AMP とポスチャ サービスの ISE 2.1 脅威中心型 NAC（TC-NAC）を設定する

目次

概要

このドキュメントでは、Identity Services Engine（ISE）2.1 で Advanced Malware Protection（AMP）を使用して脅威中心型 NAC を設定する方法について説明します。 脅威の重大度と脆弱性アセスメントの結果を使用することで、エンドポイントまたはユーザのアクセス レベルを動的に制御することができます。 ポスチャ サービスについてもこのドキュメントの一部として説明します。

> **注:** 本書の目的は、ISE 2.1 と AMP の統合について説明することであり、ポスチャ サービスは、AMP を ISE からプロビジョニングする際に必要であるために示しています。

前提条件

要件

Cisco では、次の項目について基本的な知識があることを推奨しています。

- Cisco Identity Service Engine
- 高度なマルウェア対策

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco Identity Service Engine バージョン 2.1
- ワイヤレス LAN コントローラ（WLC）8.0.121.0
- AnyConnect VPN クライアント 4.2.02075
- Windows 7 Service Pack 1

設定

ネットワーク図

詳細フロー

1. クライアントがネットワークに接続し、AMP_Profile が割り当てられます。ユーザは Anyconnect のプロビジョニング ポータルにリダイレクトされます。 Anyconnect がマシンで検出されなかった場合、設定されたすべてのモジュール（VPN、AMP、ポスチャ）がインストールされます。 設定は、そのプロファイルとともに、各モジュールにプッシュされます。

2. Anyconnect がインストールされたら、ポスチャ アセスメントが実行されます。

3. AMP イネーブラ モジュールが FireAMP コネクタをインストールします。

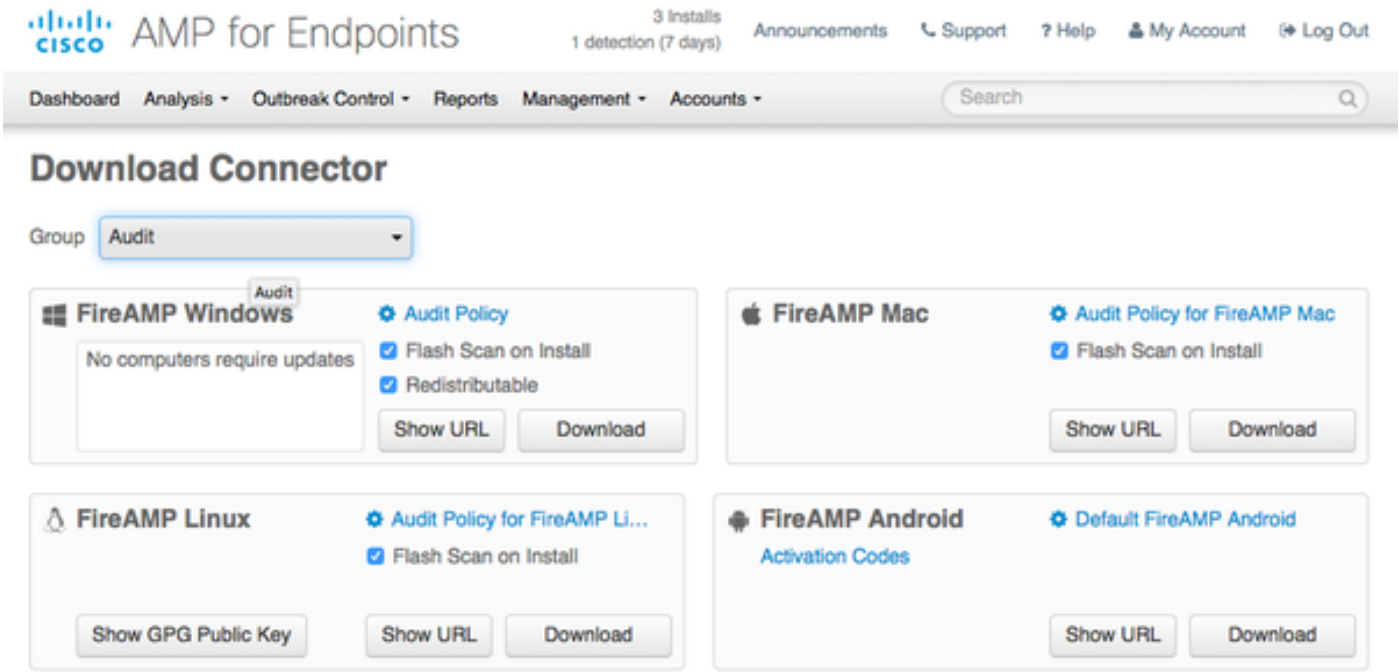
4. クライアントが悪意のあるソフトウェアをダウンロードしようとすると、AMP コネクタは警告メッセージを投じ、AMP クラウドにそれを報告します。

5. AMP クラウドは、ISE にこの情報を送信します。

AMP クラウドの設定

手順 1：AMP クラウドからコネクタをダウンロードする

コネクタをダウンロードするには、[Management] > [Download Connector] に移動します。 タイプを選択し、FireAMP (Windows、Android、Mac、Linux) をダウンロードします。 この場合、[Audit] が選択され、Windows 用の FireAMP のインストール ファイルがダウンロードされます。

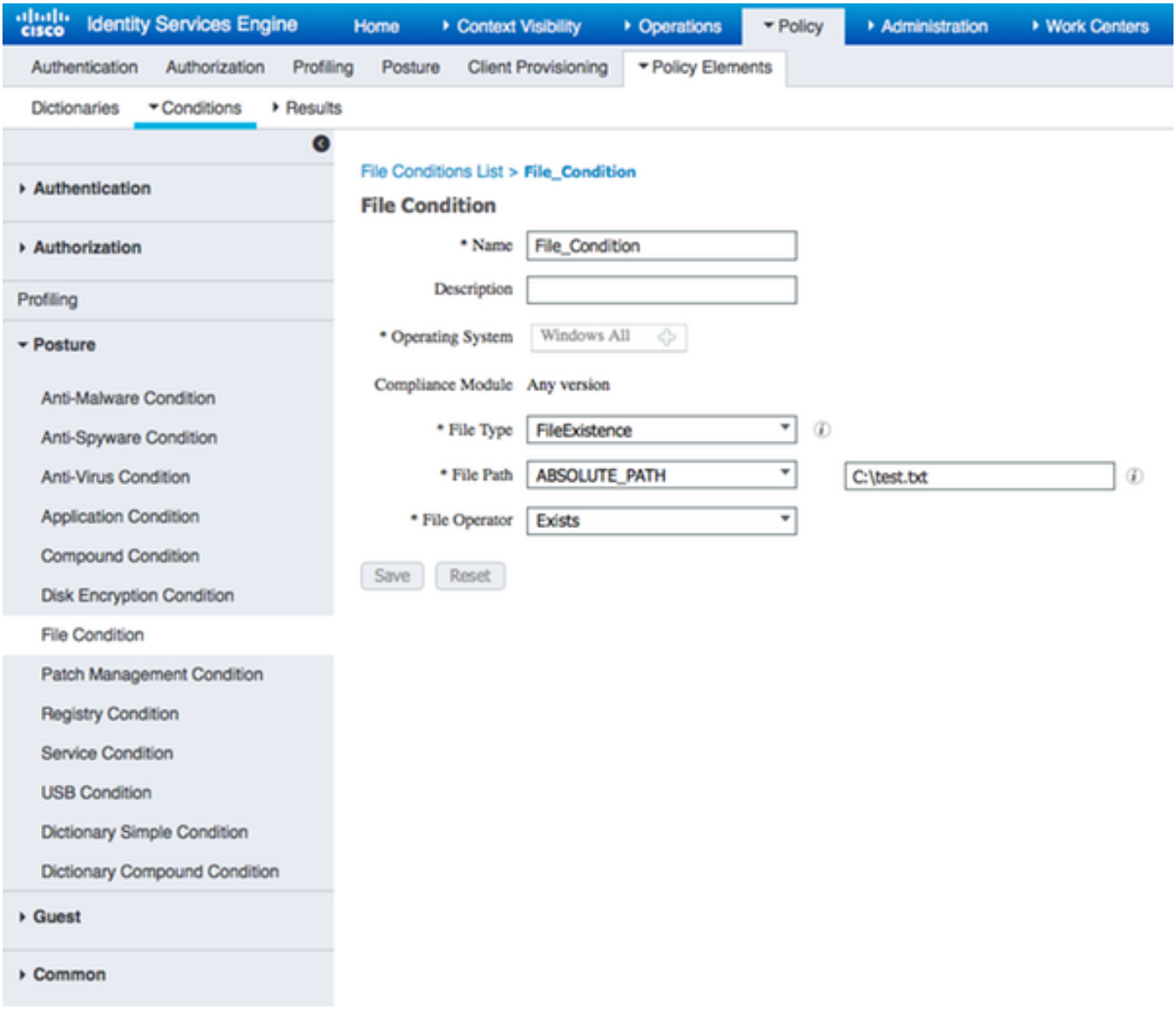


> **注:** このファイルをダウンロードすると、には、この例で **Audit_FireAMPSetup.exe** と呼ばれる .exe ファイルが生成されます。 このファイルは、ユーザが AMP の設定を依頼したときに使用できるように Web サーバに送られました。

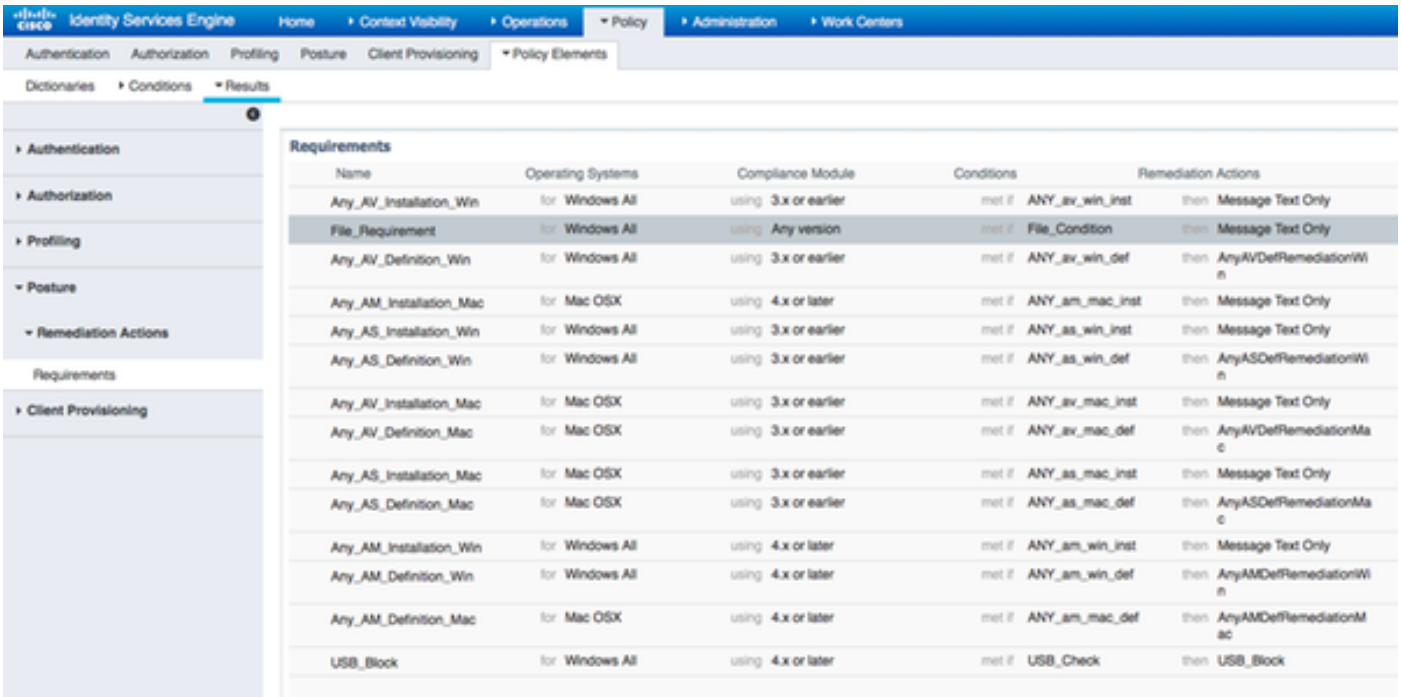
ISE の設定

手順 1：ポスチャ ポリシーと条件の設定

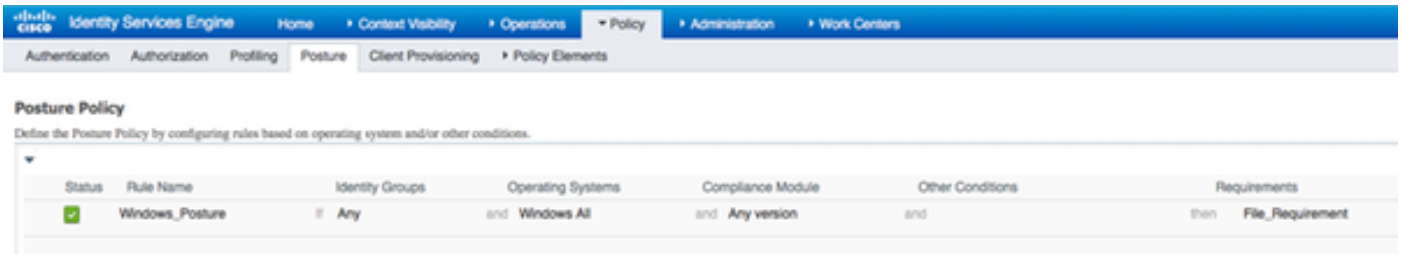
[Policy] > [Policy Elements] > [Conditions] > [Posture] > [File Condition] に移動します。ファイルの存在に関するシンプルな条件が作成されたことがわかります。 エンドポイントがポスチャ モジュールによって検証済みのポリシーに準拠する場合、ファイルは存在しなければなりません。



この条件は要件に使用されます。

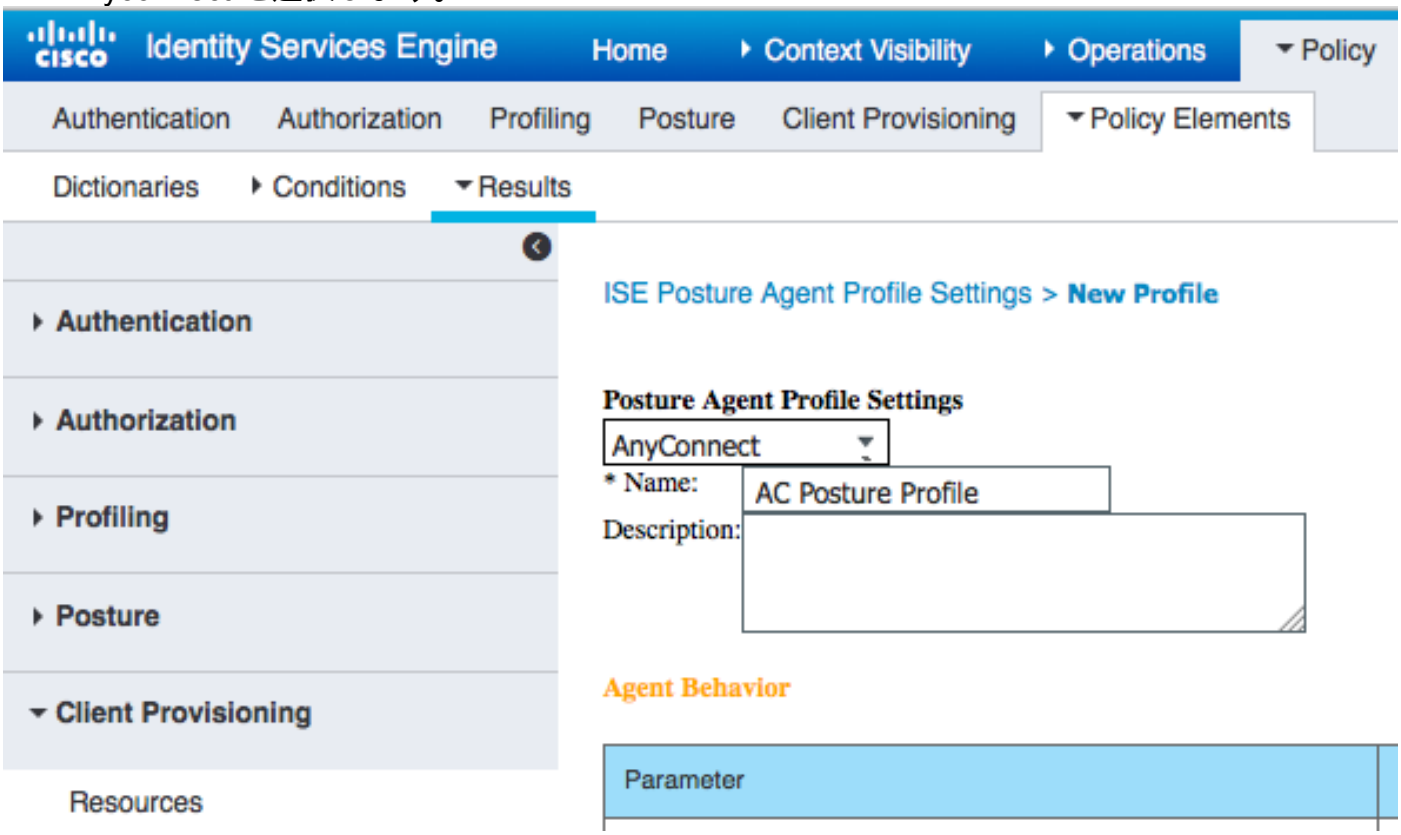


要件は、Microsoft Windows システムのポスチャ ポリシーで使用されます。

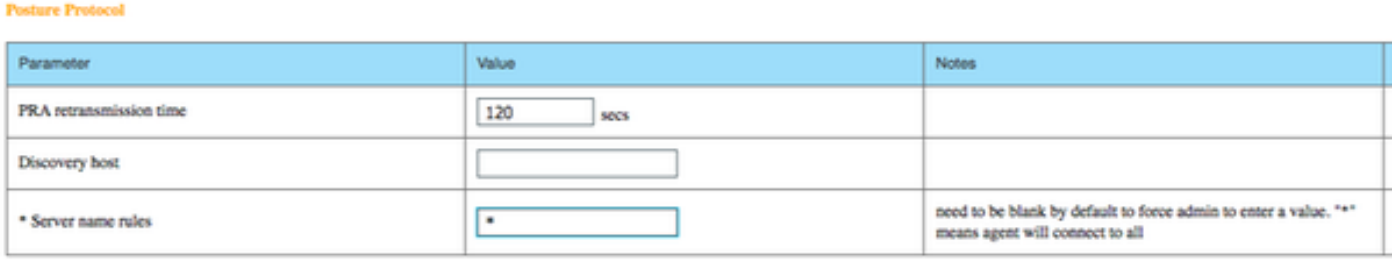


手順 2：ポスチャ プロファイルの設定

- [Policy] > [Policy Elements] > [Results] > [Client Provisioning] > [Resources] に移動し、ネットワーク アドミッション コントロール（NAC）エージェントまたは AnyConnect エージェント ポスチャ プロファイルを追加します。
- Anyconnect を選択します。



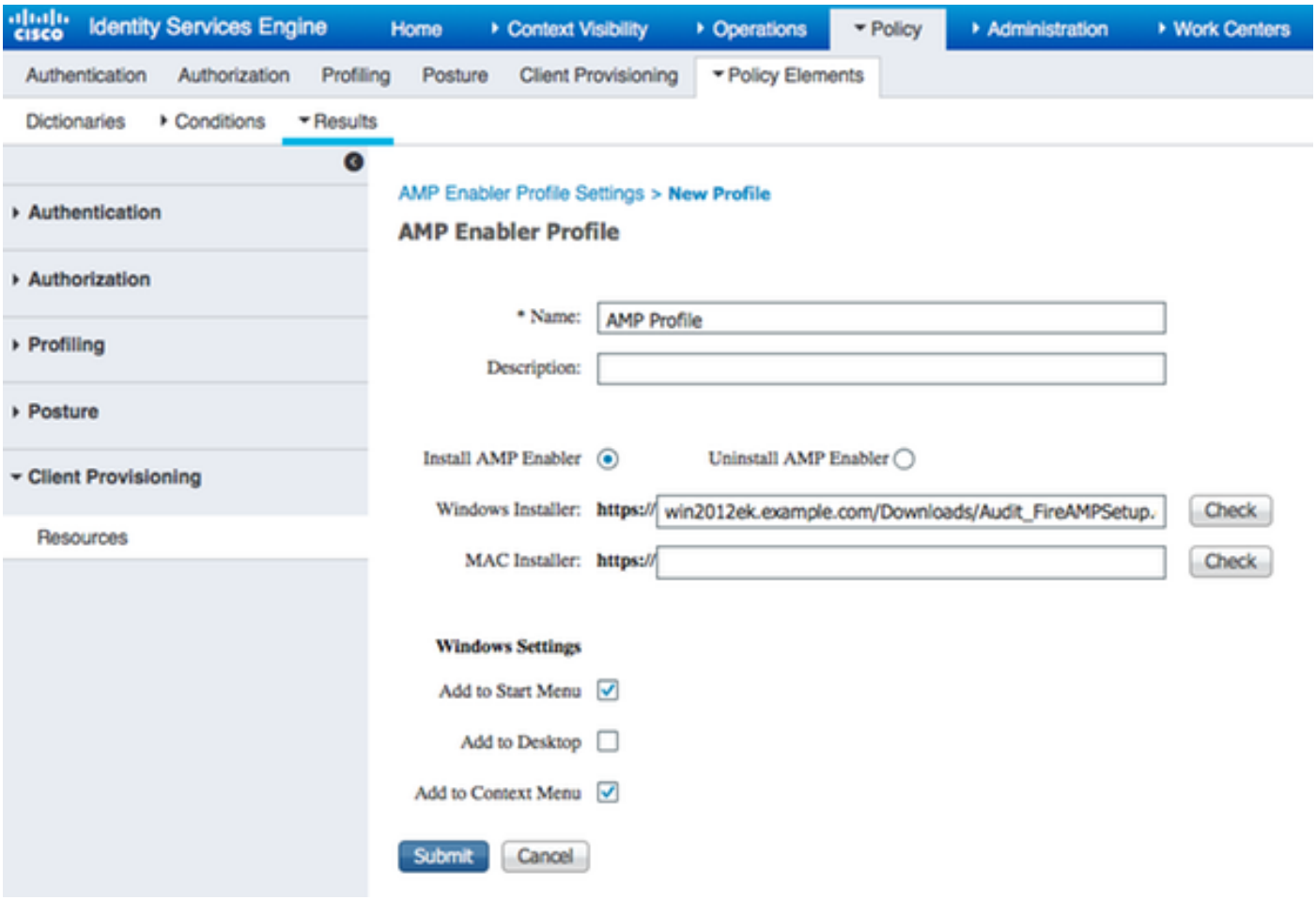
- [Posture Protocol] セクションから * を追加し、エージェントがすべてのサーバに接続できるようにします。



手順 3：AMP プロファイルの設定

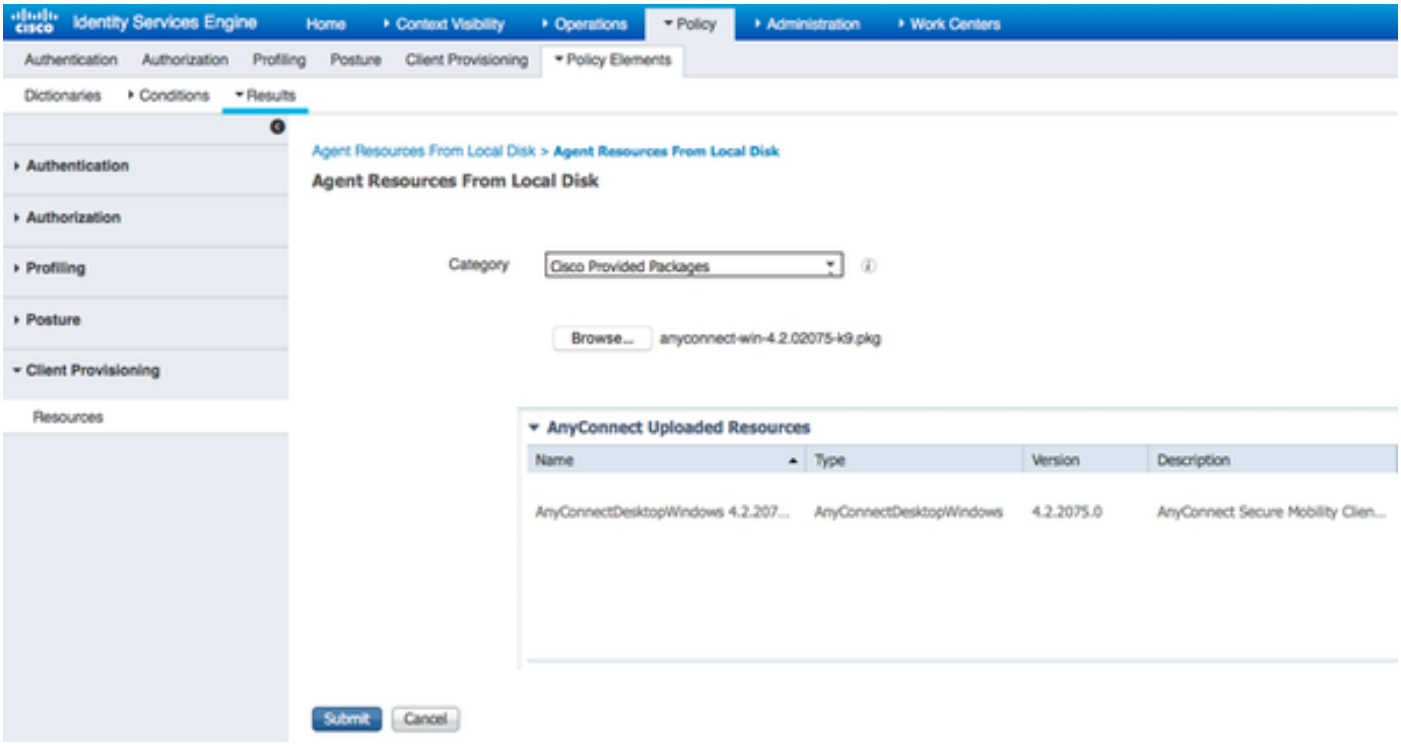
AMP プロファイルには、Windows インストーラが配置された場所の情報が含まれます。

Windows インストーラ、AMP クラウドから前もってダウンロードされています。 クライアント マシンからアクセスできるはずです。 インストーラが配置された場所にある HTTPS サーバの証明書も、クライアント マシンによって信頼されます。

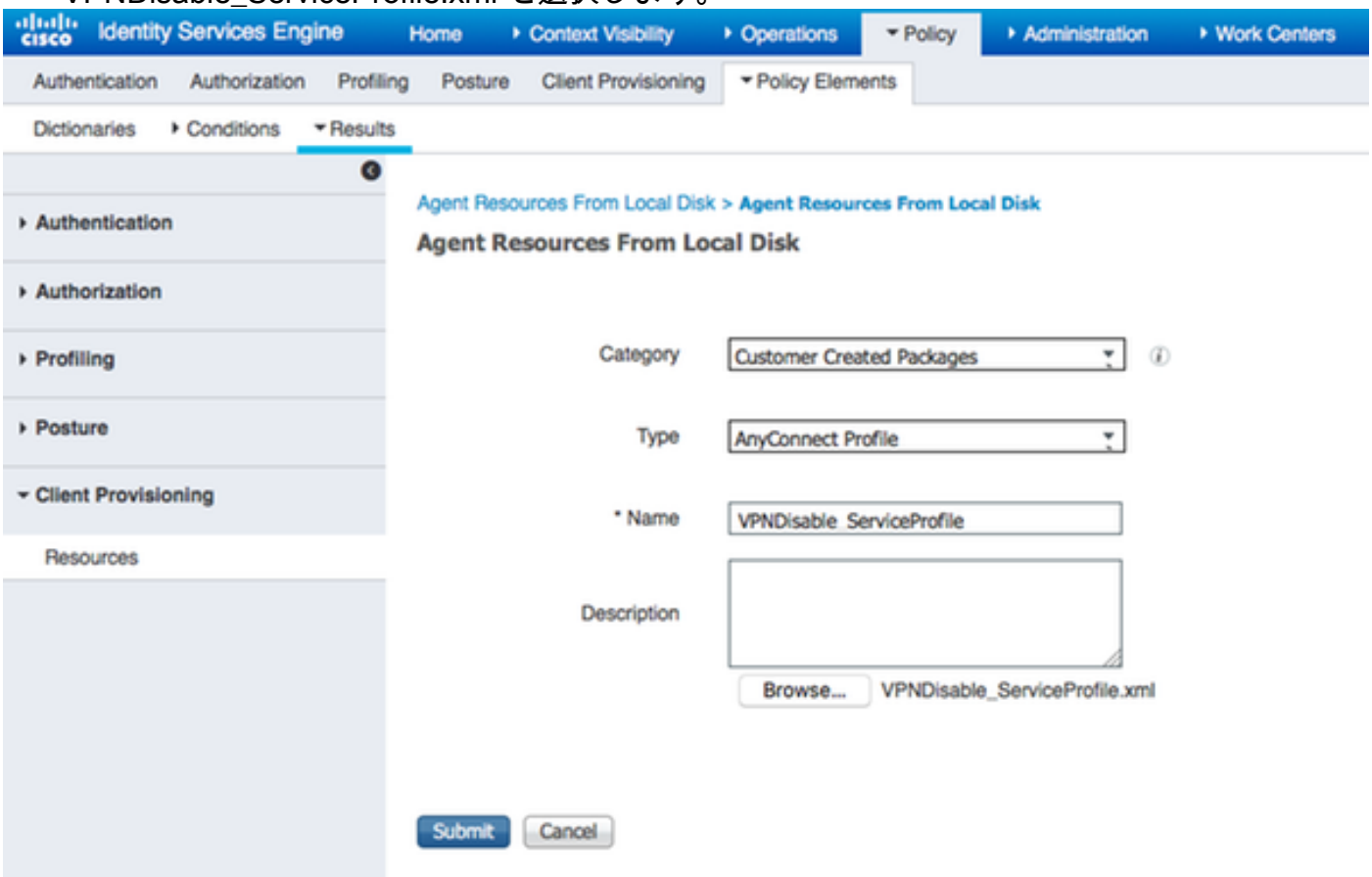


手順 2：ISE にアプリケーションと XML プロファイルをアップロードする

- Cisco のオフィシャル サイトからアプリケーションを手動でダウンロードします。 **anyconnect-win-4.2.02075-k9.pkg**
- ISE で、[Policy] > [Policy Elements] > [Results] > [Client Provisioning] > [Resources] に移動し、[Agent Resources From Local Disk] を追加します。
- [Cisco Provided Packages] を選択し、anyconnect-win-4.2.02075-k9.pkg を選択します。



- [Policy] > [Policy Elements] > [Results] > [Client Provisioning] > [Resources] に移動し、[Agent Resources From Local Disk] を追加します。
- [Customer Created Packages] を選択し、AnyConnect Profile と入力します。VPNDisable_ServiceProfile.xml を選択します。

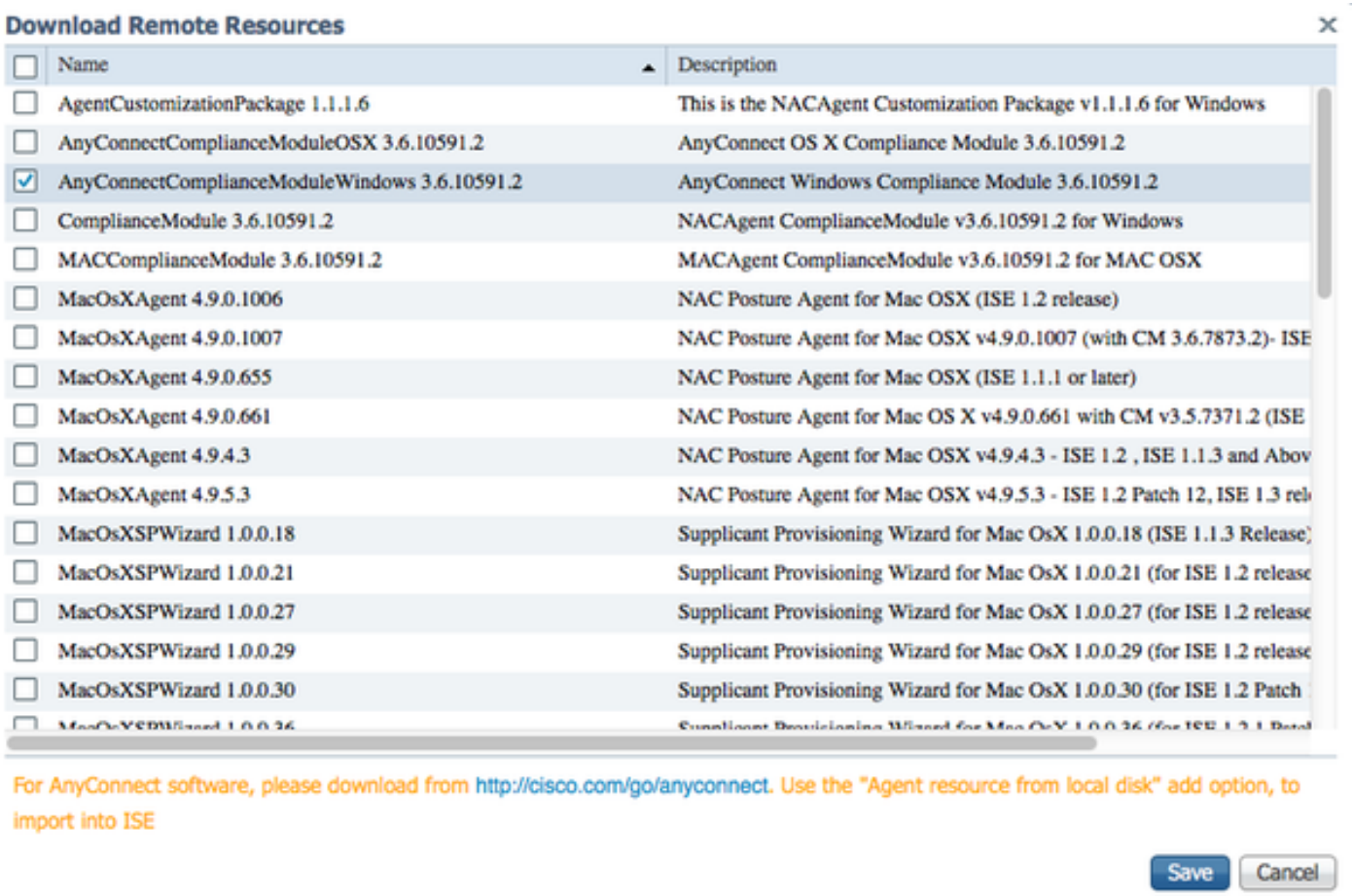


注: VPNDisable_ServiceProfile.xml は、VPN のタイトルを非表示にするために使用されます（この例では VPN モジュールを使用しないため）。 VPNDisable_ServiceProfile.xml の内容は次のとおりです。

```
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/" xmlns:
xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:
schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
 <ClientInitialization>
 <ServiceDisable>true</ServiceDisable>
 </ClientInitialization>
</AnyConnectProfile>
```

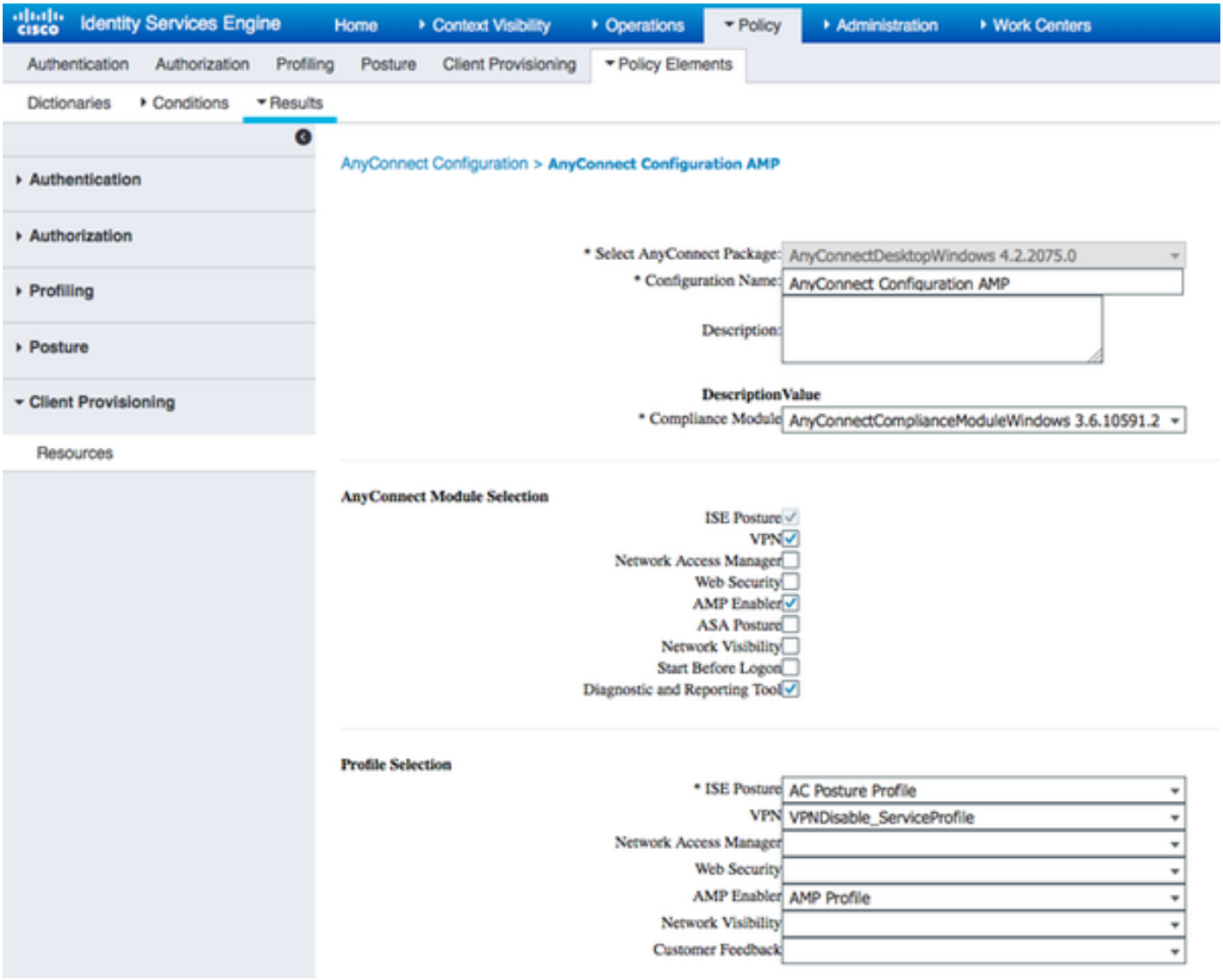
手順 3：AnyConnect コンプライアンス モジュールをダウンロードする

- [Policy] > [Policy Elements] > [Results] > [Client Provisioning] > [Resources] に移動し、[Agent Resources from Cisco site] を追加します。
- [AnyConnect Windows Compliance Module 3.6.10591.2] を選択し、[Save] をクリックします。



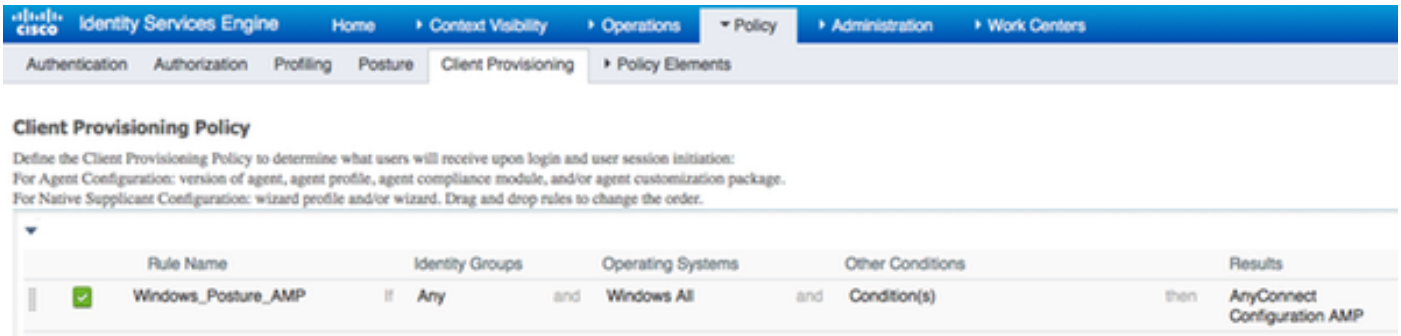
手順 4：AnyConnect 設定の追加

- [Policy] > [Policy Elements] > [Results] > [Client Provisioning] > [Resources] に移動し、[AnyConnect Configuration] を追加します。
- 名前を設定し、コンプライアンス モジュールおよび AnyConnect のすべての必須モジュール（VPN、AMP、ポスチャ）を選択します。
- [Profile Selection] で、各モジュール用に先ほど設定したプロファイルを選択します。



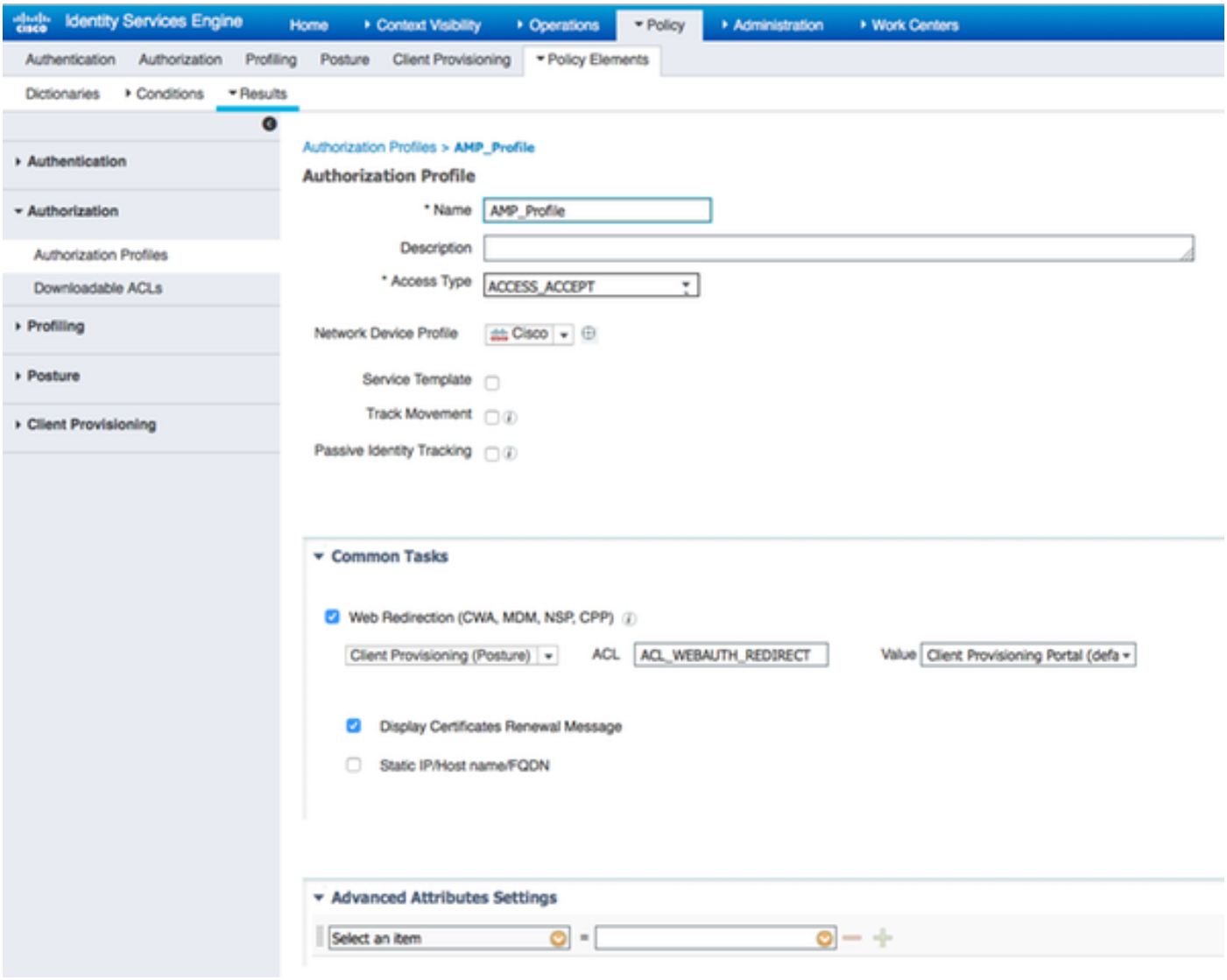
手順 5：クライアント プロビジョニング ルールの設定

先ほど作成した AnyConnect 設定は、クライアント プロビジョニング ルールで参照されます。

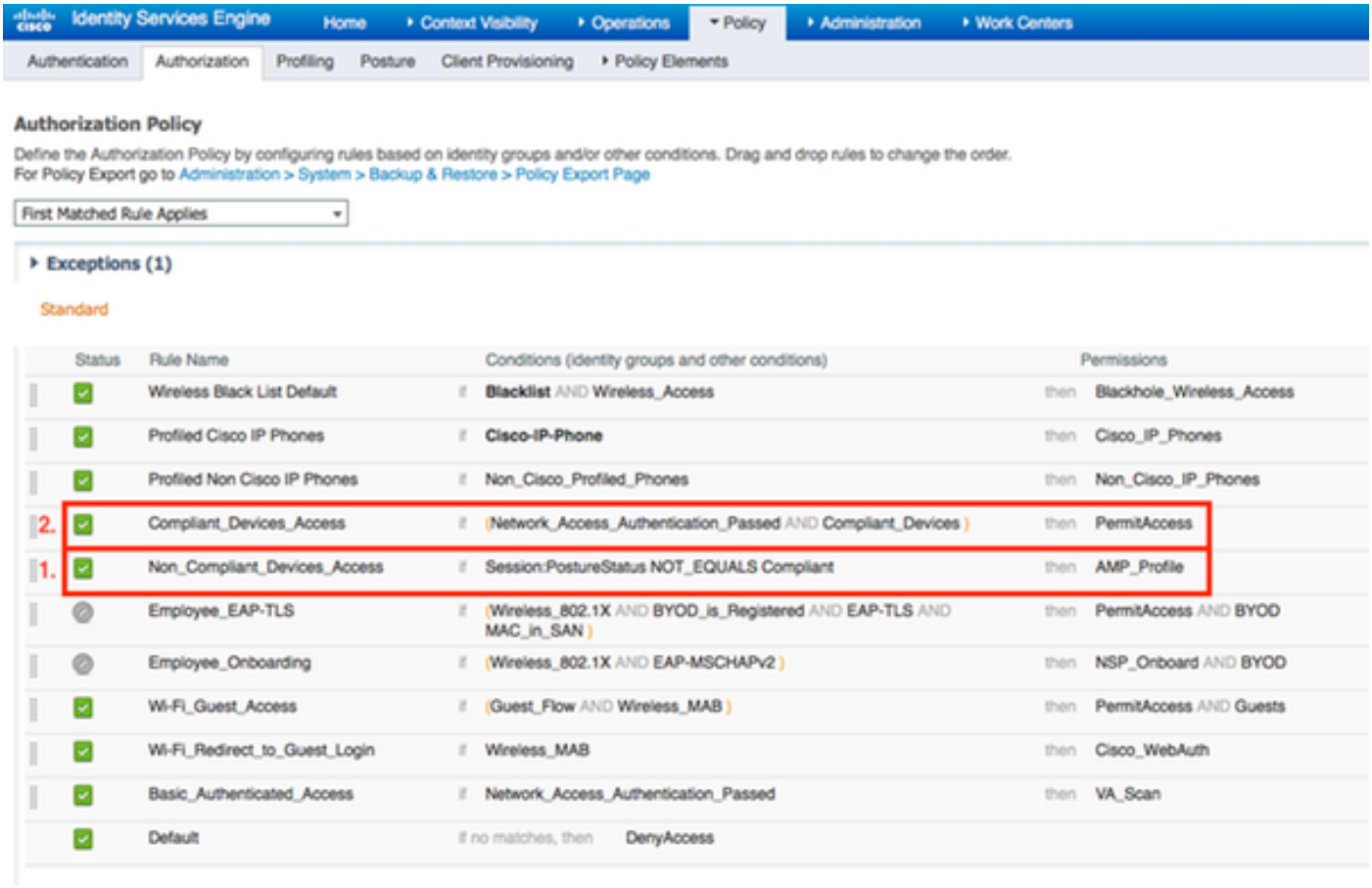


手順 6：許可ポリシーの設定

最初にクライアント プロビジョニング ポータルへのリダイレクトが行われます。 ポスチャの標準認可ポリシーが使用されます。

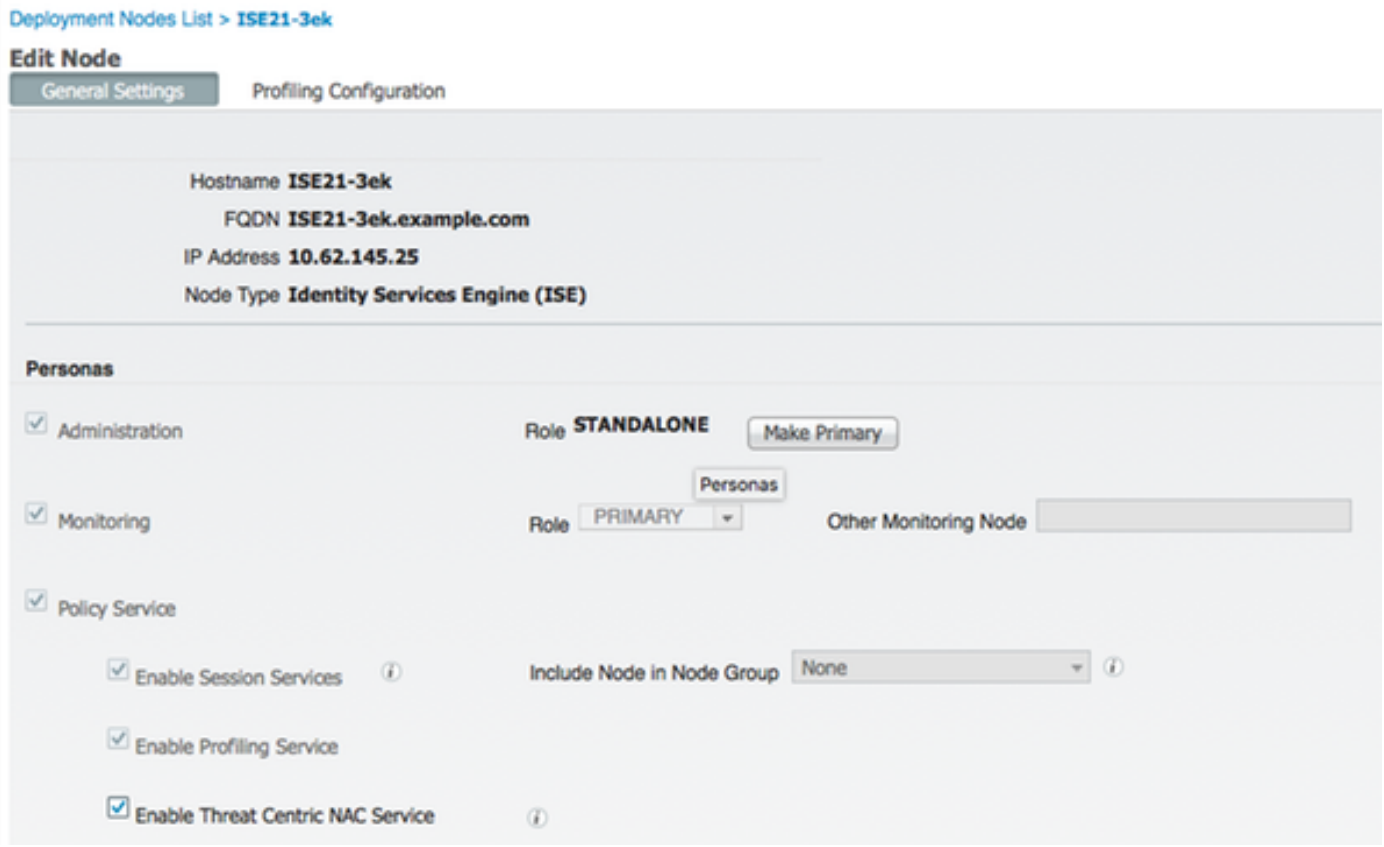


その後、[Compliant] になると、フル アクセスが指定されます。



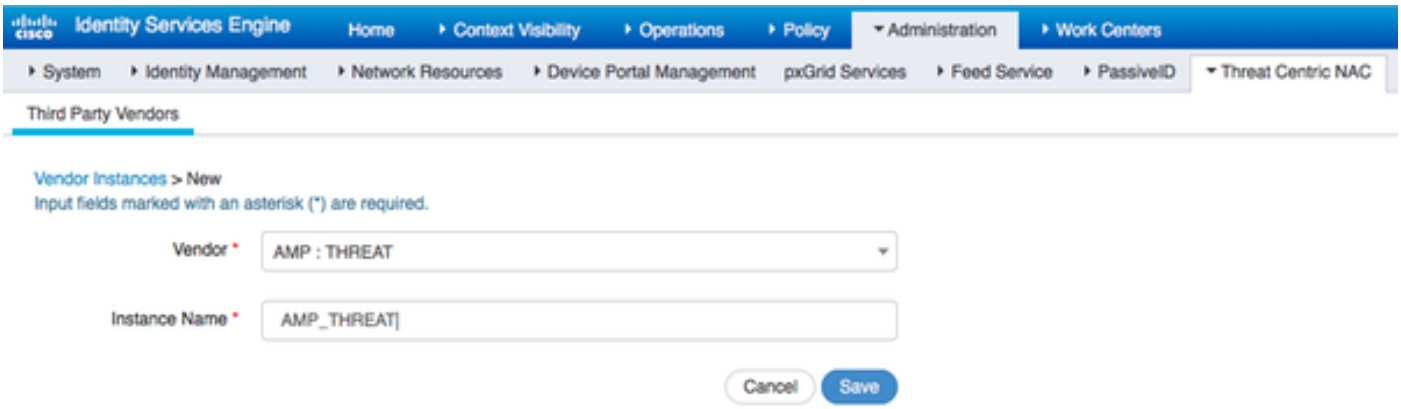
手順 7：TC-NAC サービスの有効化

[Administration] > [Deployment] > [Edit Node] で、TC-NAC サービスを有効化します。 [Enable Threat Centric NAC Service] チェックボックスを選択します。

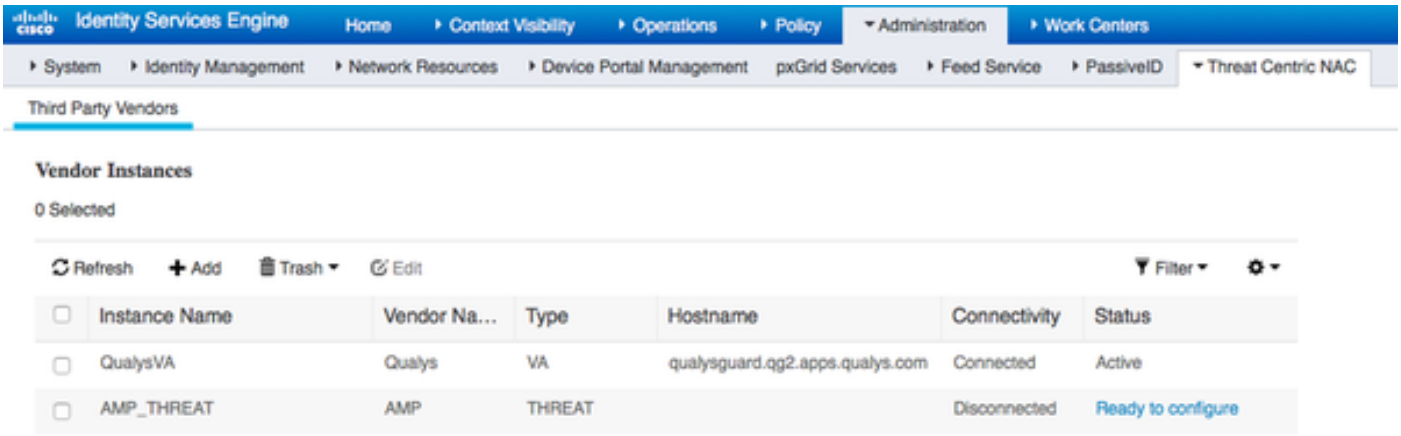


手順 8：AMP アダプタの設定

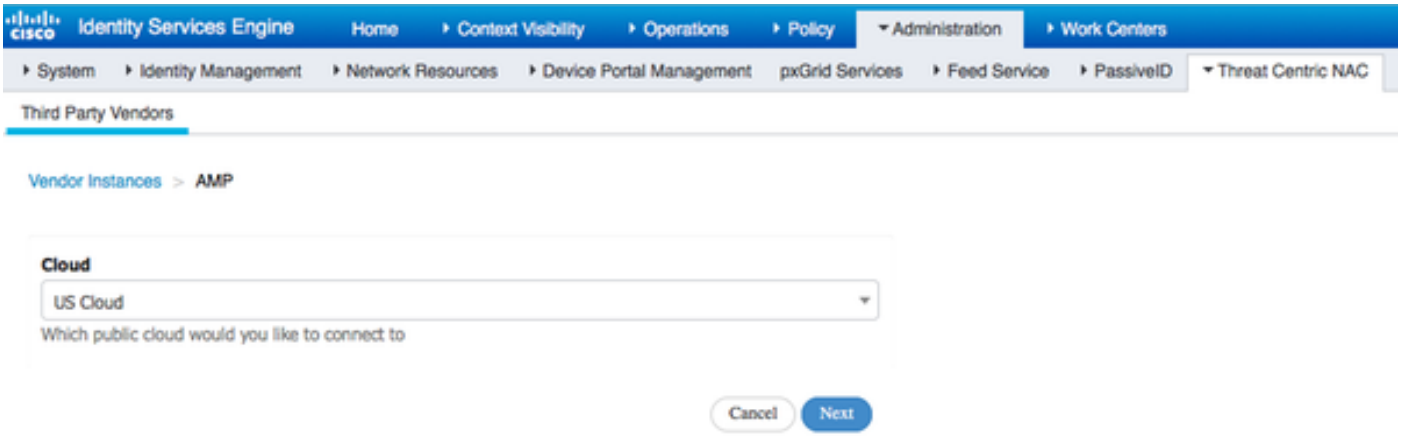
[Administration] > [Threat Centric NAC] > [Third Party Vendors] > [Add] の順に移動します。[Save] をクリックします。



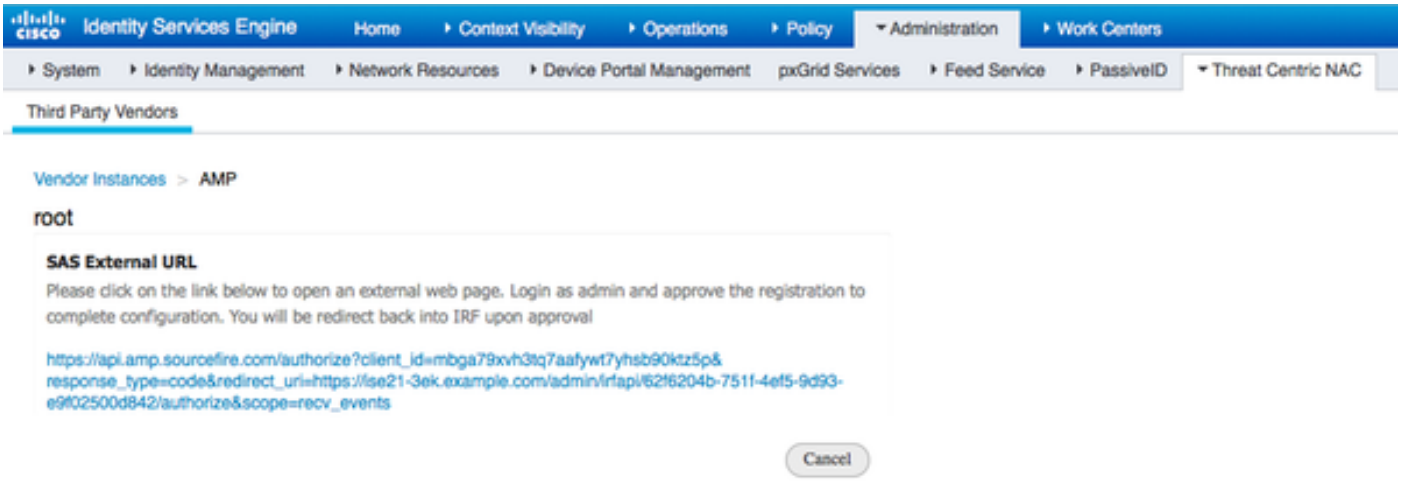
[Ready to Configure] 状態に移行するはずです。 [Ready to Configure] をクリックします。



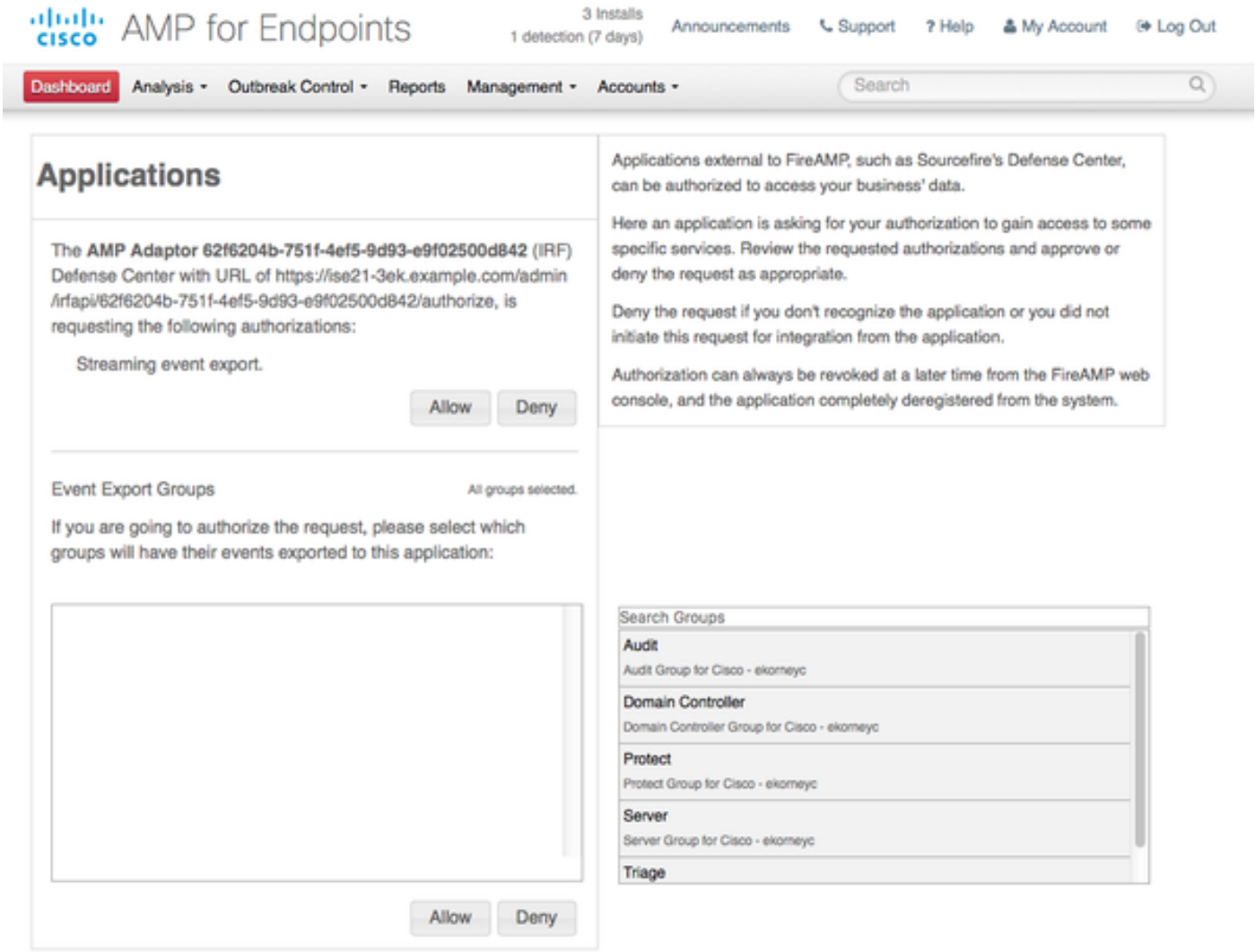
[Cloud] を選択し、[Next] をクリックします。



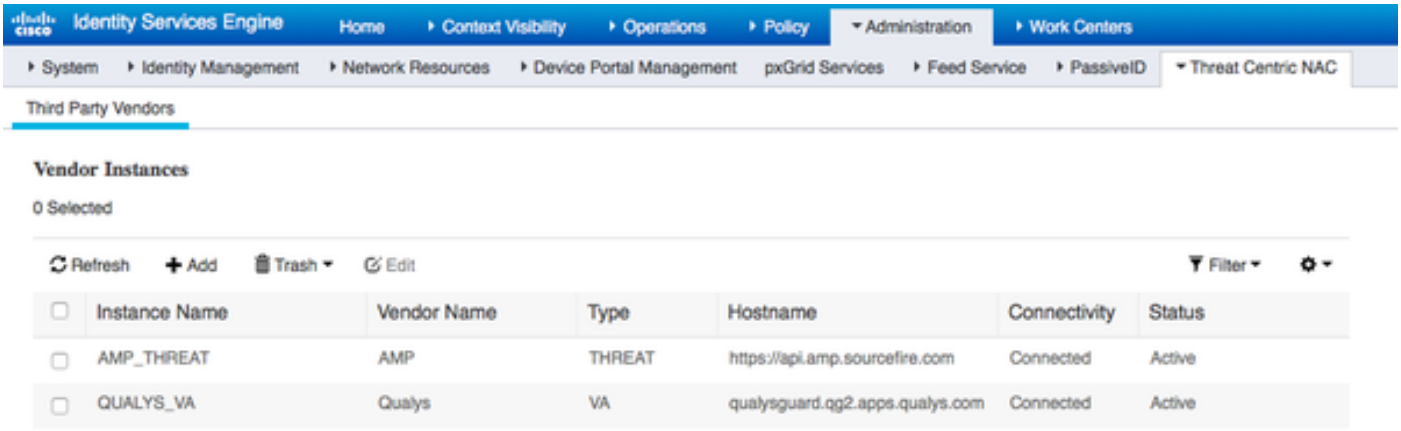
FireAMP のリンクをクリックして、admin ユーザとして FireAMP にログインします。



[Applications] パネルで [Allow] をクリックし、Streaming Event Export 要求を認可します。 このアクションが終わると、Cisco ISE へリダイレクトされます。



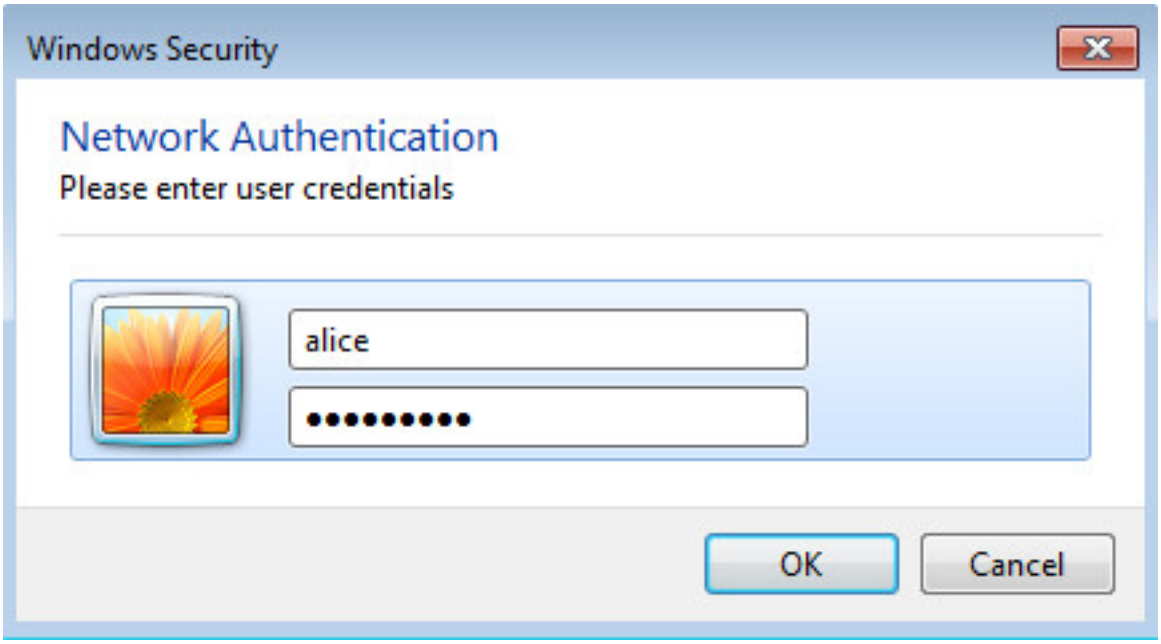
モニタするイベント (疑わしいダウンロード、疑わしいドメインへの接続、実行されたマルウェア、Java のセキュリティ侵害など) を選択します。 アダプタ インスタンス設定の概要が、設定概要ページに表示されます。 アダプタ インスタンスが [Connected/Active] 状態に移行します。



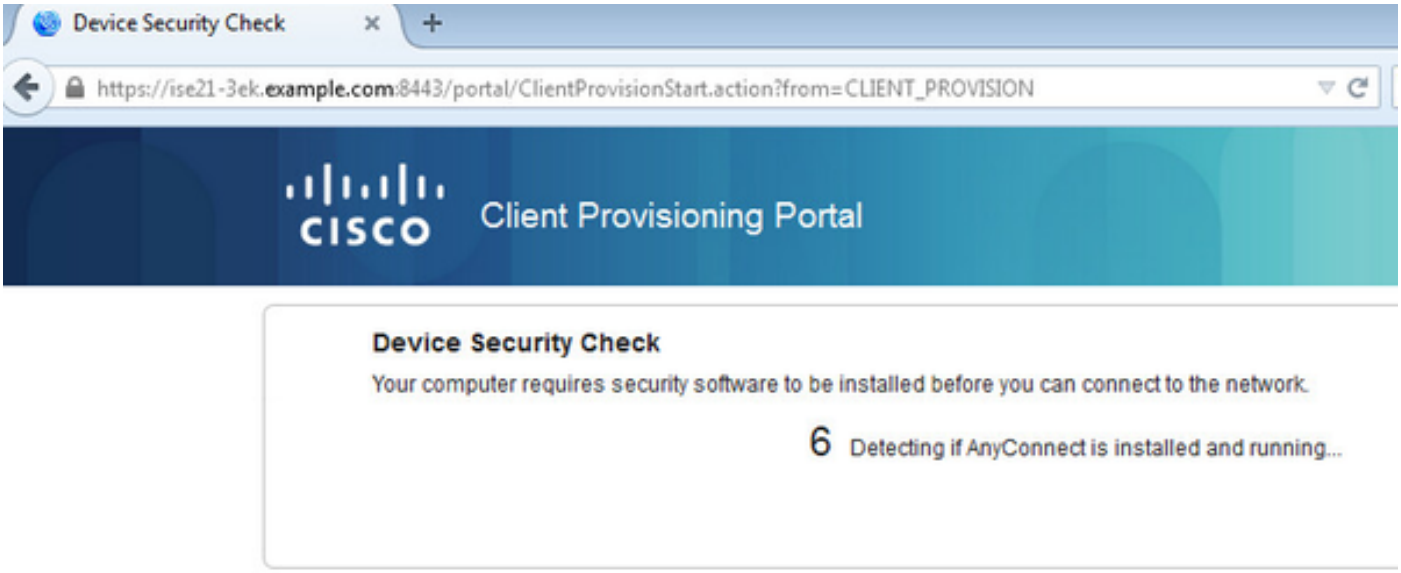
確認

Endpoint

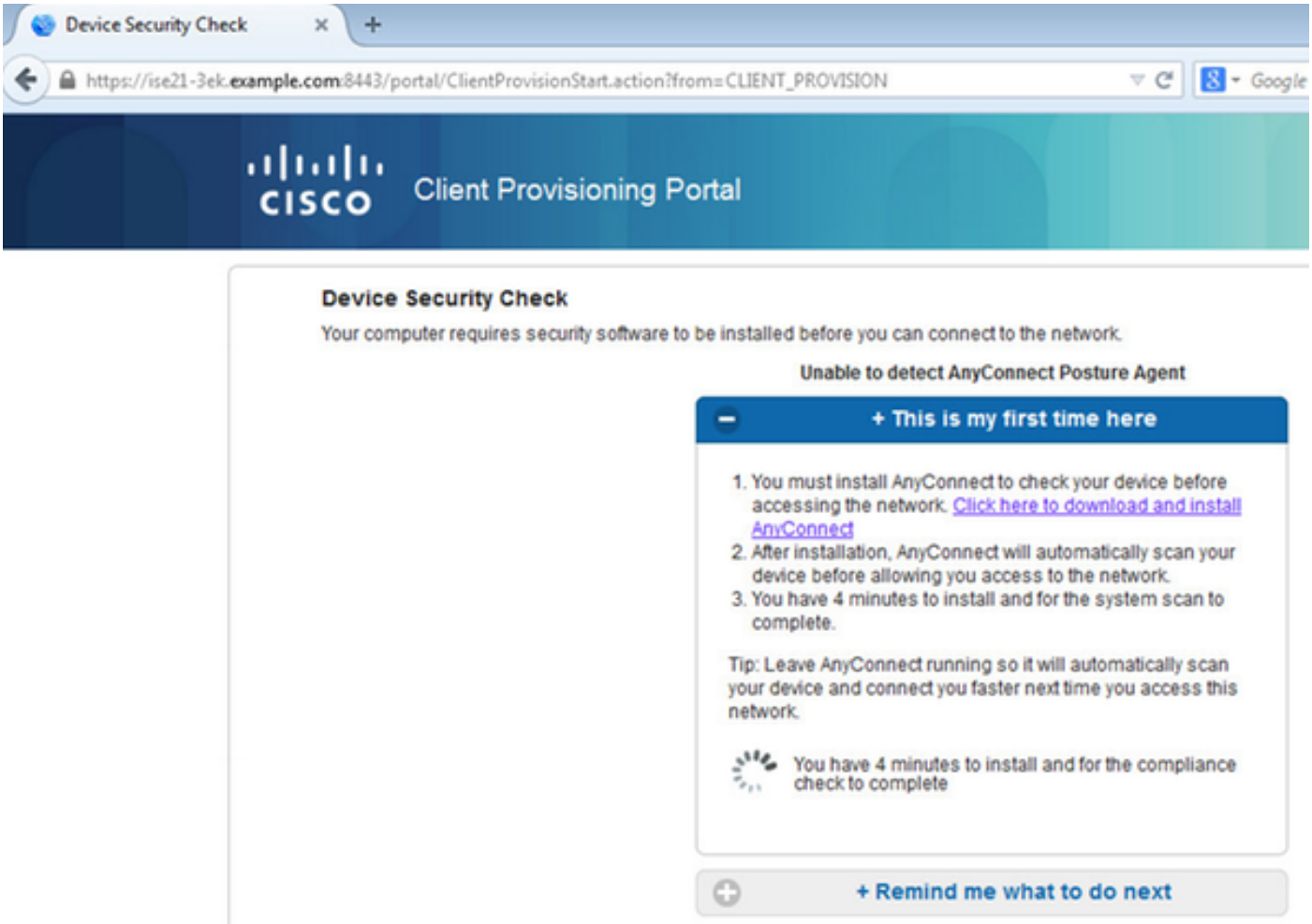
PEAP（MSCHAPv2）経由でワイヤレス ネットワークに接続します。



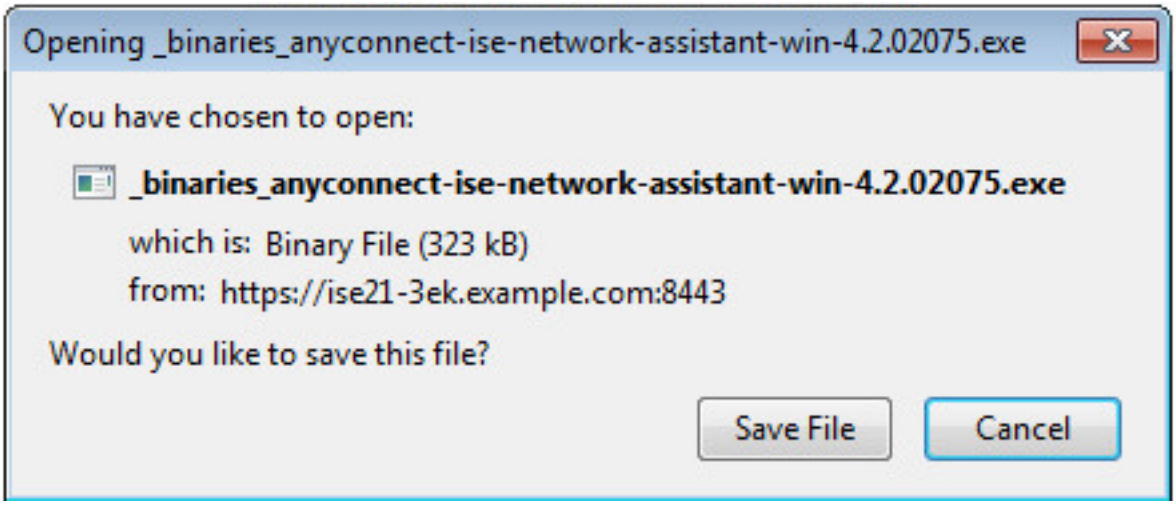
接続されると、クライアント プロビジョニング ポータルへのリダイレクトが行われます。



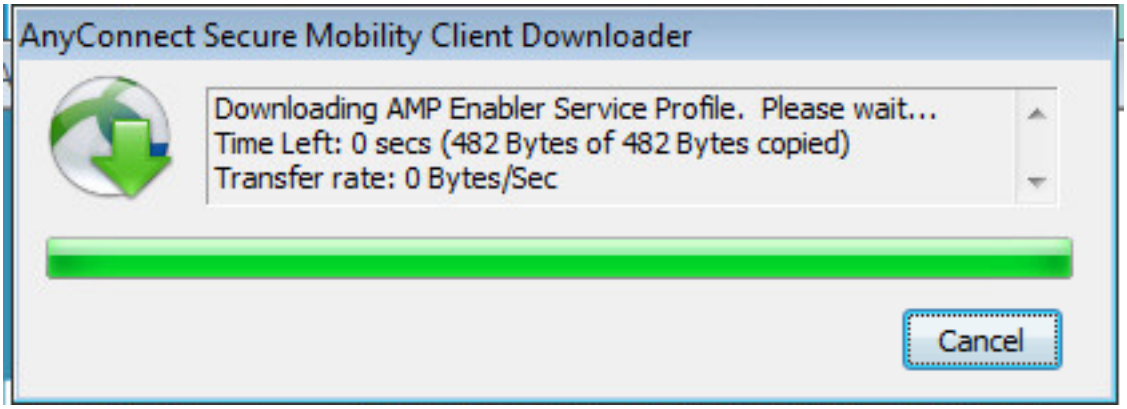
クライアント マシンに何もインストールされてないため、ISE が AnyConnect クライアントのインストールを求めます。

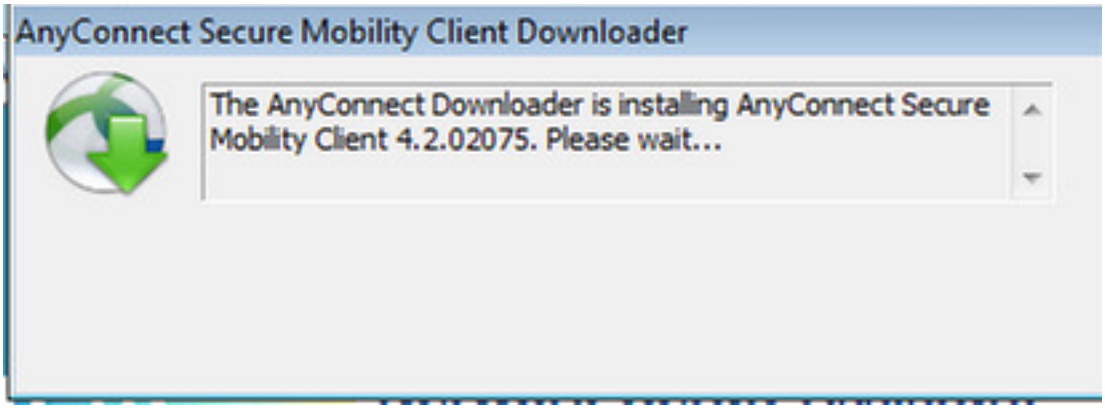


ネットワーク設定アシスタント（NSA）アプリケーションをダウンロードし、クライアント マシンから実行してください。

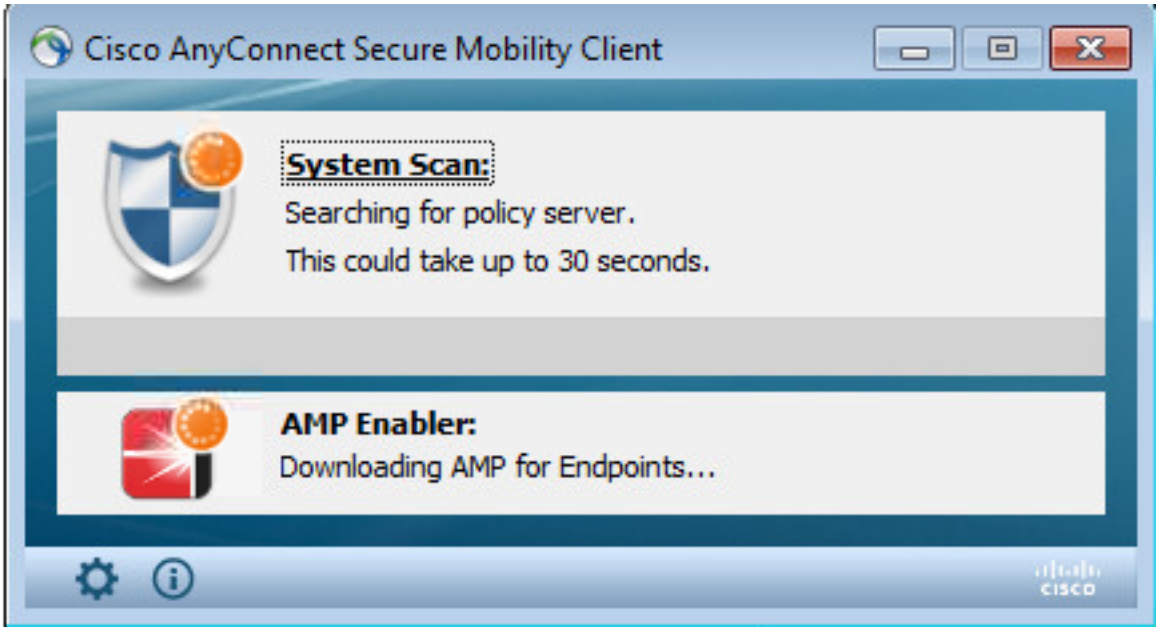


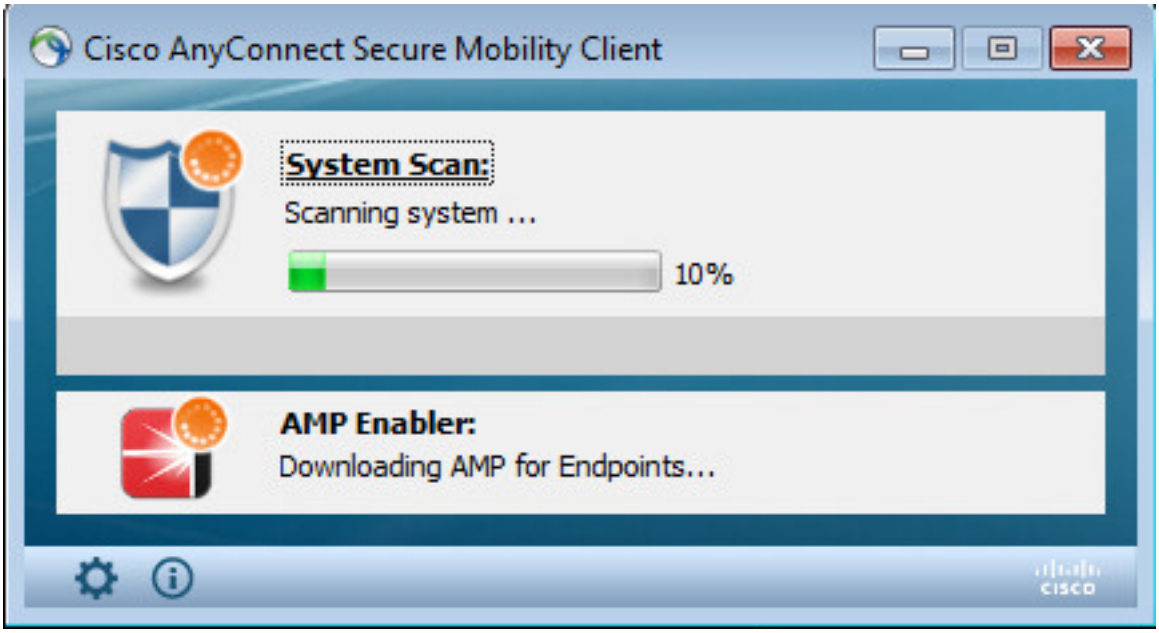
NSA が必要なコンポーネントとプロファイルのインストールを処理します。



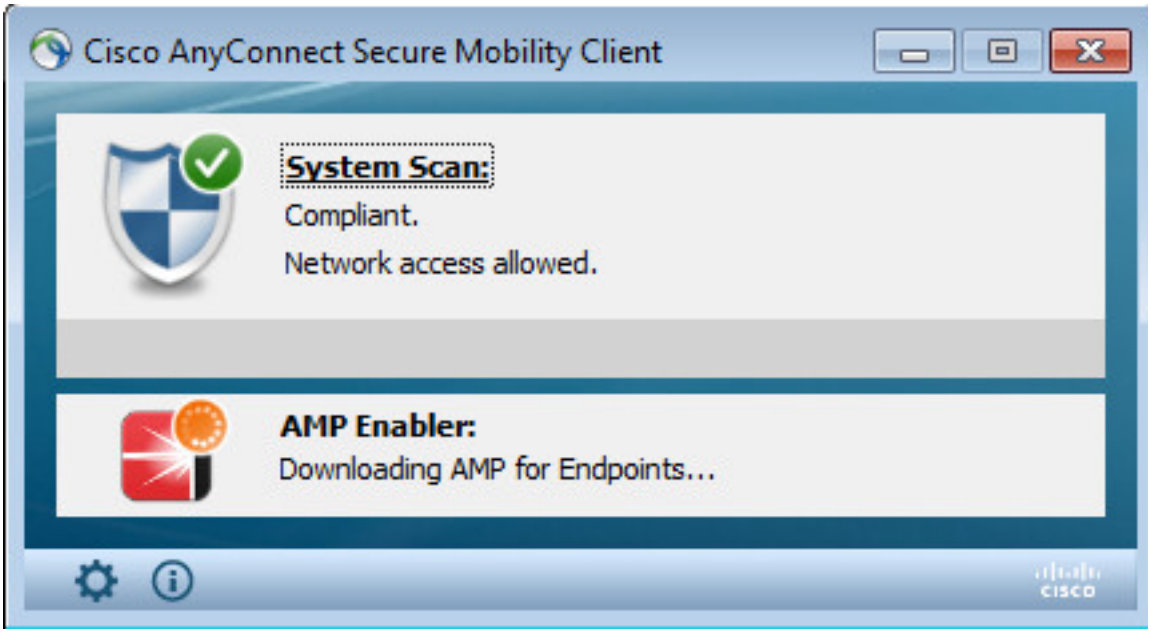


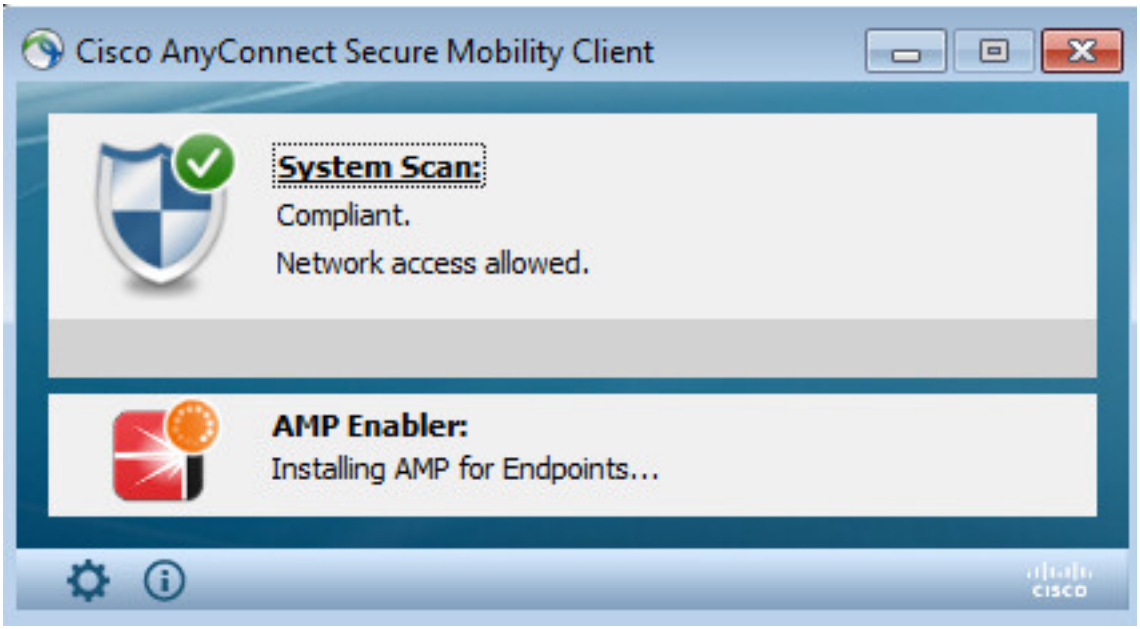
インストールが完了すると、AnyConnect ポスチャ モジュールがコンプライアンス チェックを行います。

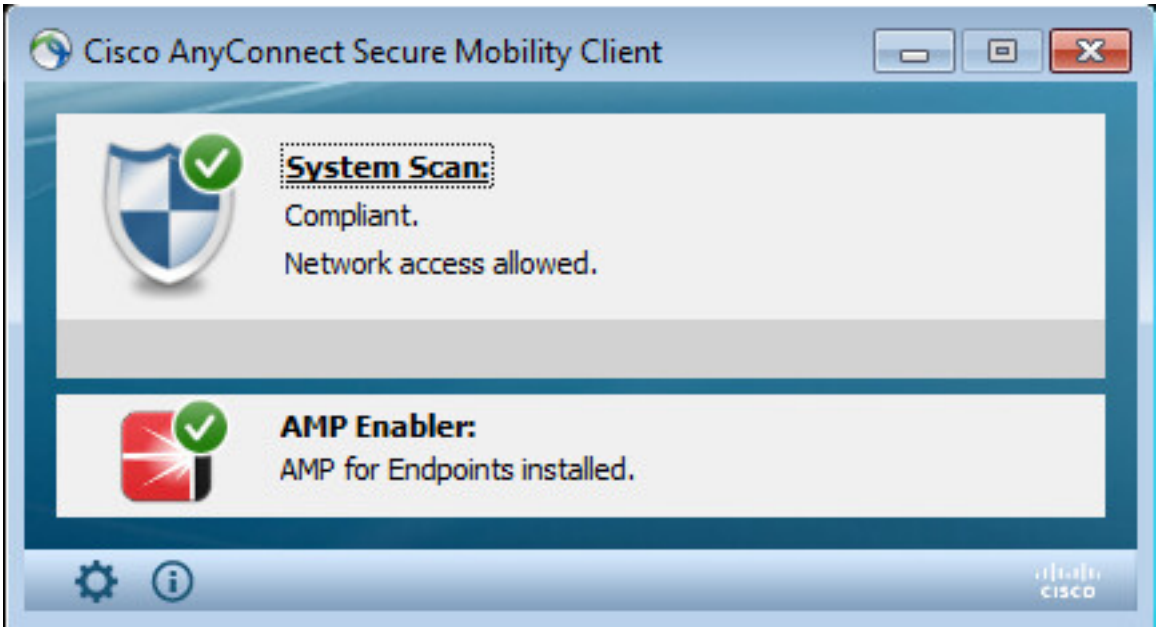




フル アクセスが与えられているため、エンドポイントが適合している場合、AMP プロファイルで先ほど指定した Web サーバから AMP がダウンロードされ、インストールされます。

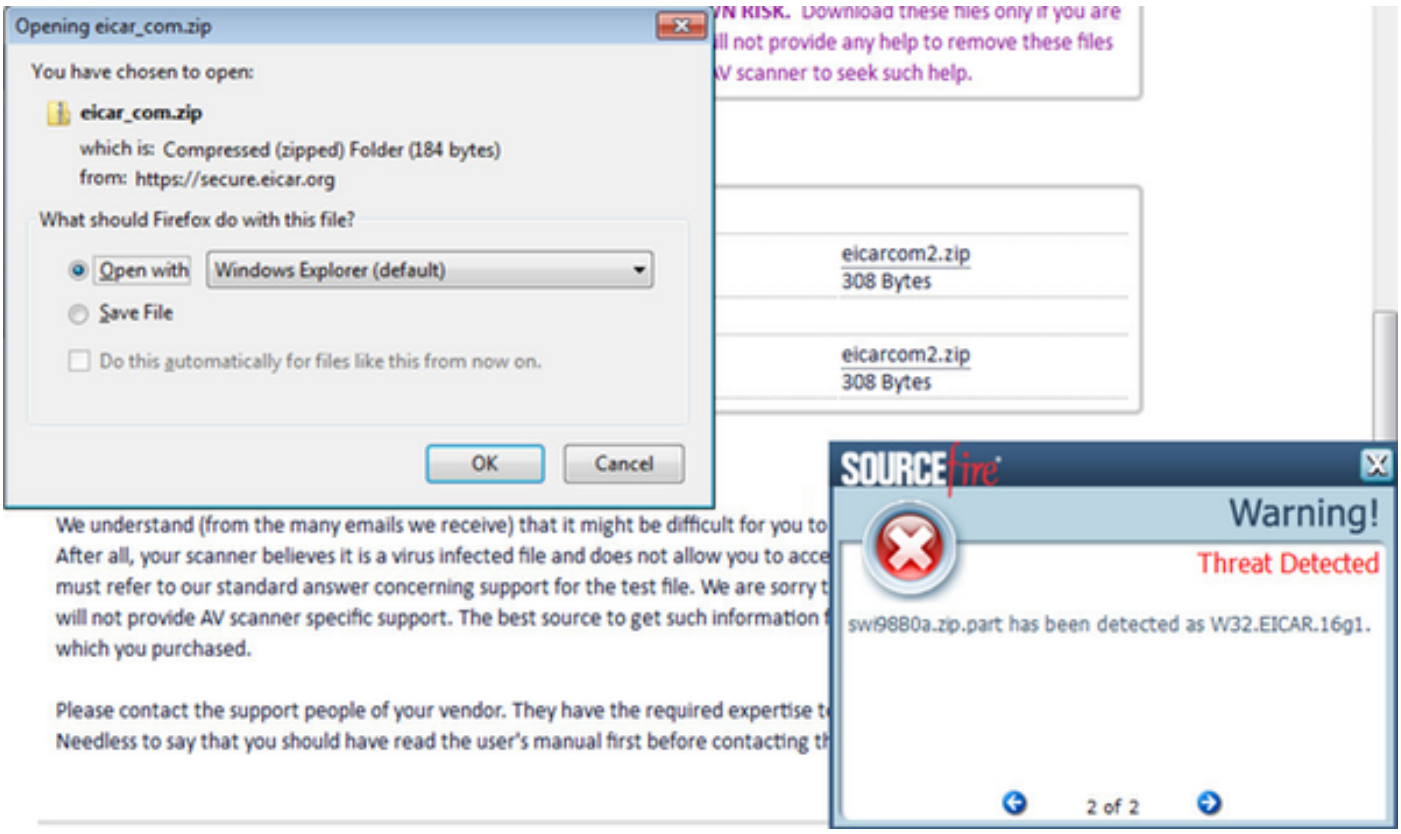






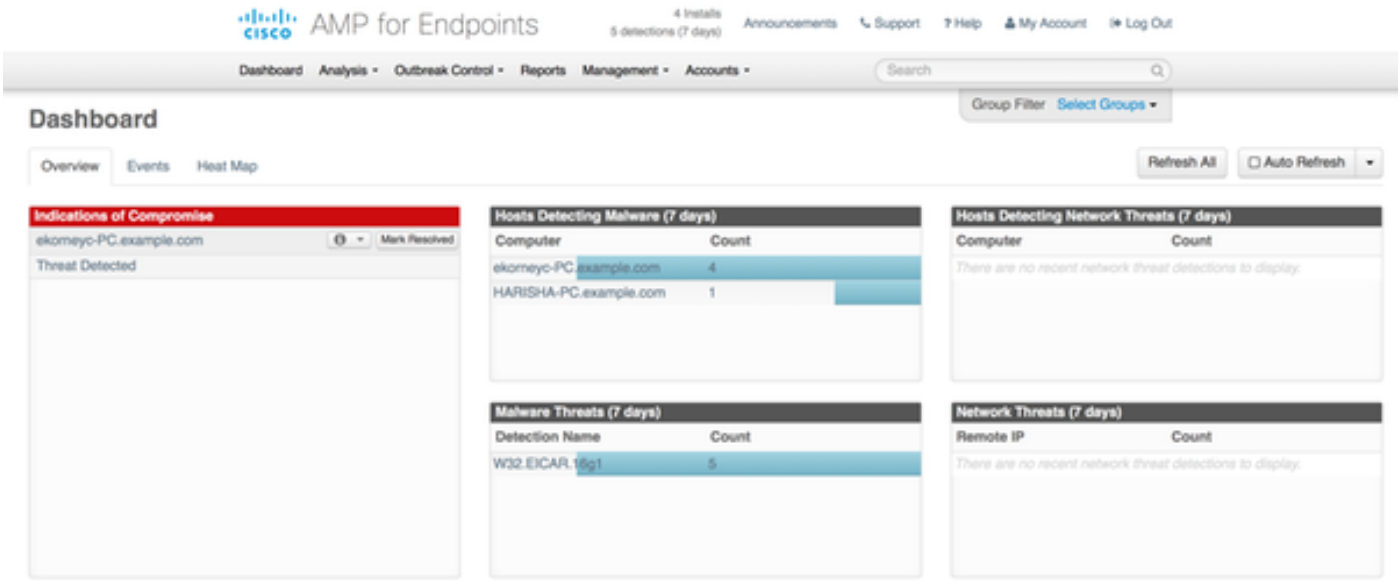
AMP コネクタが表示されます。

動作中の AMP をテストするため、ZIP ファイルに格納されている Eicar 文字列がダウンロードされます。 脅威が検出され、AMP クラウドに報告されます。

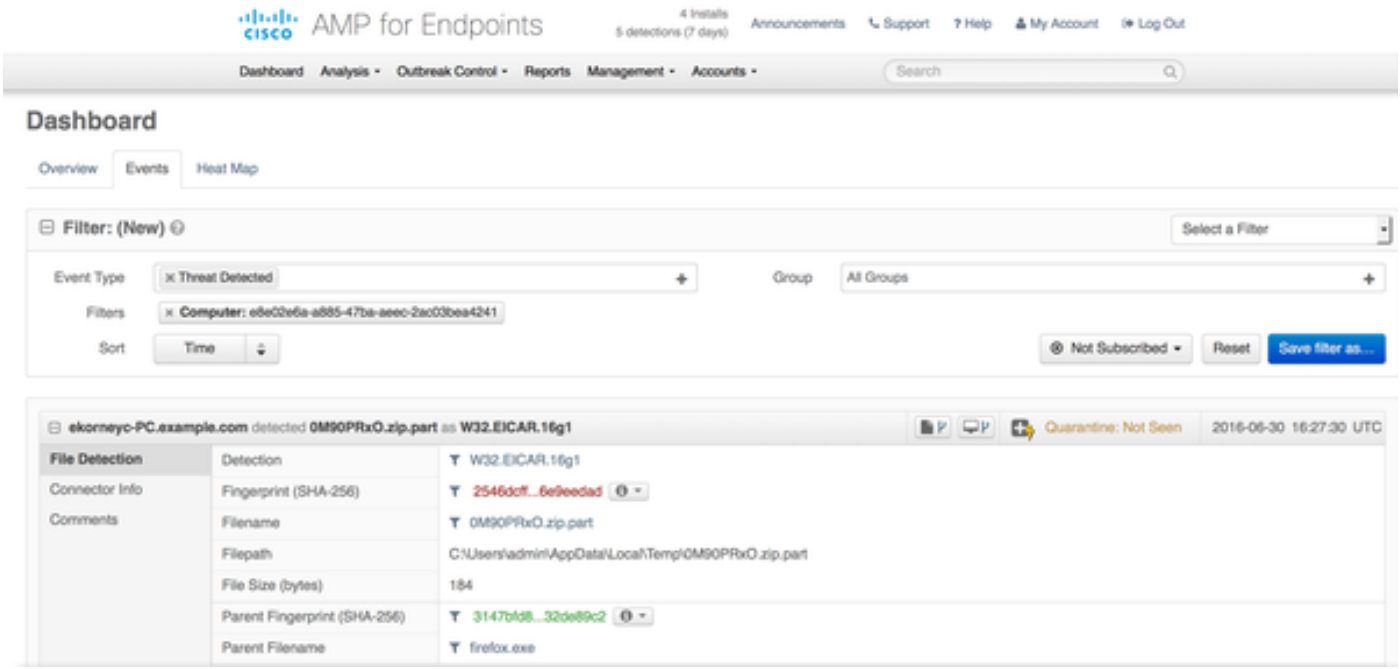


AMP クラウド

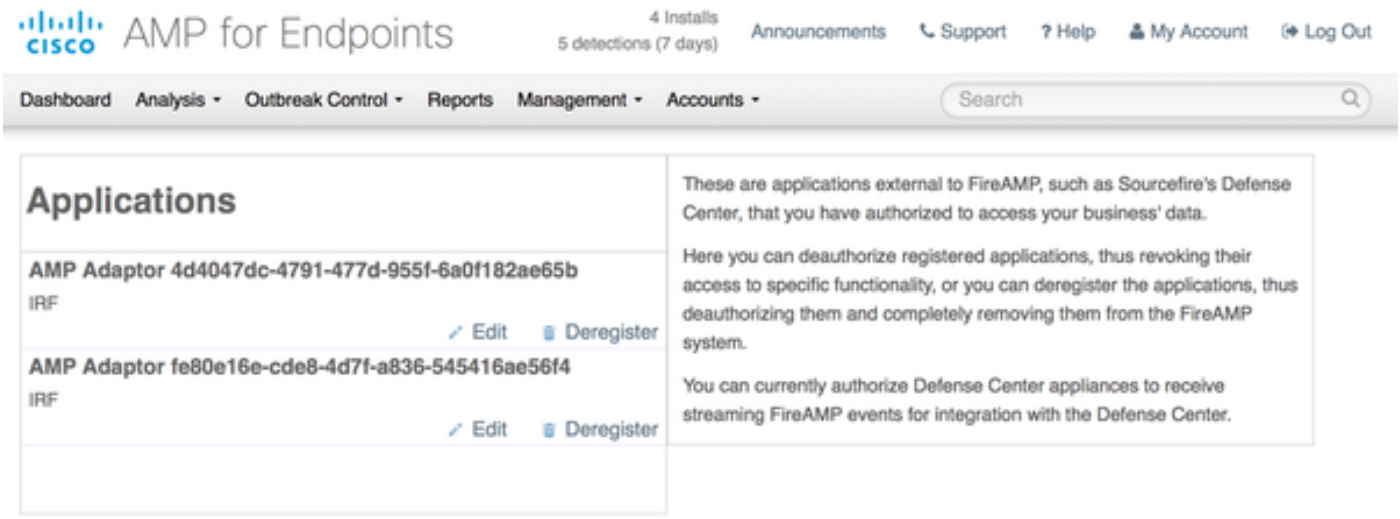
脅威の詳細を確認するには、AMP クラウドのダッシュボードを使用できます。



脅威、ファイルパスおよびフィンガープリントについての詳細を得るには、マルウェアが検出されたホストをクリックします。

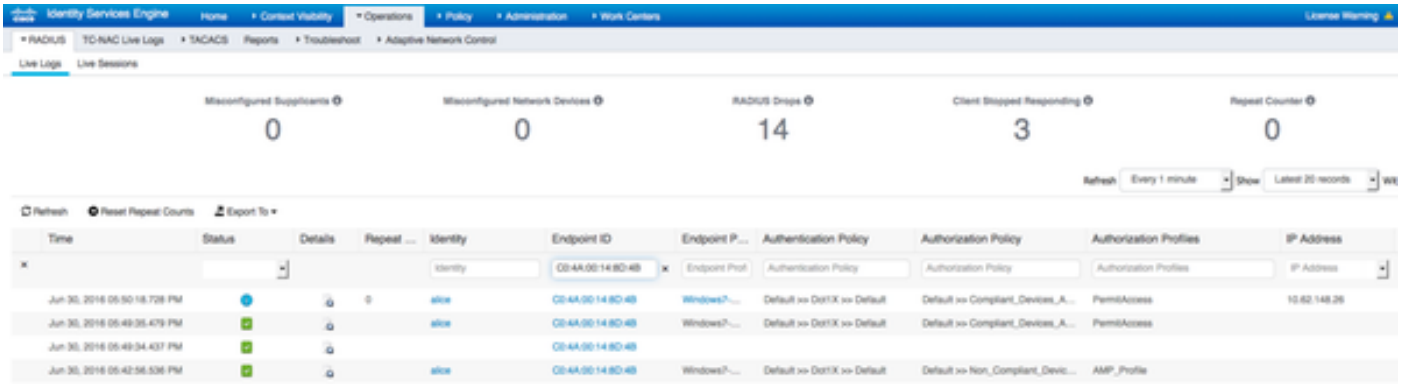


ISE のインスタンスを表示（View）または登録解除（Deregister）するには、[Accounts] > [Applications] に移動します。

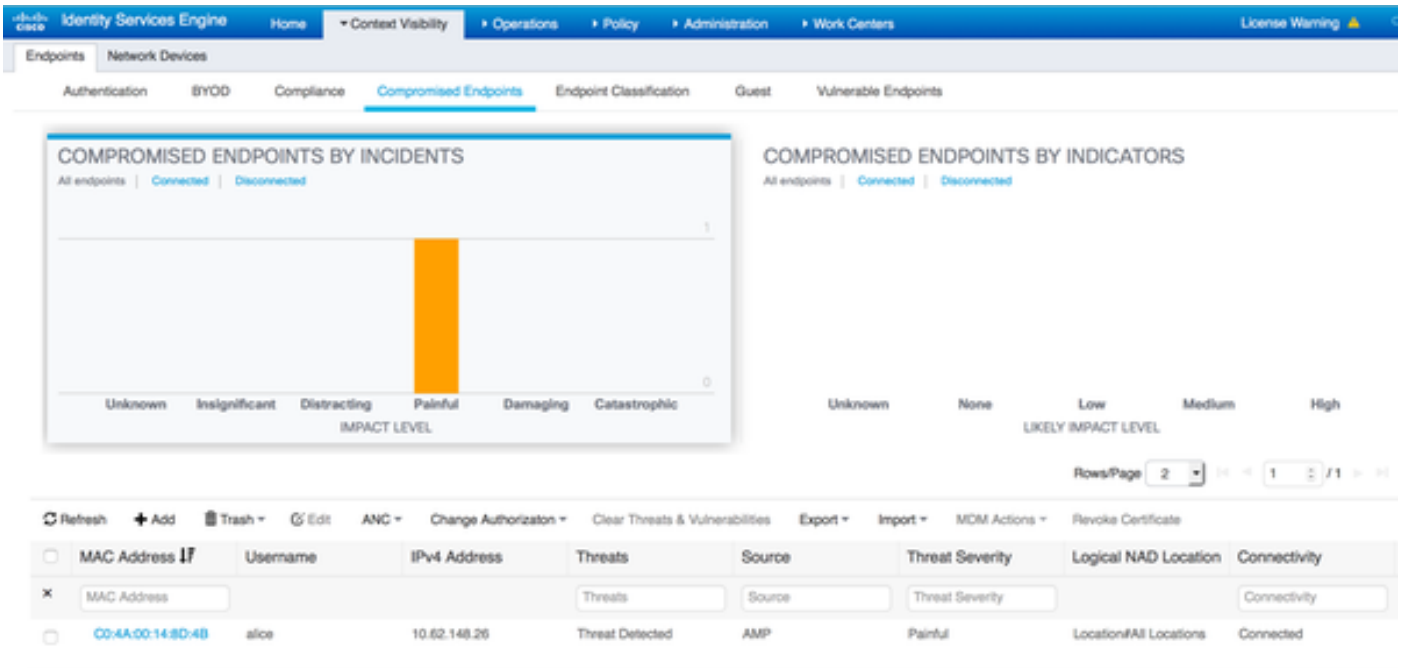


ISE

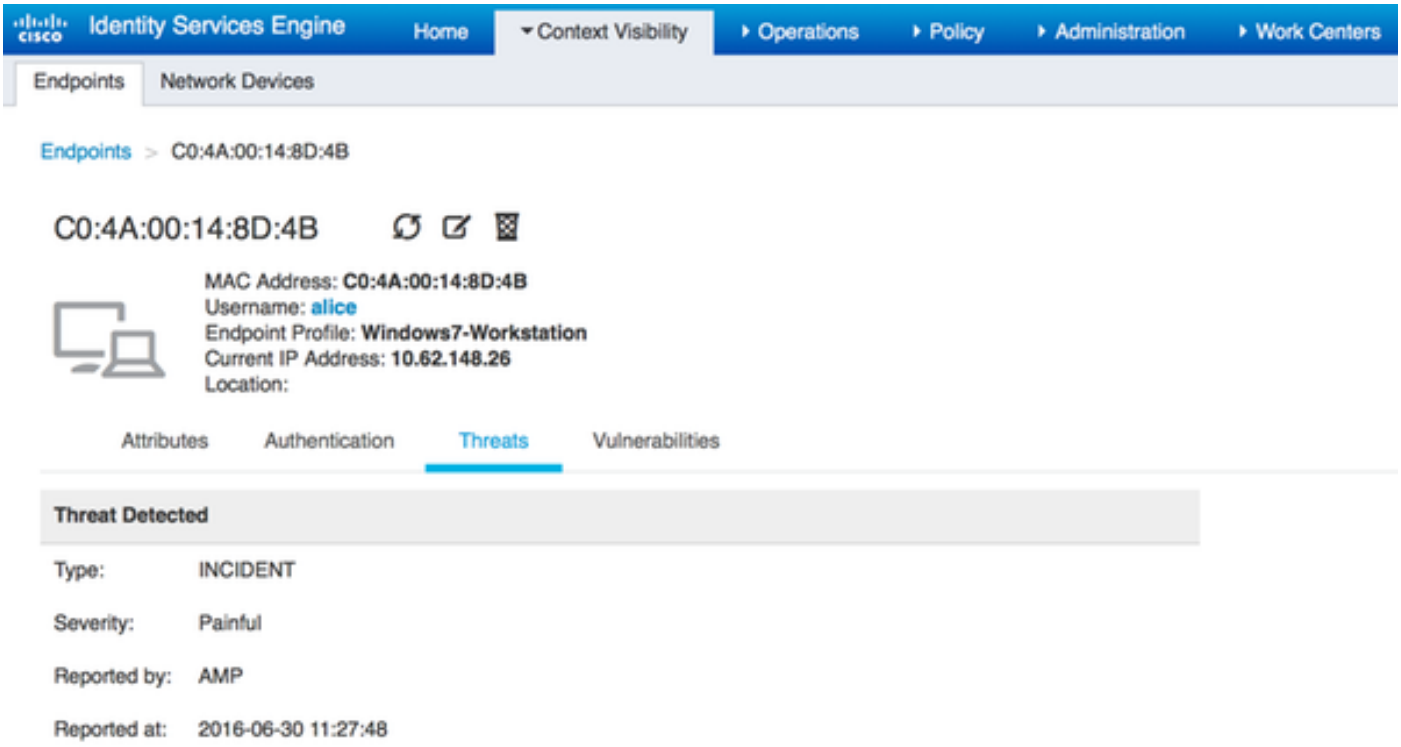
ISE 自体で定期的なポスチャ フローが見られ、ネットワークのコンプライアンスを確認するため、最初にリダイレクトが行われます。 エンドポイントが適合するとすぐに、CoA 再認証が送信され、PermitAccess を持つ新しいプロファイルが割り当てられます。



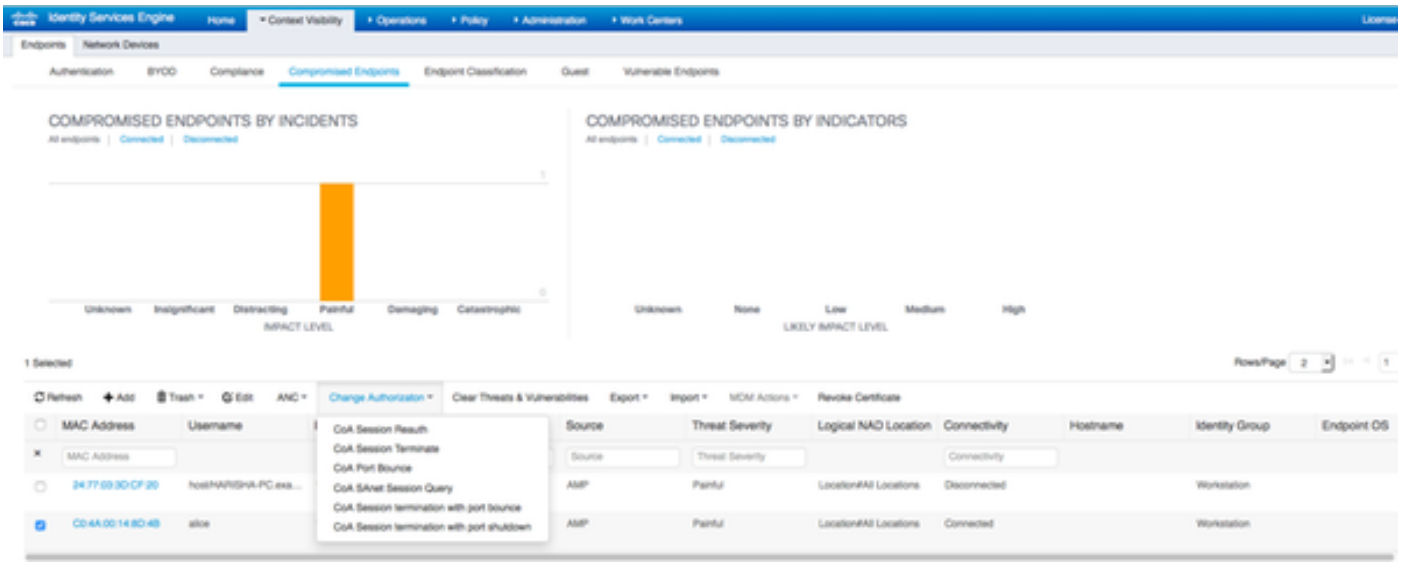
検出された脅威を表示するには、[Context Visibility] > [Endpoints] > [Compromised Endpoints] に移動します。



エンドポイントを選択し、[Threats] タブに移動すると、より多くの詳細が表示されます。



エンドポイントで脅威イベントが検出されると、[Compromised Endpoints] ページでエンドポイントの MAC アドレスを選択し、ANC ポリシーを適用することができます（設定されている場合、隔離（Quarantine）など）。 または、認可変更（Change of Authorization）を発行してセッションを終了することができます。



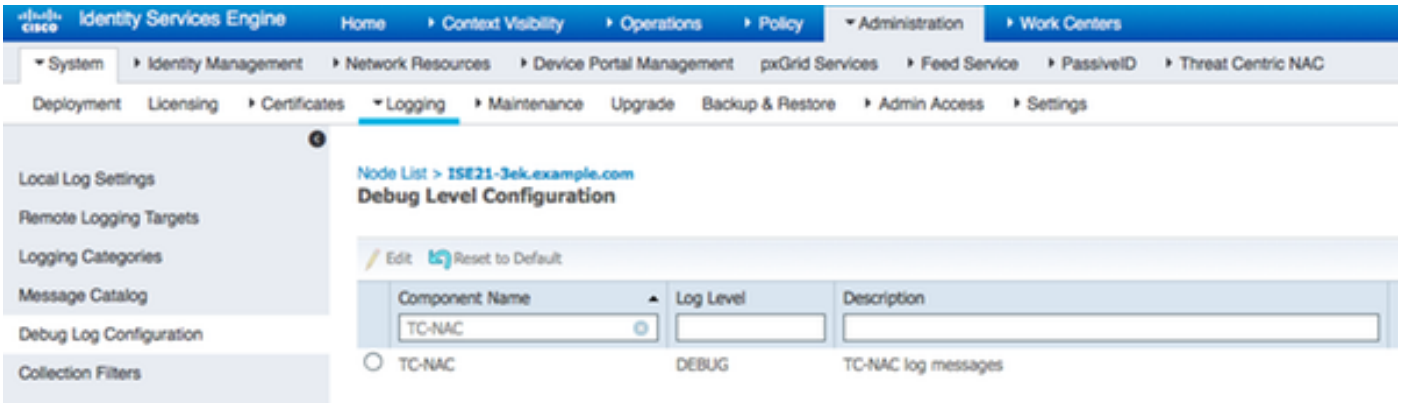
[CoA Session Terminate] を選択すると、ISE は CoA Disconnect を送信し、クライアントはネットワークへのアクセスを失います。

Other Attributes

ConfigVersionId	72
Acct-Terminate-Cause	Admin Reset
Event-Timestamp	1467305830
NetworkDeviceProfileName	Cisco
Device CoA type	Cisco CoA
Device CoA port	1700
NetworkDeviceProfileId	403ea8fc-7a27-41c3-80bb-27964031a08d
IsThirdPartyDeviceFlow	false
AcsSessionID	cfec88ac-6d2c-4b54-9fb6-716914f18744
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types
Device IP Address	10.62.148.120
CiscoAVPair	audit-session-id=0a3e9478000009ab5775481d

トラブルシューティング

ISE でデバッグを有効にするには、[Administration] > [System] > [Logging] > [Debug Log Configuration] に移動し、[TC-NAC Node] を選択して TC-NAC コンポーネントの [Log Level] を [DEBUG] に変更します。



チェックするログ：irf.log。 ISE CLI から直接次の tail コマンドを発行します。

```
ISE21-3ek/admin# show logging application irf.log tail
```

AMP クラウドから脅威イベントが届きます。

```
2016-06-30 18:27:48,617 DEBUG [IRF-AMQP-Dispatcher-Notification-0][]
cisco.cpm.irf.amqp.NotificationDispatcher:processDelivery:53 -::::: -- calling notification
handler com.cisco.cpm.irf.service.IrfNotificationHandler$MyNotificationHandler@3fac8043
Message{messageType=NOTIFICATION, messageId=THREAT_EVENT, content='{"c0:4a:00:14:8d:4b":
[{"[{"incident": {"{"Impact_Qualification": ""Painful"}, "time-stamp": 1467304068599, "vendor":
""AMP", "title": ""Threat Detected"}]}', priority=0, timestamp=Thu Jun 30 18:27:48 CEST 2016,
amqpEnvelope=Envelope(deliveryTag=79, redeliver=false, exchange=irf.topic.events,
routingKey=irf.events.threat), amqpProperties=#contentHeader<basic>(content-
type=application/json, content-encoding=null, headers=null, delivery-mode=null, priority=0,
correlation-id=null, reply-to=null, expiration=null, message-id=THREAT_EVENT, timestamp=null,
type=NOTIFICATION, user-id=null, app-id=fe80e16e-cde8-4d7f-a836-545416ae56f4, cluster-id=null)}
2016-06-30 18:27:48,617 DEBUG [IRF-AMQP-Dispatcher-Notification-0][]
cisco.cpm.irf.service.IrfNotificationHandler:handle:140 -::::: -- Added to the pending queue:
Message{messageType=NOTIFICATION, messageId=THREAT_EVENT, content='{"c0:4a:00:14:8d:4b":
[{"[{"incident": {"{"Impact_Qualification": ""Painful"}, "time-stamp": 1467304068599, "vendor":
""AMP", "title": ""Threat Detected"}]}', priority=0, timestamp=Thu Jun 30 18:27:48 CEST 2016,
amqpEnvelope=Envelope(deliveryTag=79, redeliver=false, exchange=irf.topic.events,
routingKey=irf.events.threat), amqpProperties=#contentHeader<basic>(content-
type=application/json, content-encoding=null, headers=null, delivery-mode=null, priority=0,
correlation-id=null, reply-to=null, expiration=null, message-id=THREAT_EVENT, timestamp=null,
type=NOTIFICATION, user-id=null, app-id=fe80e16e-cde8-4d7f-a836-545416ae56f4, cluster-id=null)}
2016-06-30 18:27:48,617 DEBUG [IRF-AMQP-Dispatcher-Notification-0][]
cisco.cpm.irf.amqp.NotificationDispatcher:processDelivery:59 -::::: -- DONE processing
notification: Envelope(deliveryTag=79, redeliver=false, exchange=irf.topic.events,
routingKey=irf.events.threat) #contentHeader<basic>(content-type=application/json, content-
encoding=null, headers=null, delivery-mode=null, priority=0, correlation-id=null, reply-to=null,
expiration=null, message-id=THREAT_EVENT, timestamp=null, type=NOTIFICATION, user-id=null, app-
id=fe80e16e-cde8-4d7f-a836-545416ae56f4, cluster-id=null)
2016-06-30 18:27:48,706 DEBUG [IRF-EventProcessor-0][]
cisco.cpm.irf.service.IrfEventProcessor:parseNotification:221 -::::: -- parsing notification:
Message{messageType=NOTIFICATION, messageId=THREAT_EVENT, content='{"c0:4a:00:14:8d:4b":
[{"[{"incident": {"{"Impact_Qualification": ""Painful"}, "time-stamp": 1467304068599, "vendor":
""AMP", "title": ""Threat Detected"}]}', priority=0, timestamp=Thu Jun 30 18:27:48 CEST 2016,
amqpEnvelope=Envelope(deliveryTag=79, redeliver=false, exchange=irf.topic.events,
routingKey=irf.events.threat), amqpProperties=#contentHeader<basic>(content-
type=application/json, content-encoding=null, headers=null, delivery-mode=null, priority=0,
correlation-id=null, reply-to=null, expiration=null, message-id=THREAT_EVENT, timestamp=null,
type=NOTIFICATION, user-id=null, app-id=fe80e16e-cde8-4d7f-a836-545416ae56f4, cluster-id=null)}
```

脅威が PAN に送信されたことに関する情報

```
2016-06-30 18:27:48,724 DEBUG [IRF-EventProcessor-0][]
cisco.cpm.irf.service.IrfEventProcessor:storeEventsInES:366 -::::: -- Adding threat event info
to send to PAN - c0:4a:00:14:8d:4b {incident={Impact_Qualification=Painful}, time-
stamp=1467304068599, vendor=AMP, title=Threat Detected}
```