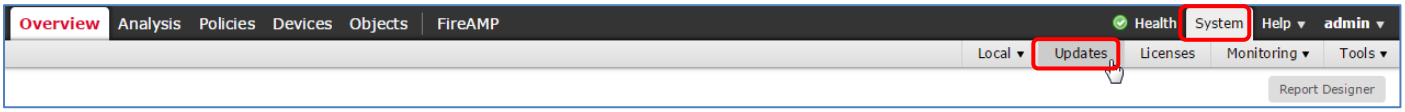
SRU(Sourcefire Rule Update)インストール方法

2015/02/15

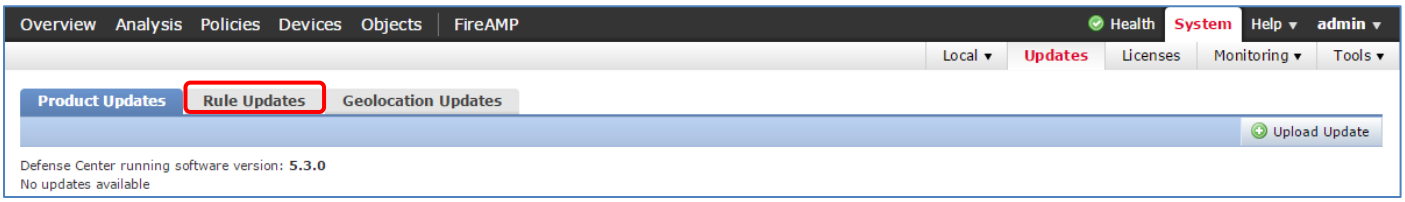
Rev1.0

FireSight(Defense Center) 上にて、手動での SRU(Sourcefire Rule Update) のアップデート方法をご紹介します。FirePower については、FireSight 上でアップデートを実施した後に FireSight から FirePower に新しい SRU 情報をアップデートします。FirePower の SRU アップデートについては本ドキュメント中で説明いたします。

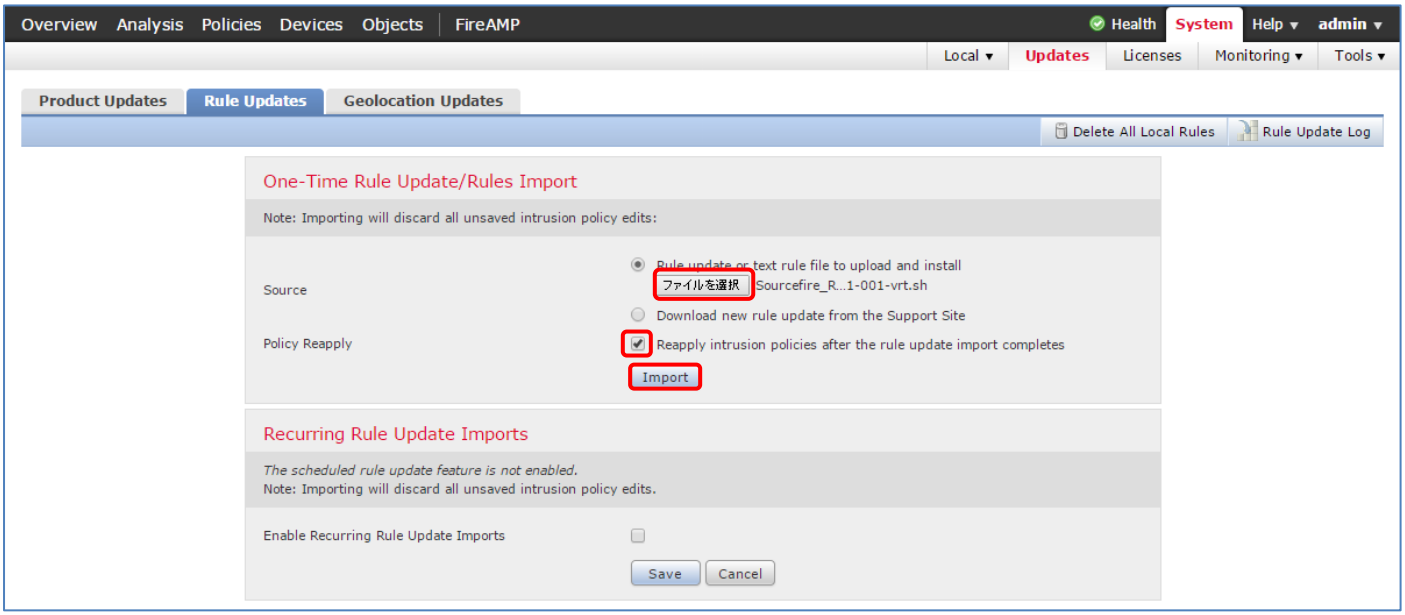
FireSight の GUI にログインします。(https://<FireSight IP アドレス>)
トップ画面から、System -> Updates に移動します。



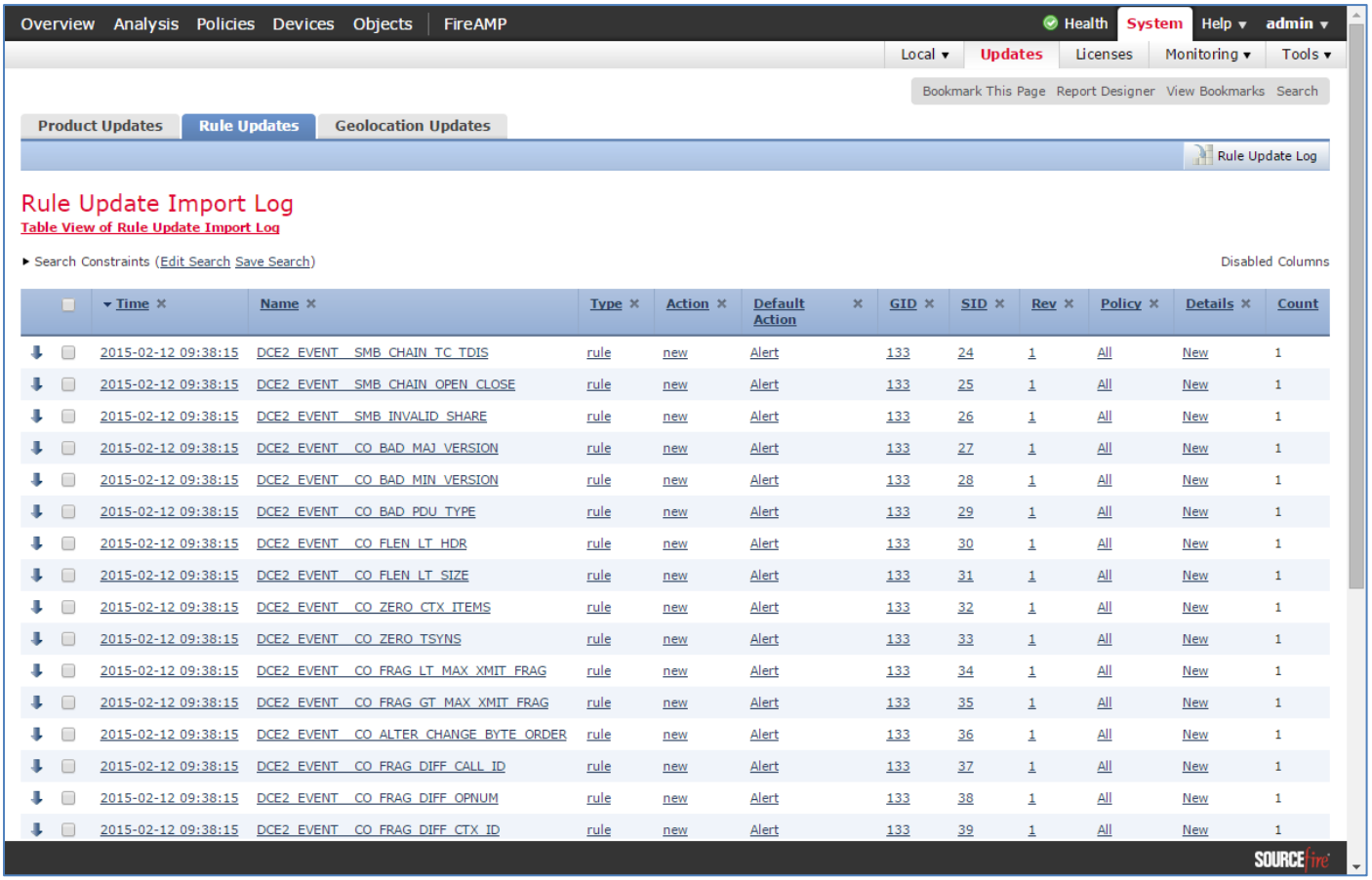
Rule Updates タブをクリックします。



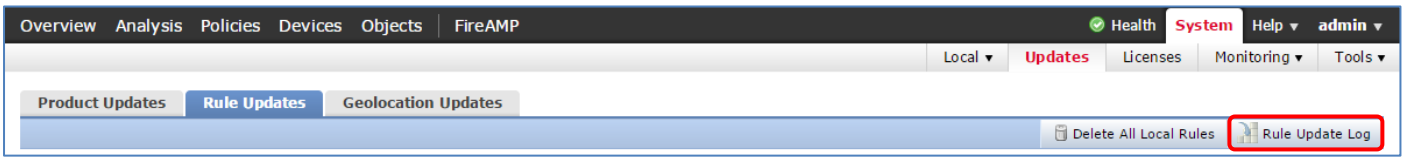
・ファイルを選択 ボタンをクリックして、適応したい SRU を選択する。(PC 上に SRU ファイルがある必要があります)
・(オプション)Policy intrusion policies after the rule update import completes のチェックボックスにチェックして、FirePower に新しい SRU 情報を FS に適用後に、適用します。※1
・Import ボタンを押して、SRU 情報をアップデートします。
※数分の間、この画面で止まっている状態となります。



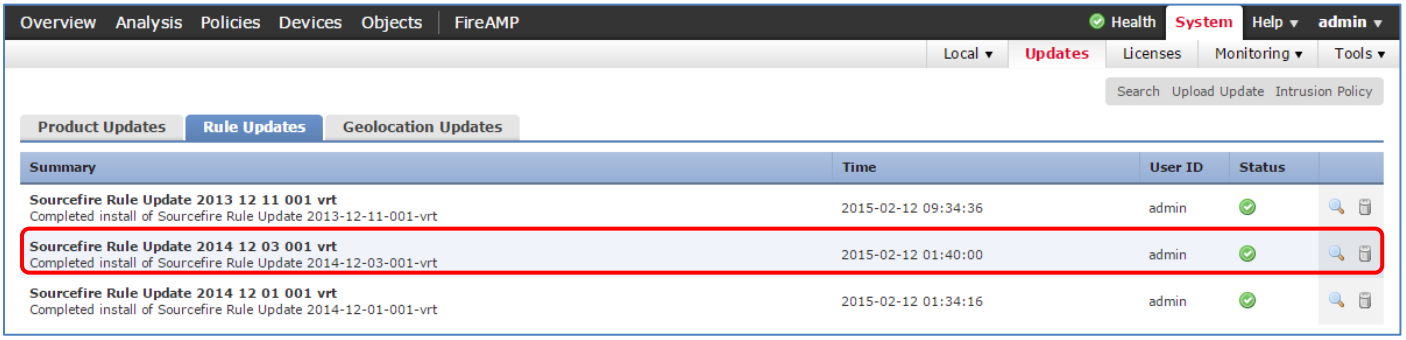
数分後、以下のような新しいルールの一覧が自動的に表示されます。
以上で、FS への SRU アップデートは完了です。本画面が表示されると、自動的に FirePower へ新しい SRU のアップデートが開始されます。



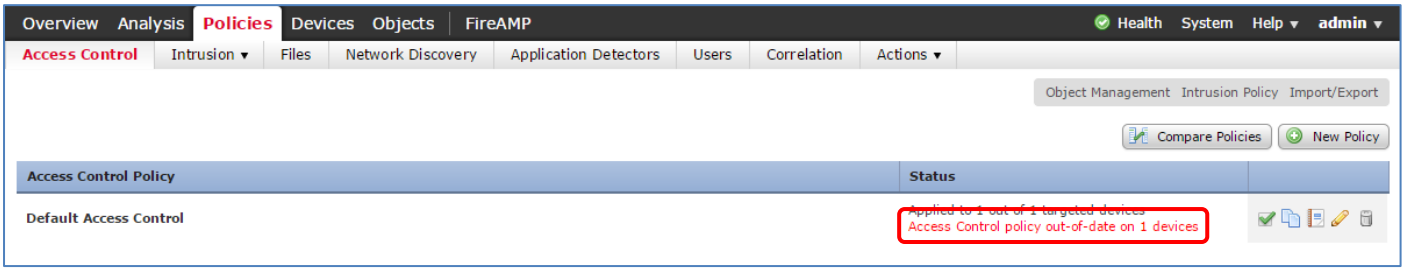
FireSight 上への SRU 更新完了確認方法
System > Updates > Rule Updates 上の Rule Update Log ボタンをクリックする。



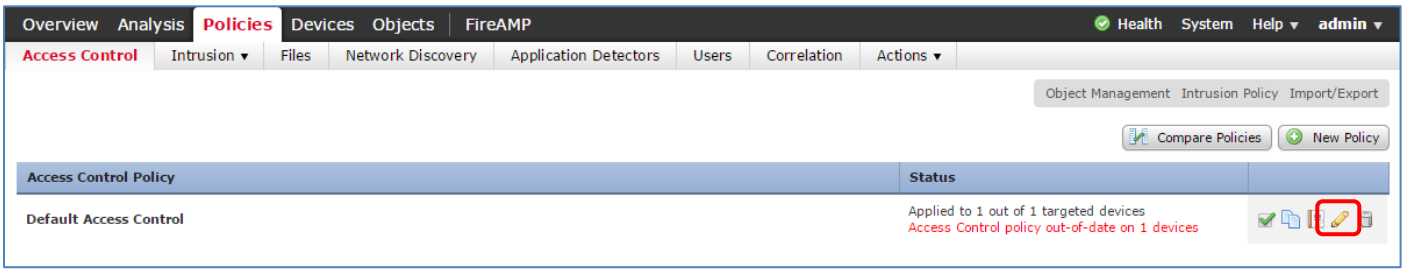
適応した SRU が表示され、Status が ● になっていることを確認する。



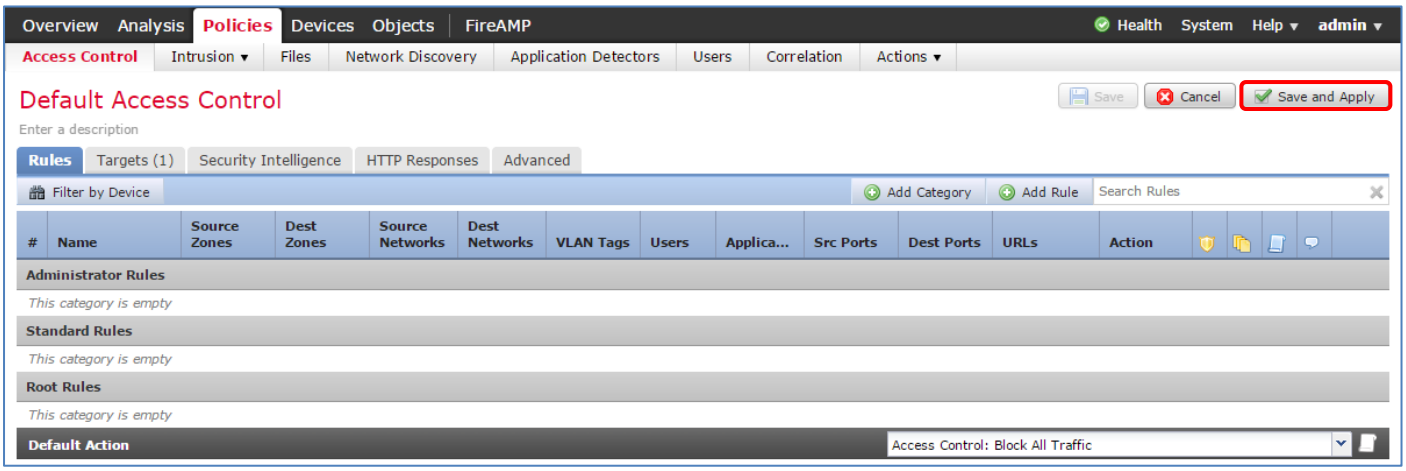
※1
(オプション)Policy intrusion policies after the rule update import completes のチェックボックスでチェックしなかった場合には、FireSight の SRU 適応が完了しても自動的には FirePower には適応しません。
完了後、FireSight の Policy > Access Control のページに移動すると Access Control policy out-of-date on xx devices というメッセージが表示されます。これは、FireSight と FirePower の SRU バージョンが違う際に表示されます。
※これ以前に、Access Control Policy を変更している場合には、SRU 以外の他の変更点がある場合があります。



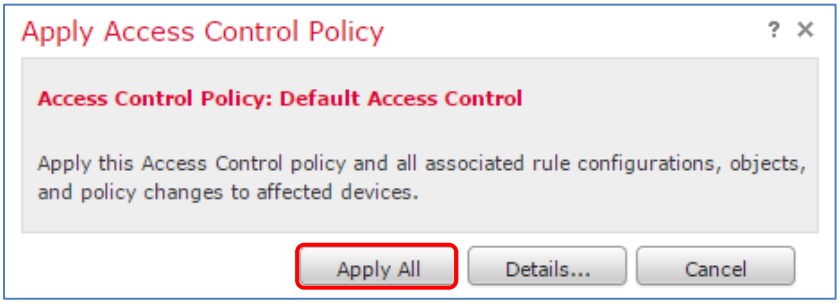
FirePower にも新しい SRU を適用するには
Access Control policy out-of-date on xx devices メッセージの右側にある ボタンをクリックする。



Save and Apply ボタンをクリックする。



Apply All ボタンを押すと、新しいポリシー(新しい SRU)を FirePower に適用します。



以上