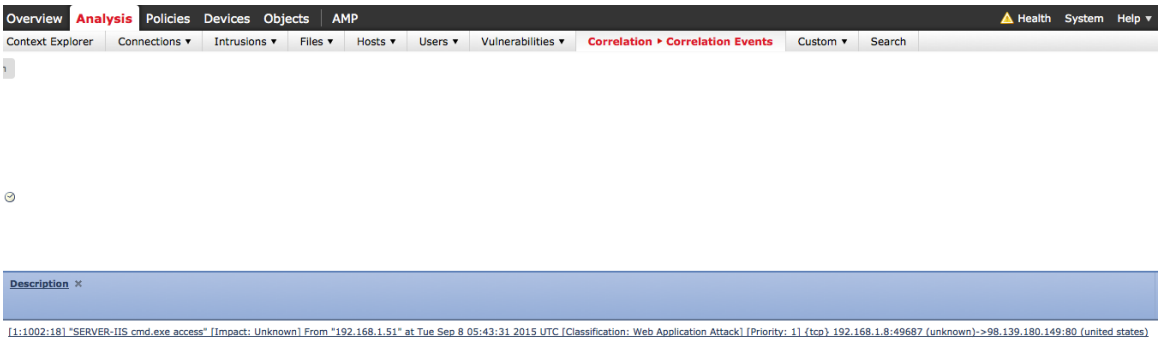


ステップ 3 また、「相関イベント」もトリガーします。
送信元 IP アドレスに属するエンドユーザ セッションが強制終了することに注意してください。

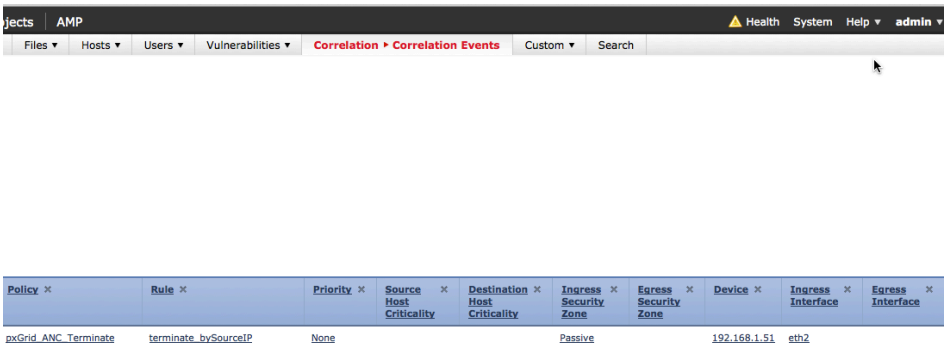
注: ネットワーク検出のホストおよびユーザが有効になっていないため、ユーザ情報はありません。



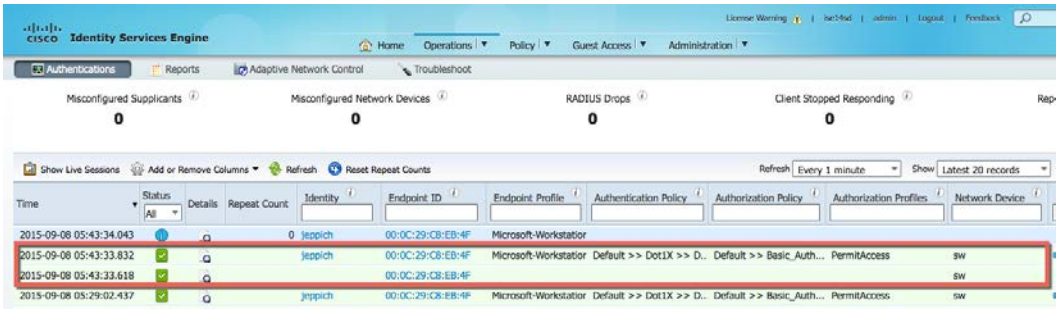
ステップ 4 同じイベントの作業を続けます。
pxGrid_Intrusion_Policy ルールに含まれているルール違反に注意してください。



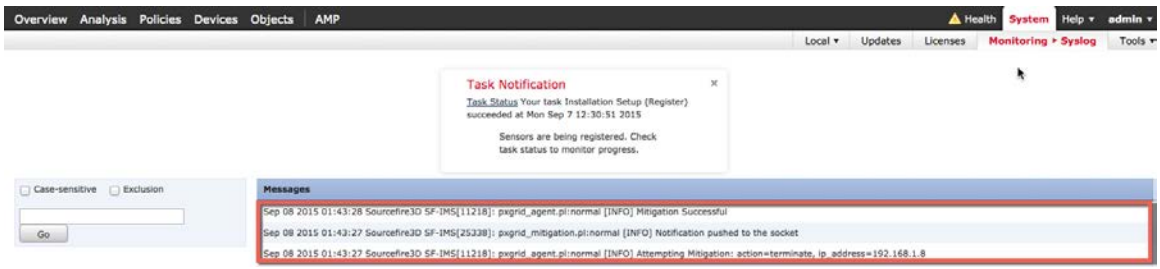
ステップ 5 同じイベントの作業を続けます。
割り当てられた強制終了軽減応答をトリガーした相関ポリシーおよび相関ルールに注意してください。



ステップ 6 ISE の応答を表示するには、[運用（Operations）] -> [認証（Authentications）] を選択します。



ステップ 7 また、FireSIGHT Management Center syslog イベントを表示して、強制終了軽減アクションが成功したことを確認できます。

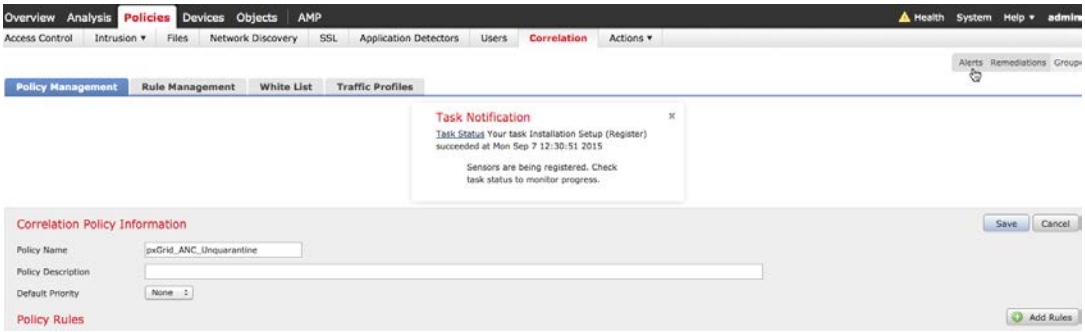


検疫解除相関ポリシー

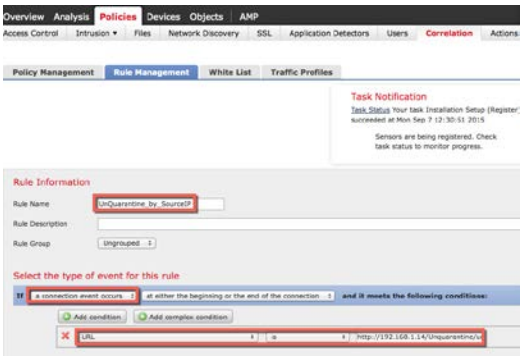
検疫解除相関ポリシーおよびルールは他の相関ポリシーと同様のプロセスで作成します。ただ 1 つの違いは、この相関ルールは「侵入」イベントではなく「接続」イベントからトリガーされることです。エンドユーザが検疫解除ルールで定義される URL を参照すると、検疫解除軽減応答がエンドポイントの検疫を解除します。

また、すべての HTTP/HTTPS トラフィックがモニタおよびロギングされ、pxGrid 侵入ポリシーも含むデフォルト アクセス ポリシーに割り当てられるように、「接続」ルールも作成する必要があります。

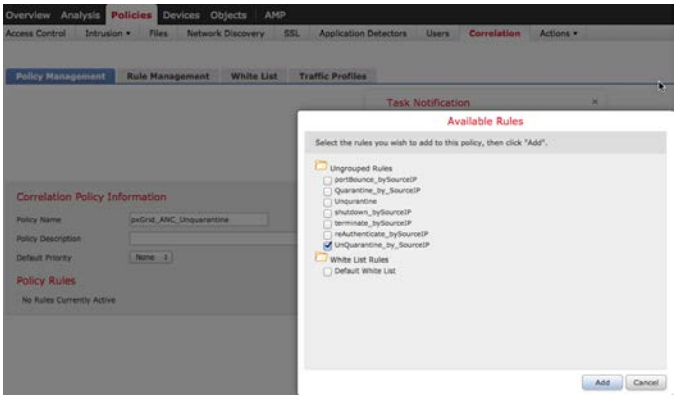
ステップ 1 [ポリシー（Policies）] -> [相関（Correlation）] -> [ポリシー管理（Policy Management）] -> [ポリシーの作成（Create Policy）] -> [pxGrid_ANC_Unquarantine] -> [保存（Save）] を選択します。



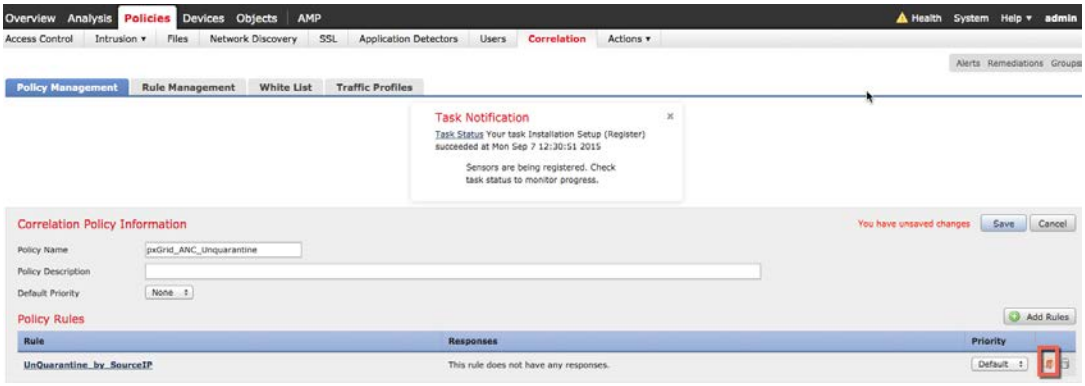
ステップ 2 [ポリシー（Policies）] -> [相関（Correlation）] -> [ルール管理（Rule Management）] -> [ルールの作成（Create Rule）] を選択し、**UnQuarantine_by_DestinationIP** というルール名を追加して、保存します。



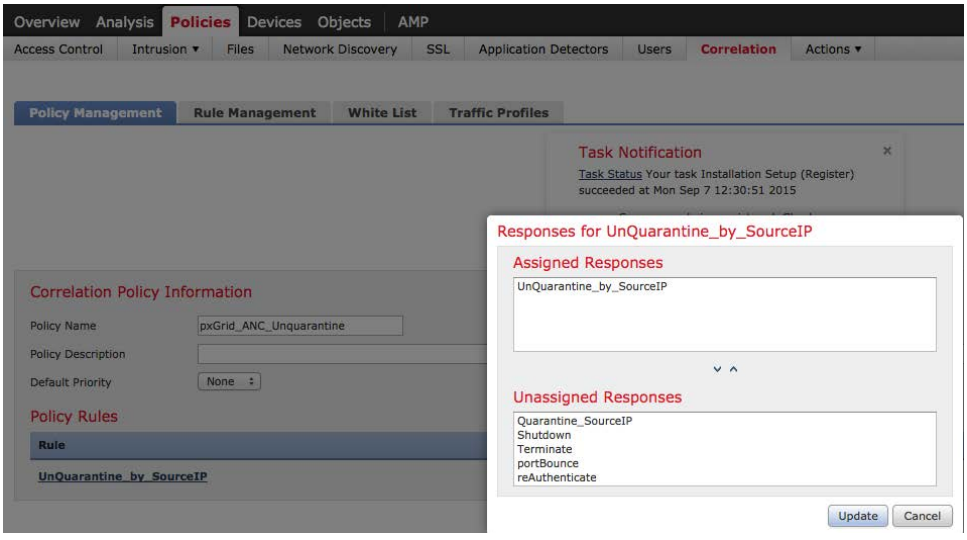
ステップ 3 [ポリシー（Policies）] -> [相関（Correlation）] -> [ポリシー管理（Policy Management）] -> [pxGrid_ANC_Unquarantine] > [ルールの追加（Add rules）] -> [UnQuarantine_by_DestinationIP] を選択して、変更を保存します。



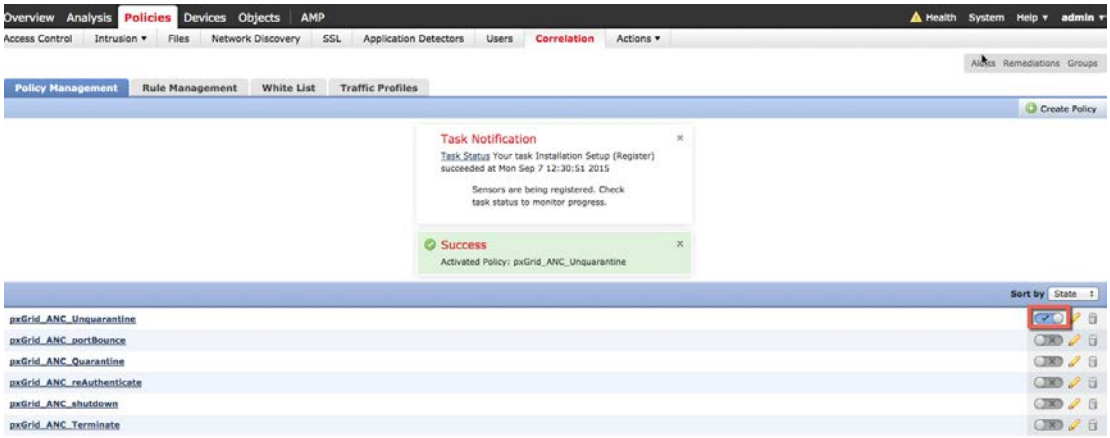
ステップ 4 次に、応答を追加します。[応答（Responses）] タブをクリックします。



ステップ 5 [ポリシー（Policies）] -> [相関（Correlation）] -> [UnQuarantine_by_DestinationIP] を選択し、[UnQuarantine_SourceIP] を [割り当てられた応答（Assigned Responses）] に移動し、[更新（Update）] -> [保存（Save）] を選択します。



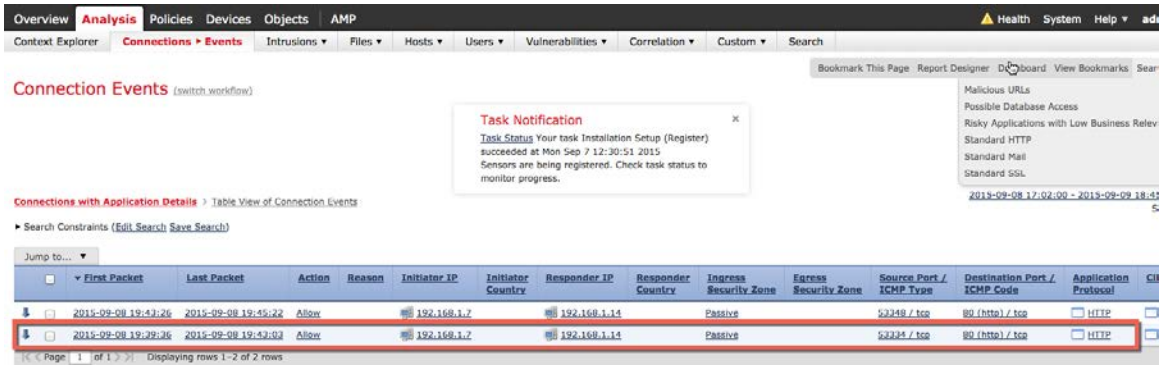
ステップ 6　ポリシーをアクティブ化します。



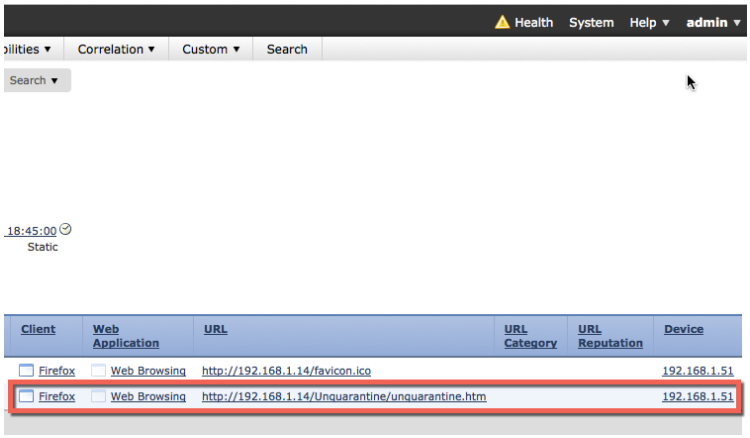
テスト

エンドユーザがブラウザ ウィンドウに www.yahoo.com/cmd.exe と入力すると、FireSIGHT の pxGrid 侵入ポリシーの「SERVER-IIS.cmd.exe アクセス」ルール違反から侵入イベントがトリガーされます。エンドポイントは、相関ポリシーで定義されているルールに割り当てられた検疫解除軽減応答に基づいて検疫解除されます。

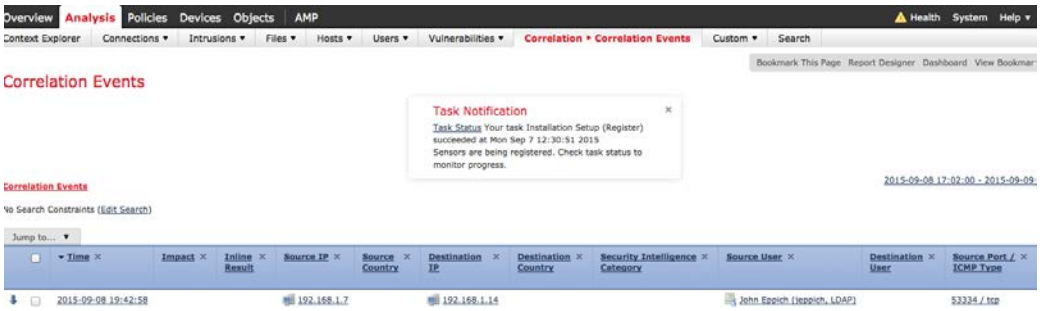
ステップ 1　エンドユーザはブラウザで http://192.168.1.14/Unquarantine/unquarantine.htm と入力します。
ステップ 2　これは「接続」イベントをトリガーします。



ステップ 3　ここでは、接続イベントが継続します。

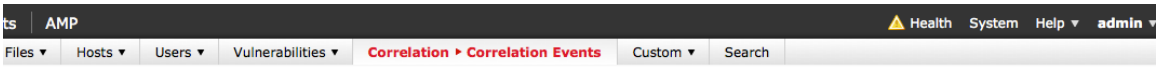


ステップ 4　また、「相関イベント」もトリガーします。
送信元 IP アドレスが検疫解除されることに注意してください。



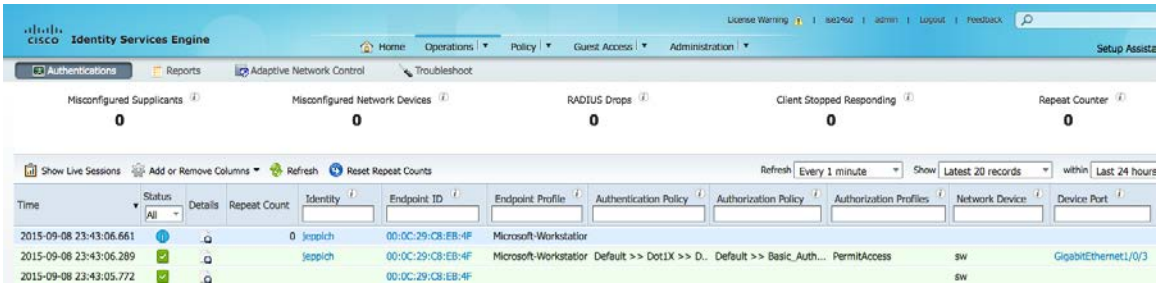
ステップ 5　同じイベントの作業を続けます。
接続イベントに注意してください。

ステップ 6　同じイベントの作業を続けます。
割り当てられた検疫軽減応答をトリガーした相関ポリシーおよび相関ルールに注意してください。

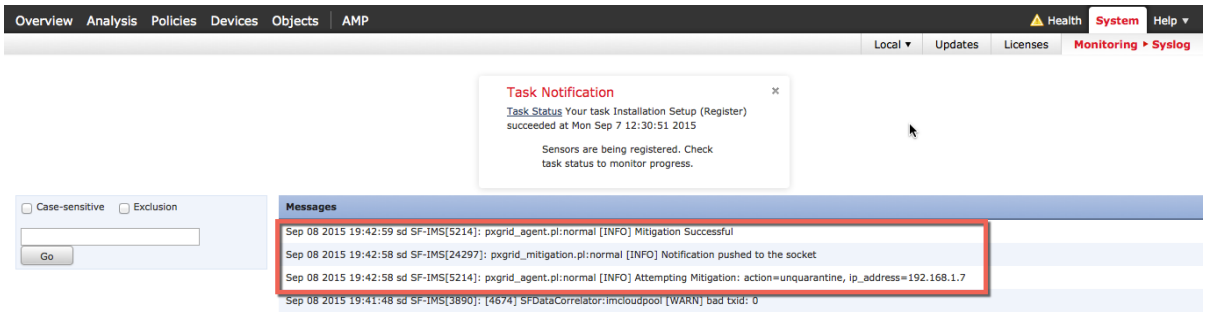


Policy	Rule	Priority	Source Host Criticality	Destination Host Criticality	Ingress Security Zone	Egress Security Zone	Device	Ingress Interface	Egress Interface
pxGrid_ANC_Unquarantine	UnQuarantine_by_SourceIP	None	None	None	Passive		192.168.1.51	eth2	

ステップ 7　ISE の応答を表示するには、[運用（Operations）] -> [認証（Authentications）] を選択します。



ステップ 8　また、FireSIGHT Management Center syslog イベントを表示して、検疫解除軽減アクションが成功したことを確認できます。



トラブルシューティング

ISE pxGrid サービスが起動しない

解決策：ISE pxGrid ノードで「**application stop ise**」を実行して停止します。

pxGrid エージェント証明書エラー メッセージ

解決策：FireSIGHT Management Center Syslog メッセージを表示して、証明書エラー メッセージを確認します。

証明書のフル パスが正しいことを確認します。**/Volume/home/admin/…**

FireSIGHT Management Center と ISE pxGrid ノード間で時刻が同期されていることを確認します。

FireSIGHT、ISE pxGrid ノード、およびエンドポイントはすべて DNS 解決可能である必要があります。

FireSiGHT Management Center が ISE と通信していない

解決策：FireSIGHT、ISE pxGrid ノード、およびエンドポイントはすべて DNS 解決可能である必要があります。

FireSIGHT Management Center、センサー、および ISE pxGrid ノード間で時刻が同期されていることを確認します。

FireSIGHT Management Center を再起動します。

FireSIGHT Management Center に相関イベントがまったく表示されない

解決策：FireSIGHT Management Center、センサー、および ISE pxGrid ノード間で時刻が同期されていることを確認します。

FireSIGHT が軽減試行に失敗した

解決策：FireSIGHT Management Center、センサー、および ISE pxGrid ノード間で時刻が同期されていることを確認します。

FireSIGHT Management Center を再起動します。

軽減試行で「ルックアップ失敗」

解決策：デバイスの IP アドレスが ISE によって認証されていることを確認します。修復タイプを送信元に対して設定しておきます。

pxGrid 接続障害により FireSIGHT Management Console からのエラー メッセージが syslog に記録される

解決策：FireSIGHT Management Console CLI で次を実行し、ISE pem ファイルに証明書が含まれていることを確認します。

```
openssl x509 -noout -text -in ise14lab.pem
```

pem ファイルには証明書が含まれている必要があります。

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            56:19:bf:90:00:00:00:00:ab:b7:4f:a0:57:21:a0:03
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=ise14.lab8.com
        Validity
            Not Before: Oct 11 01:46:56 2015 GMT
            Not After : Oct 10 01:46:56 2016 GMT
        Subject: CN=ise14.lab8.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:a3:9e:b5:4e:68:e7:f9:db:4b:c6:3f:f4:f9:12:
                    e8:6f:ba:05:4d:b6:0b:13:fc:3c:35:61:ed:d6:d1:
                    0d:65:f4:e5:38:3d:5a:55:ac:94:e6:34:57:44:30:
                    64:75:9c:35:6f:f2:9c:0a:d6:f4:86:9d:94:10:2f:
                    b6:eb:ba:76:e2:33:84:77:70:20:71:a0:23:21:4b:
                    af:cc:6a:d9:c2:ba:9a:9c:eb:27:e6:b3:64:a7:e5:
                    29:31:65:03:23:06:d8:39:b9:74:48:32:75:de:6a:
                    5c:71:6a:27:8e:e6:d3:58:d0:44:e6:52:ec:3f:d8:
                    38:5b:d2:fc:c2:d6:90:02:e8:5a:9f:a7:a2:dc:44:
                    81:31:fc:5e:fd:60:41:40:e6:57:09:9b:d6:11:0e:
                    a6:93:1b:b0:c1:c5:9b:c4:98:45:af:78:1b:9c:55:
                    02:d3:e5:91:48:8b:1c:77:46:e6:49:d5:f0:5f:4c:
                    51:6c:d0:9b:82:25:b3:32:3b:ab:64:32:49:e5:b7:
                    45:db:9e:2c:c4:87:dc:d1:ff:9c:f8:99:d7:88:be:
                    c6:9d:7c:c6:ea:74:bd:b0:c5:a2:b5:a4:d4:fd:04:
                    64:61:db:c5:cb:07:69:d3:c7:72:8f:17:a7:2e:04:
                    11:d5:58:0d:00:aa:26:3a:5f:c3:08:2c:dc:a0:26:
                    e8:87
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:TRUE
            X509v3 Key Usage:
                Digital Signature, Key Encipherment, Key Agreement, Certificate Sign
            X509v3 Subject Key Identifier:
                8E:C0:5C:25:3A:5C:4E:9F:C4:6F:66:41:33:C3:6A:27:4C:00:A1:17
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            Netscape Cert Type:
                SSL Server
    Signature Algorithm: sha1WithRSAEncryption
         40:cc:1b:4d:94:94:d9:68:7b:95:6e:36:e4:3a:41:41:6c:f1:
         4e:f0:1a:fa:3e:42:7e:b0:73:80:ad:0f:4a:bb:d4:ce:cd:da:
         ef:32:f9:d0:58:f0:c4:90:0c:97:20:88:26:f5:9c:96:d7:61:
         fe:05:09:40:0a:f6:33:04:dc:30:ec:10:d2:82:f2:ec:5d:f9:
         b2:d1:69:5e:ed:ae:a5:b4:6d:b1:c4:16:bf:67:14:e9:ec:4f:
         9c:83:07:35:64:26:9d:e4:41:bb:65:5e:77:7b:e5:da:d1:98:
         9c:c0:50:fc:ba:a4:dc:51:c4:e5:49:28:55:9f:40:0c:61:20:
```

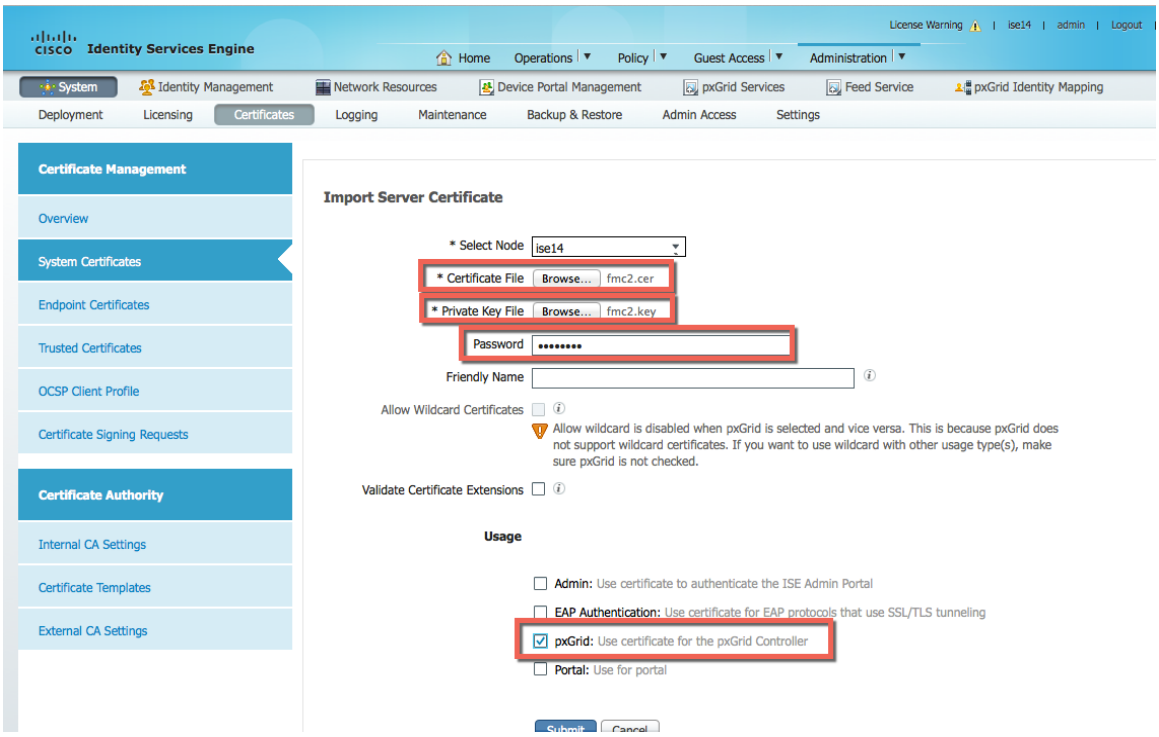
```
1d:49:e3:ca:a5:a2:35:74:5c:57:71:17:32:71:2c:2b:51:2c:
cf:49:30:9e:31:28:19:4a:62:1b:4a:86:21:0d:54:73:b8:86:
92:df:8c:ae:3d:92:91:5f:70:d5:17:4c:14:07:d1:0c:59:0b:
3d:6d:6a:16:ca:a9:3a:06:b8:37:f1:28:af:c5:03:32:30:82:
3d:53:8b:77:ed:e7:8a:5a:38:b6:3b:0e:c0:93:63:c1:f6:2e:
a3:ce:33:a4:0a:82:d4:f7:8f:0f:c2:99:9e:96:36:c5:89:a2:
9f:f3:66:01:12:da:13:53:d4:92:ef:17:9e:2b:26:4b:3c:7d:
1f:6f:a3:b4
```

このように表示されない場合は、ISE 識別自己署名公開/秘密キー ペアをエクスポートし、パスワードを指定して、ISE 識別自己署名証明書を FMC 信頼 CA ストアに追加します。

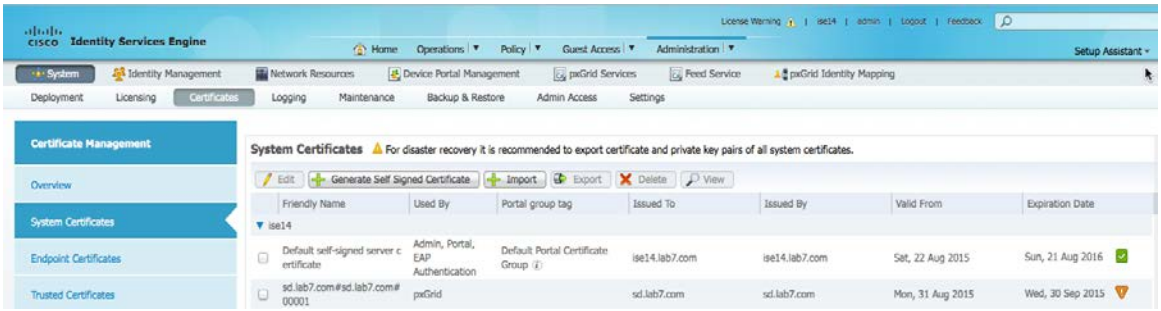
ISE システム ストアへのインポートによる自己署名証明書の検証

解決策：これは必ずしも問題ではありませんが、ベンダーの公開/秘密キー ペアは ISE 信頼システム ストアにインポートされることがあります。これは pxGrid SDK の ISE サンプル証明書を使用することが原因です。これはテストにのみ使用するべきであり、本番用には推奨されません。自己署名証明書の設定には、「自己署名証明書用の FireSIGHT Management Center の設定」の手順を使用してください。

ステップ 1 FireSIGHT 内部 CA 公開/秘密キー ペアを ISE 証明書システム ストアにインポートします。秘密キーのパスワードが必要です。
[管理（Administration）] -> [システム（System）] -> [証明書（Certificates）] -> [システム証明書（System Certificates）] を選択し、FireSIGHT 内部公開/秘密キー ペアをインポートします。秘密キーのパスワードを入力します。



ステップ 2 証明書の [用途（Usage）] には [pxGrid] を選択し、送信します。
ステップ 3 次が表示されます。


Identity Services Engine
Home
Operations
Policy
Guest Access
Administration
Setup Assistant
System
Identity Management
Network Resources
Device Portal Management
pxGrid Services
Feed Service
pxGrid Identity Mapping
Deployment
Licensing
Certificates
Logging
Maintenance
Backup & Restore
Admin Access
Settings
Certificate Management
Overview
System Certificates
Endpoint Certificates
Trusted Certificates
System Certificates
For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.
Edit
Generate Self Signed Certificate
Import
Export
Delete
View
Friendly Name
Used By
Portal group tag
Issued To
Issued By
Valid From
Expiration Date
ise14
Default self-signed server certificate
Admin, Portal, EAP Authentication
Default Portal Certificate Group
ise14.lab7.com
ise14.lab7.com
Sat, 22 Aug 2015
Sun, 21 Aug 2016
sd.lab7.com#sd.lab7.com#00001
pxGrid
sd.lab7.com
sd.lab7.com
Mon, 31 Aug 2015
Wed, 30 Sep 2015

不具合の解決

pxGrid & Identity マッピング サービスが再起動する

説明：証明書が ISE 展開の信頼ストアからインポートまたは削除された場合、ISE pxGrid ノードで pxGrid & Identity マッピング サービスが再起動します。

提起された障害：CSCuv43145

回避策：サービスは自動的に再起動するために回避策は必要ありませんが、サービスが再起動中は新しい検疫イベントは処理されません。

解決の計画：ISE Carlsbad リリース 2016 年春

アクティブな pxGrid ノードが GUI に反映されない。CLI には反映される

説明：pxGrid HA 展開で 2 つの pxGrid ノードが利用可能な場合、1 つはアクティブで、もう 1 つはスタンバイです。どちらがアクティブかを識別する際、管理者は CLI で pxGrid のステータスを確認する必要があります。ステータスは UI の [展開（Deployment）] ページに表示されません。この追加は Carlsbad で行われます。

回避策：CLI を使用してアクティブ/パッシブの状態を判別します。

解決の計画：ISE Carlsbad リリース 2016 年春

参考資料

分散 ISE 環境での pxGrid の設定:
http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-88-Configuring-pxGrid-in-an-ISE-Distributed-Environment.pdf

Cisco pxGrid による 証明書の展開方法。CA 署名 ISE pxGrid ノードおよび CA 署名 pxGrid クライアントの設定:
http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-89-CA_signed_pxGridISEnode_CAsigned_pxGridclient.pdf

Cisco pxGrid による証明書の展開方法。ISE pxGrid ノードと pxGrid クライアントを使用する自己署名証明書:
http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-90-Self_signed_pxGridClient_selfsigned_pxGrid.pdf