Konfigurieren von ISE 2.1 Threat-Centric NAC (TC-NAC) mit AMP und Statusservices

Inhalt

Einführung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Konfigurieren
Netzwerkdiagramm
Detaillierter Datenfluss
Konfigurieren der AMP-Cloud
Schritt 1: Connector von AMP Cloud herunterladen
ISE konfigurieren
Schritt 1: Konfigurieren von Statusrichtlinien und -bedingungen
Schritt 2: Konfigurieren des Status-Profils
Schritt 3: Konfigurieren des AMP-Profils
Schritt 2: Hochladen von Anwendungen und XML-Profil auf die ISE
Schritt 3: AnyConnect Compliance-Modul herunterladen
Schritt 4: AnyConnect-Konfiguration hinzufügen
Schritt 5: Konfigurieren von Client-Bereitstellungsregeln
Schritt 6: Autorisierungsrichtlinien konfigurieren
Schritt 7: Aktivieren von TC-NAC-Services
Schritt 8: Konfigurieren des AMP-Adapters
Überprüfen
Endpunkt
AMP-Cloud
ISE
Fehlerbehebung

Einführung

In diesem Dokument wird beschrieben, wie Threat-Centric NAC mit Advanced Malware Protection (AMP) auf Identity Services Engine (ISE) 2.1 konfiguriert wird. Die Schweregrade von Bedrohungen und Ergebnisse der Schwachstellenbewertung können verwendet werden, um die Zugriffsstufe eines Endpunkts oder Benutzers dynamisch zu steuern. Statusservices werden ebenfalls in diesem Dokument behandelt.

> **Hinweis**: Das Dokument beschreibt die ISE 2.1-Integration mit AMP. Die Statusservices werden bei der Bereitstellung von AMP von der ISE als erforderlich angezeigt.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über grundlegende Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco Identity Service Engine
- Advanced Malware Protection

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Identity Service Engine Version 2.1
- Wireless LAN Controller (WLC) 8.0.121.0
- AnyConnect VPN Client 4.2.02075
- Windows 7 Service Pack 1

Konfigurieren

Netzwerkdiagramm

Detaillierter Datenfluss

1. Der Client stellt eine Verbindung zum Netzwerk her, das **AMP_Profile** wird zugewiesen und der Benutzer wird zum AnyConnect-Bereitstellungsportal umgeleitet. Wenn AnyConnect auf dem Computer nicht erkannt wird, werden alle konfigurierten Module (VPN, AMP, Status) installiert. Konfiguration wird für jedes Modul zusammen mit diesem Profil übernommen.

2. Sobald AnyConnect installiert ist, wird eine Statusüberprüfung ausgeführt.

3. Das AMP Enabler-Modul installiert den FireAMP-Anschluss

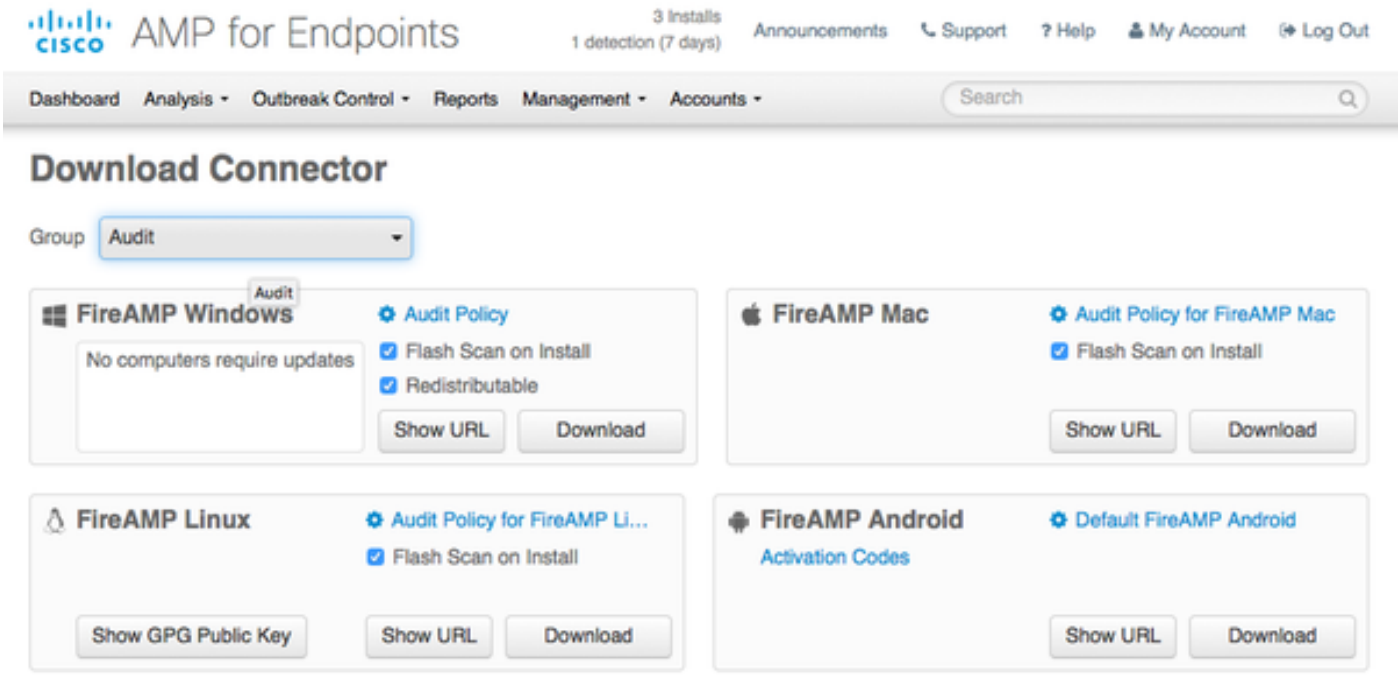
4. Wenn ein Client versucht, schädliche Software herunterzuladen, löst der AMP-Connector eine Warnmeldung aus und meldet sie an die AMP-Cloud

5. AMP Cloud sendet diese Informationen an die ISE

Konfigurieren der AMP-Cloud

Schritt 1: Connector von AMP Cloud herunterladen

Um den Connector herunterzuladen, navigieren Sie zu Management > Download Connector (Management > Anschluss herunterladen). Wählen Sie anschließend Typ und **Download** FireAMP (Windows, Android, Mac, Linux) aus. In diesem Fall wurde **Audit** ausgewählt und die Installationsdatei von FireAMP für Windows.

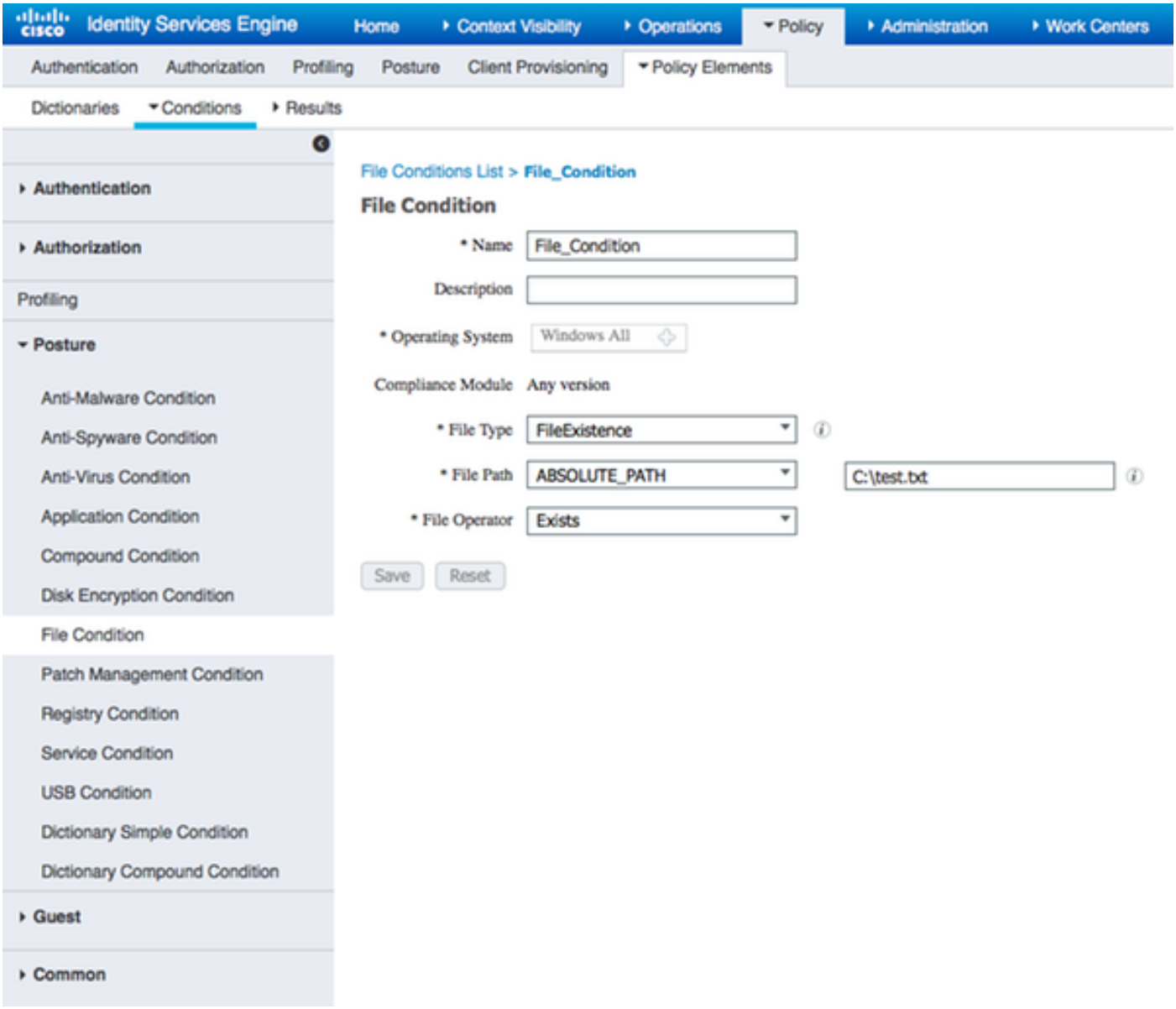


> **Hinweis**: Beim Herunterladen dieser Datei wird eine .exe-Datei mit dem Namen **Audit_FireAMPSetup.exe** im Beispiel generiert. Diese Datei wurde an den Webserver gesendet, um verfügbar zu sein, sobald der Benutzer die Konfiguration von AMP anfordert.

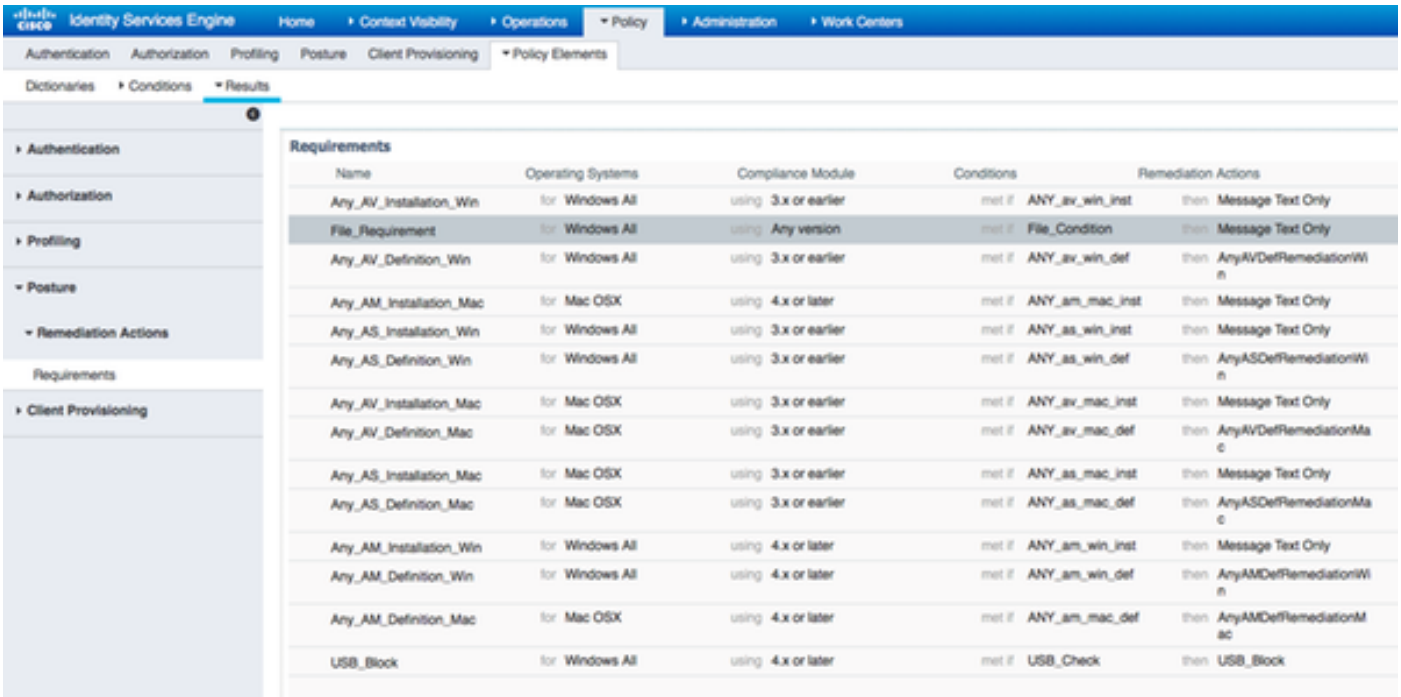
ISE konfigurieren

Schritt 1: Konfigurieren von Statusrichtlinien und -bedingungen

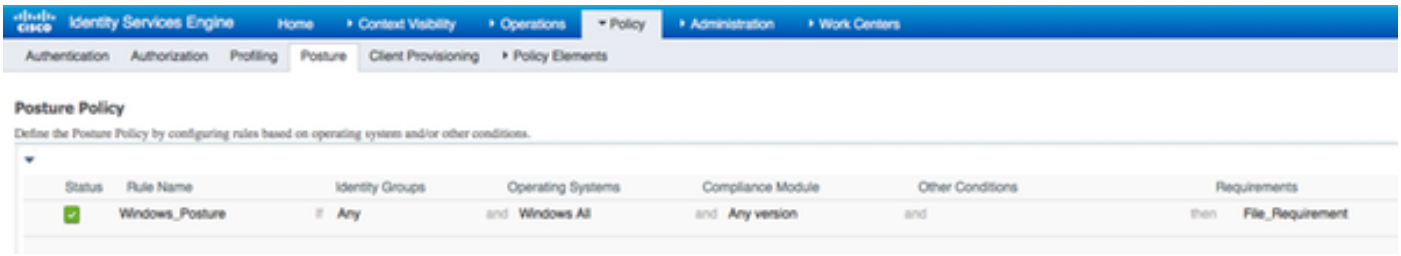
Navigieren Sie zu Richtlinien > Richtlinienelemente > Bedingungen > Status > Dateibedingung.Sie können sehen, dass eine einfache Bedingung für das Vorhandensein einer Datei erstellt wurde. Wenn der Endpunkt mit der vom Postmodul verifizierten Richtlinie übereinstimmen soll, muss eine Datei vorhanden sein:



Diese Bedingung wird für eine Anforderung verwendet:

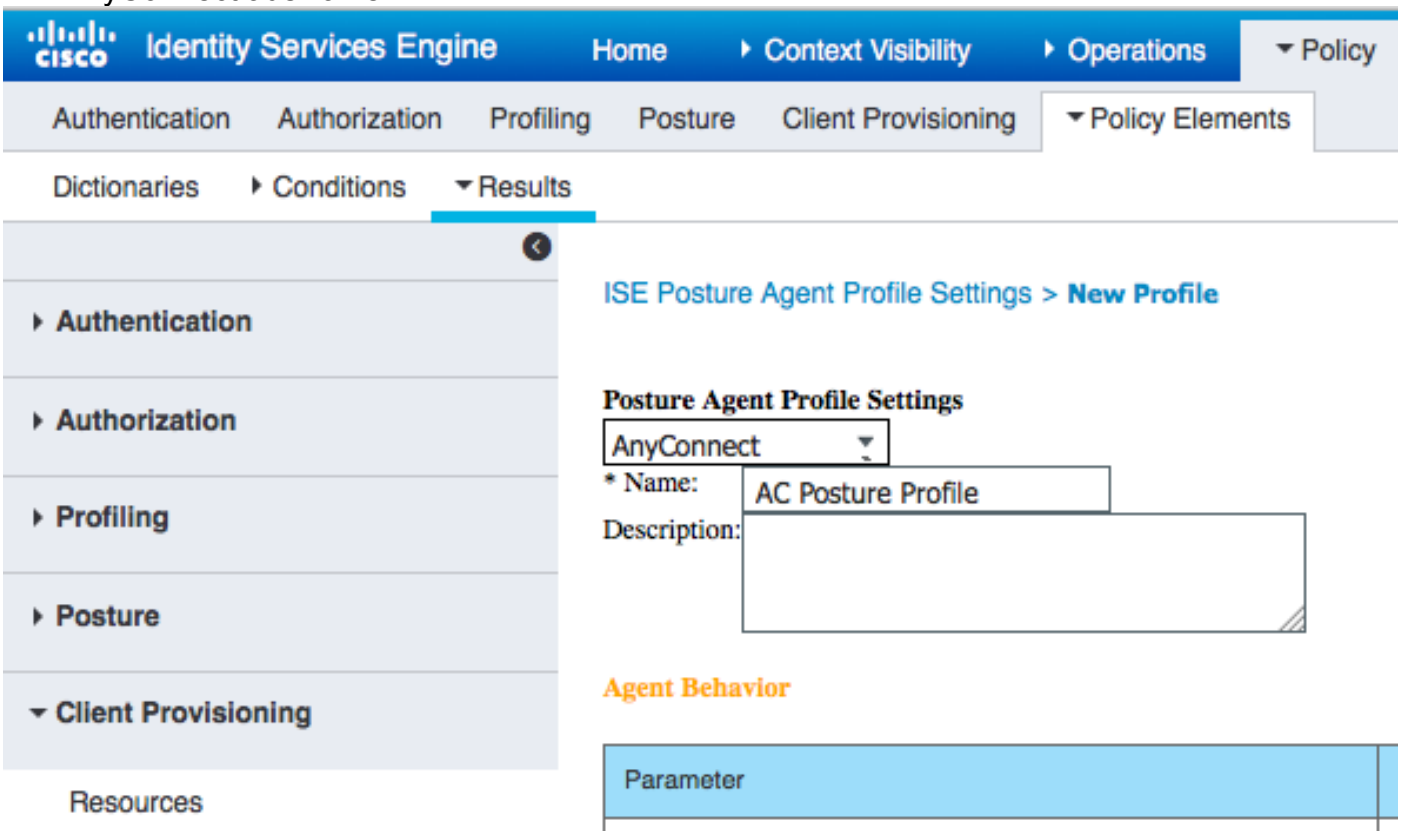


Diese Anforderung wird in der Statusrichtlinie für Microsoft Windows-Systeme verwendet:

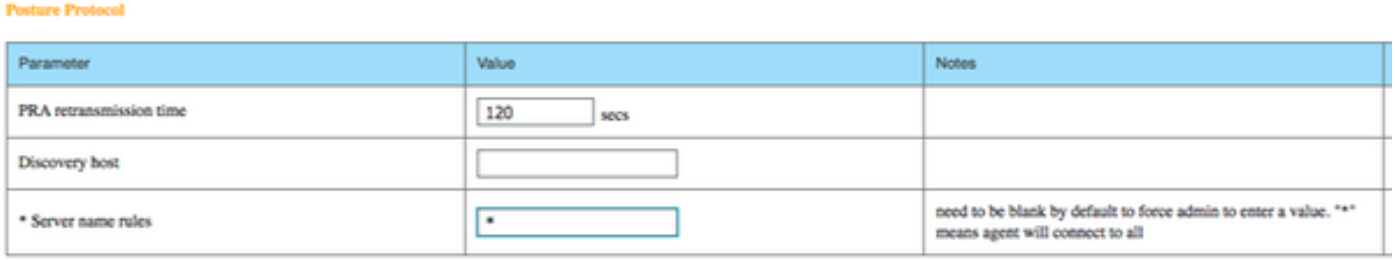


Schritt 2: Konfigurieren des Status-Profils

- Navigieren Sie zu Richtlinien > Richtlinienelemente > Ergebnisse > Client Provisioning > Resources, und fügen Sie ein NAC-Agent (Network Admission Control) oder ein AnyConnect Agent-Statusprofil hinzu.
- AnyConnect auswählen



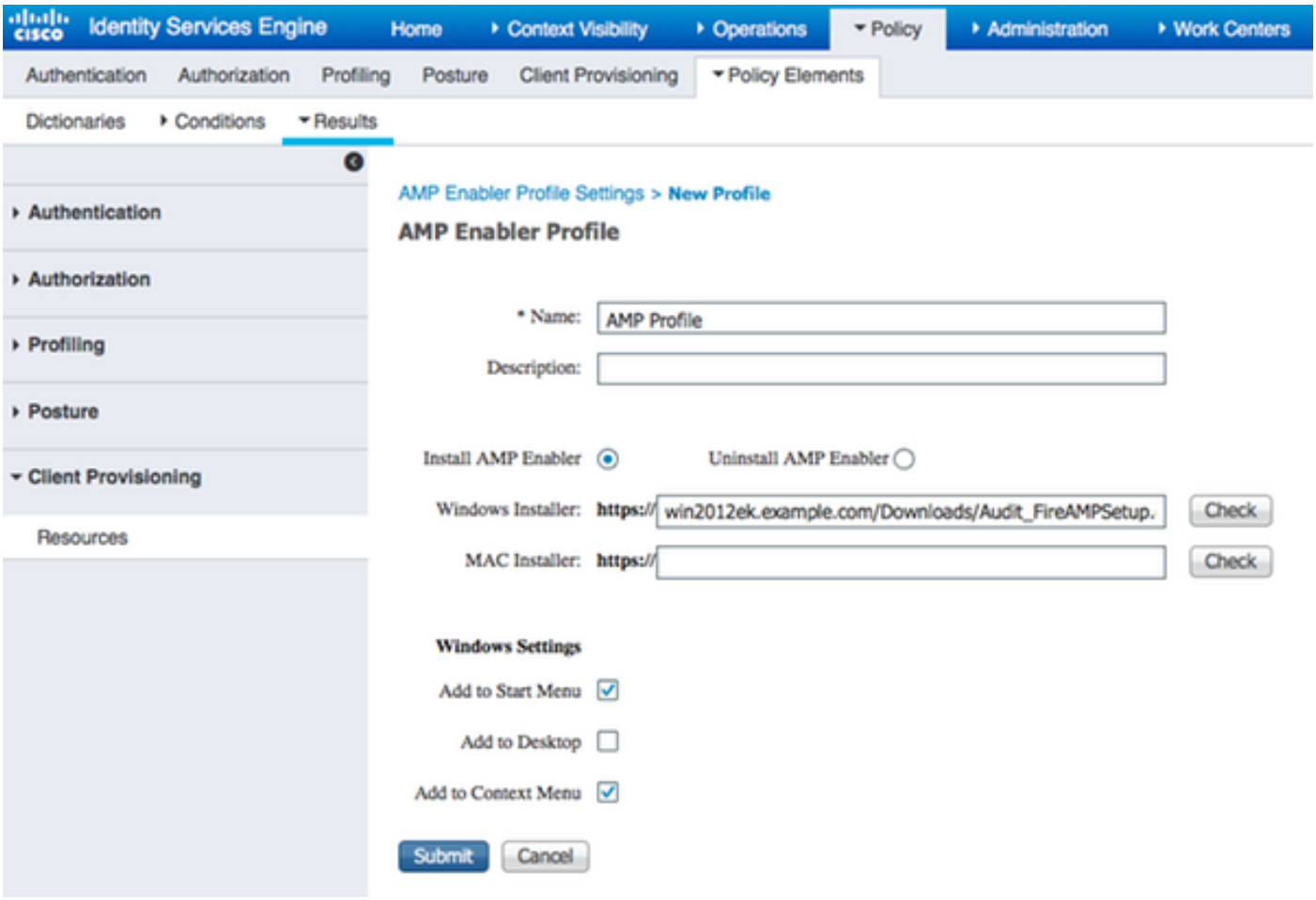
- Fügen Sie im Abschnitt Status Protocol (Status-Protokoll) * hinzu, damit der Agent eine Verbindung zu allen Servern herstellen kann.



Schritt 3: Konfigurieren des AMP-Profils

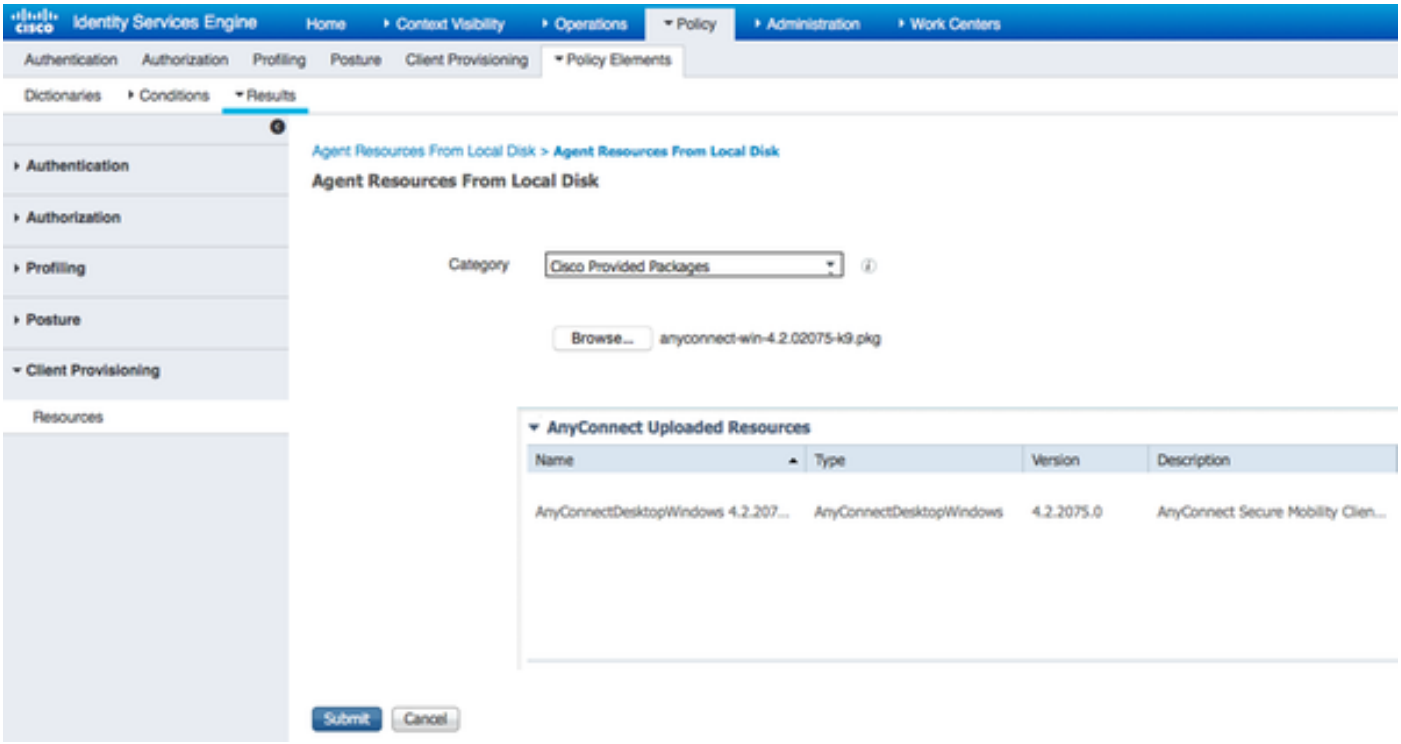
Das AMP-Profil enthält Informationen zum Speicherort des Windows-Installationsprogramms.

Windows Installer wurde zuvor von der AMP-Cloud heruntergeladen. Der Zugriff sollte vom Client-Computer aus möglich sein. Das Zertifikat des HTTPS-Servers, in dem sich Installer befindet, sollte auch vom Clientcomputer vertrauenswürdig sein.

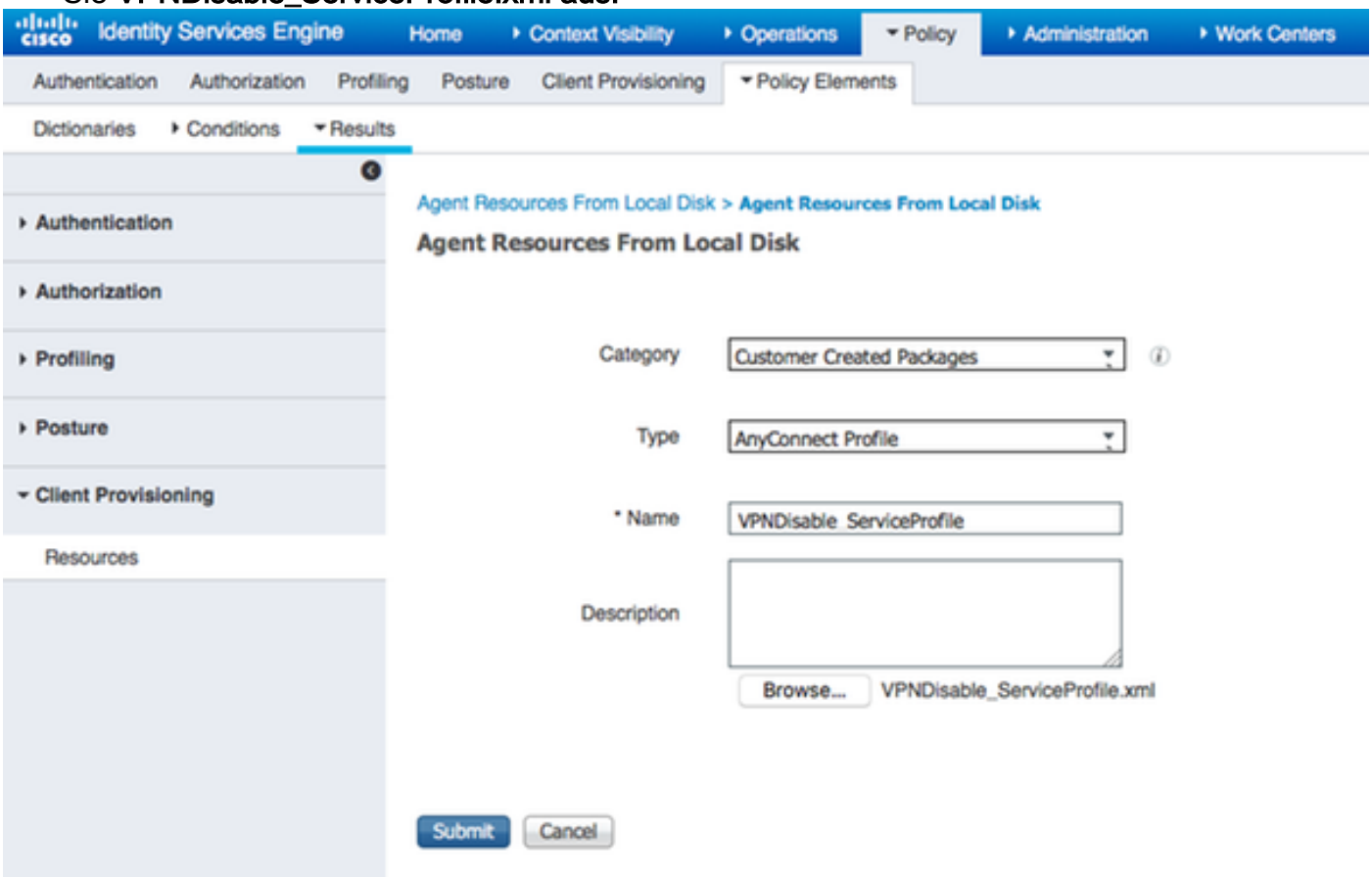


Schritt 2: Hochladen von Anwendungen und XML-Profil auf die ISE

- Laden Sie die Anwendung manuell von der offiziellen Cisco Website herunter: **anyconnect-win-4.2.02075-k9.pkg**
- Navigieren Sie auf der ISE zu Richtlinien > Richtlinienelemente > Ergebnisse > Client Provisioning > Resources, und fügen Sie **Agent Resources from Local Disk** hinzu.
- Wählen Sie **Von Cisco bereitgestellte Pakete** aus, und wählen Sie **anyconnect-win-4.2.02075-k9.pkg**



- Navigieren Sie zu Richtlinien > Richtlinienelemente > Ergebnisse > Client Provisioning > Resources, und fügen Sie **Agent Resources from Local Disk** hinzu.
- Wählen Sie **vom Kunden erstellte Pakete aus**, und geben Sie **AnyConnect Profile ein**. Wählen Sie **VPNDisable_ServiceProfile.xml aus.**

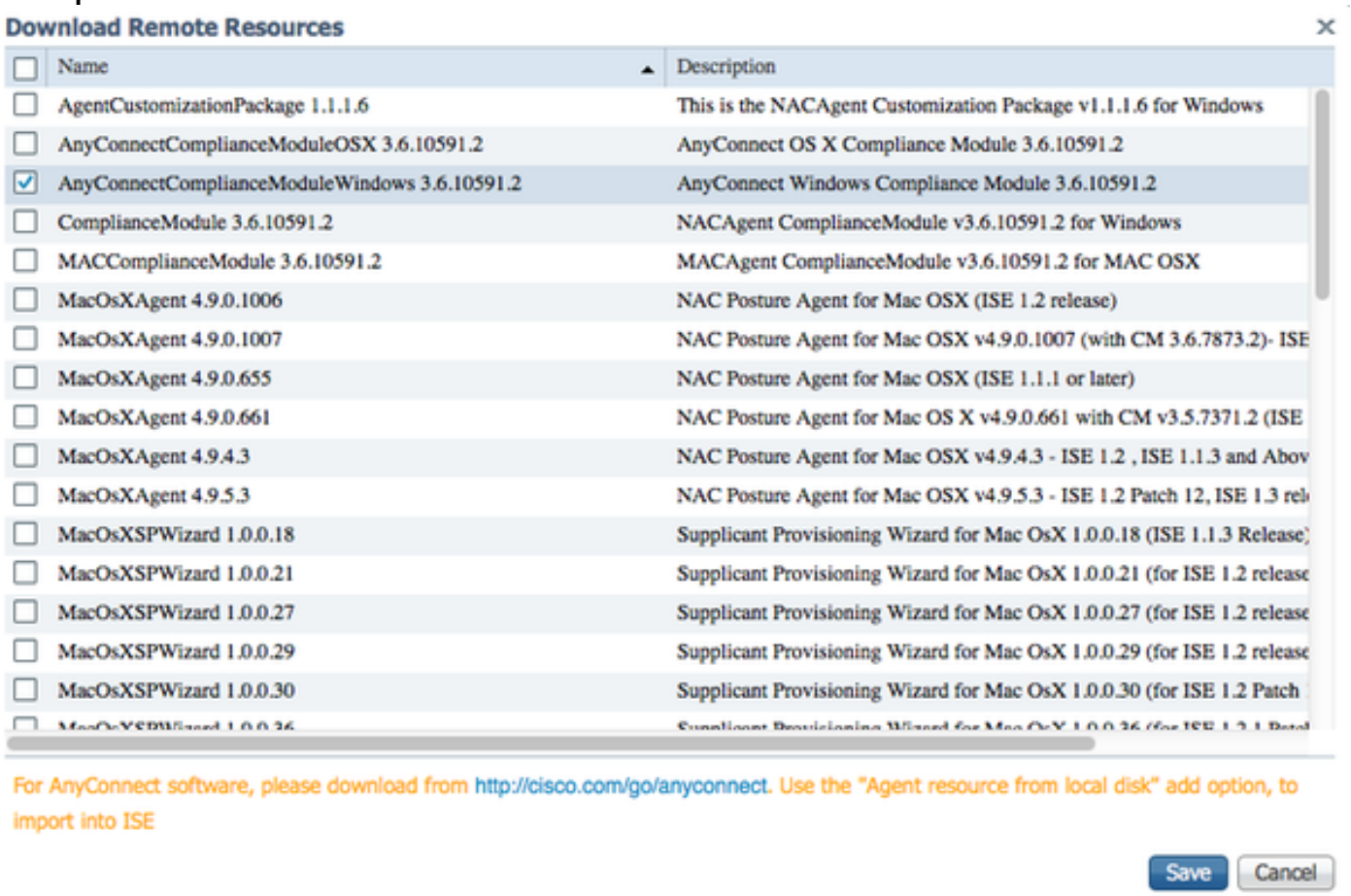


Hinweis: **VPNDisable_ServiceProfile.xml** wird verwendet, um den VPN-Titel auszublenden, da in diesem Beispiel kein VPN-Modul verwendet wird. Dies ist der Inhalt von **VPNDisable_ServiceProfile.xml**:

```
<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>
```

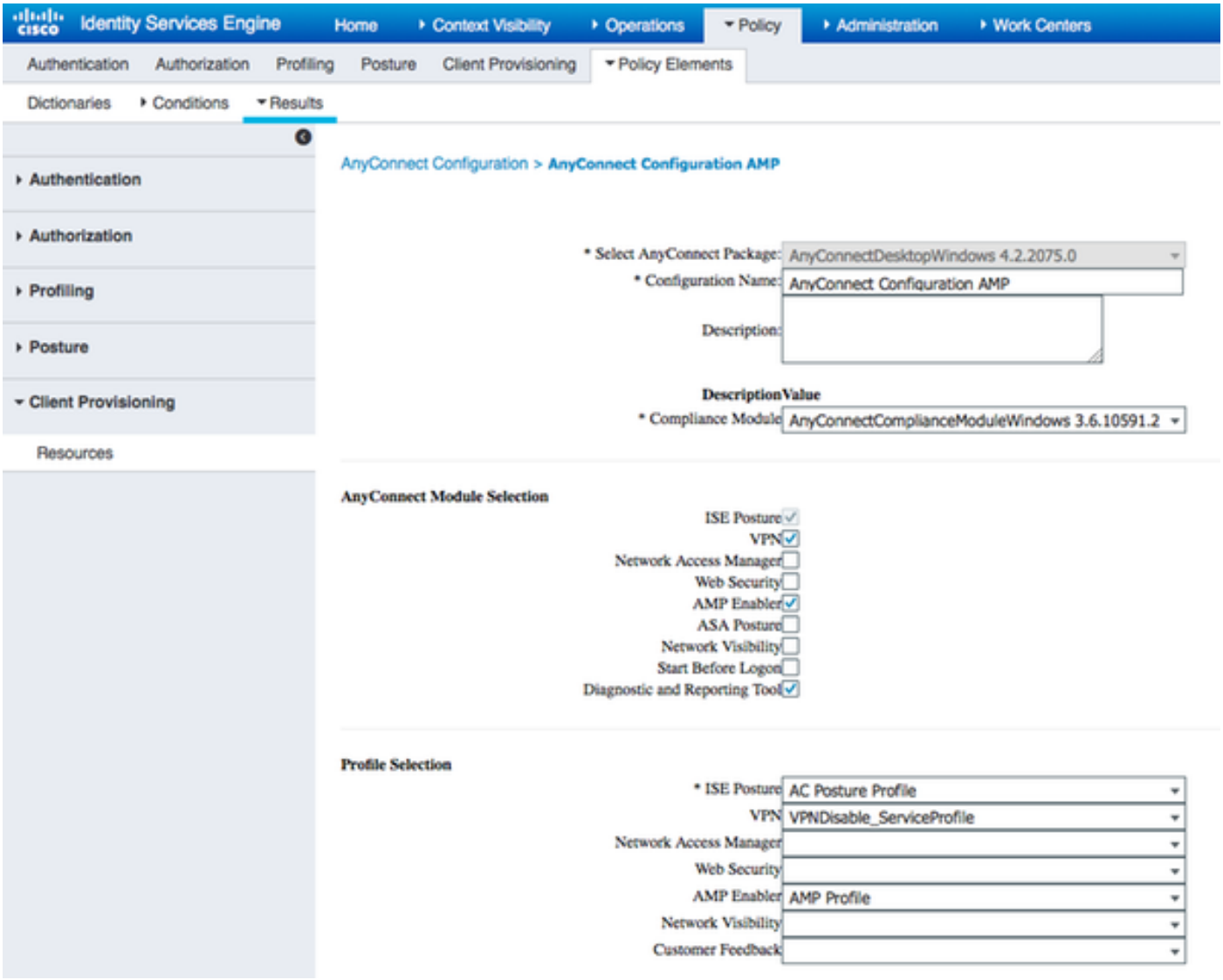
Schritt 3: AnyConnect Compliance-Modul herunterladen

- Navigieren Sie zu Richtlinien > Richtlinienelemente > Ergebnisse > Client Provisioning > Resources, und fügen Sie **Agent Resources von Cisco hinzu.**
- Wählen Sie **AnyConnect Windows Compliance Module 3.6.10591.2 aus,** und klicken Sie auf **Speichern.**



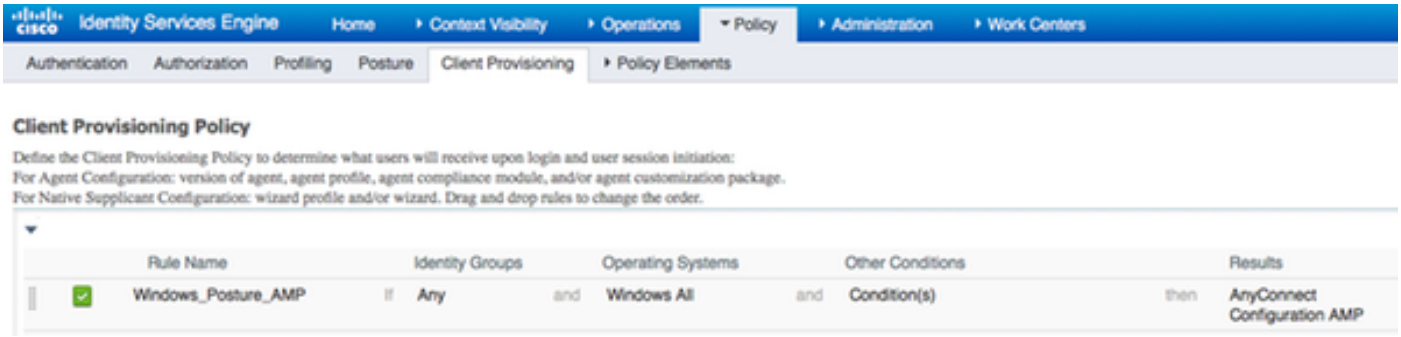
Schritt 4: AnyConnect-Konfiguration hinzufügen

- Navigieren Sie zu Richtlinien > Richtlinienelemente > Ergebnisse > Client Provisioning > Resources, und fügen Sie die **AnyConnect-Konfiguration** hinzu
- Konfigurieren Sie den Namen, und wählen Sie das Compliance-Modul und alle erforderlichen AnyConnect-Module (VPN, AMP und Status) aus.
- Wählen Sie in **Profile Selection** (Profilauswahl) das Profil aus, das zuvor für jedes Modul konfiguriert wurde.



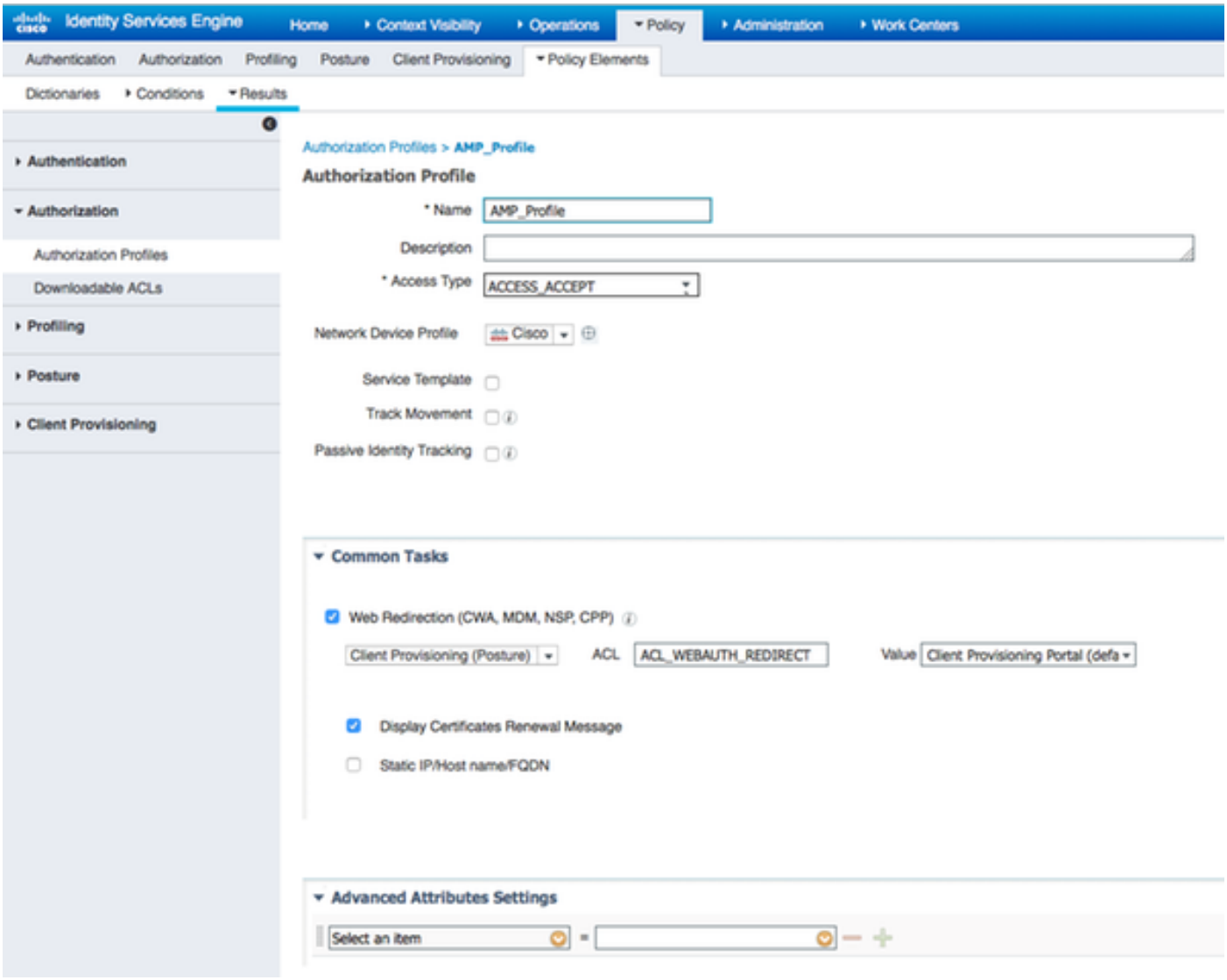
Schritt 5: Konfigurieren von Client-Bereitstellungsregeln

Auf die zuvor erstellte AnyConnect-Konfiguration wird in den **Client Provisioning**-Regeln verwiesen.

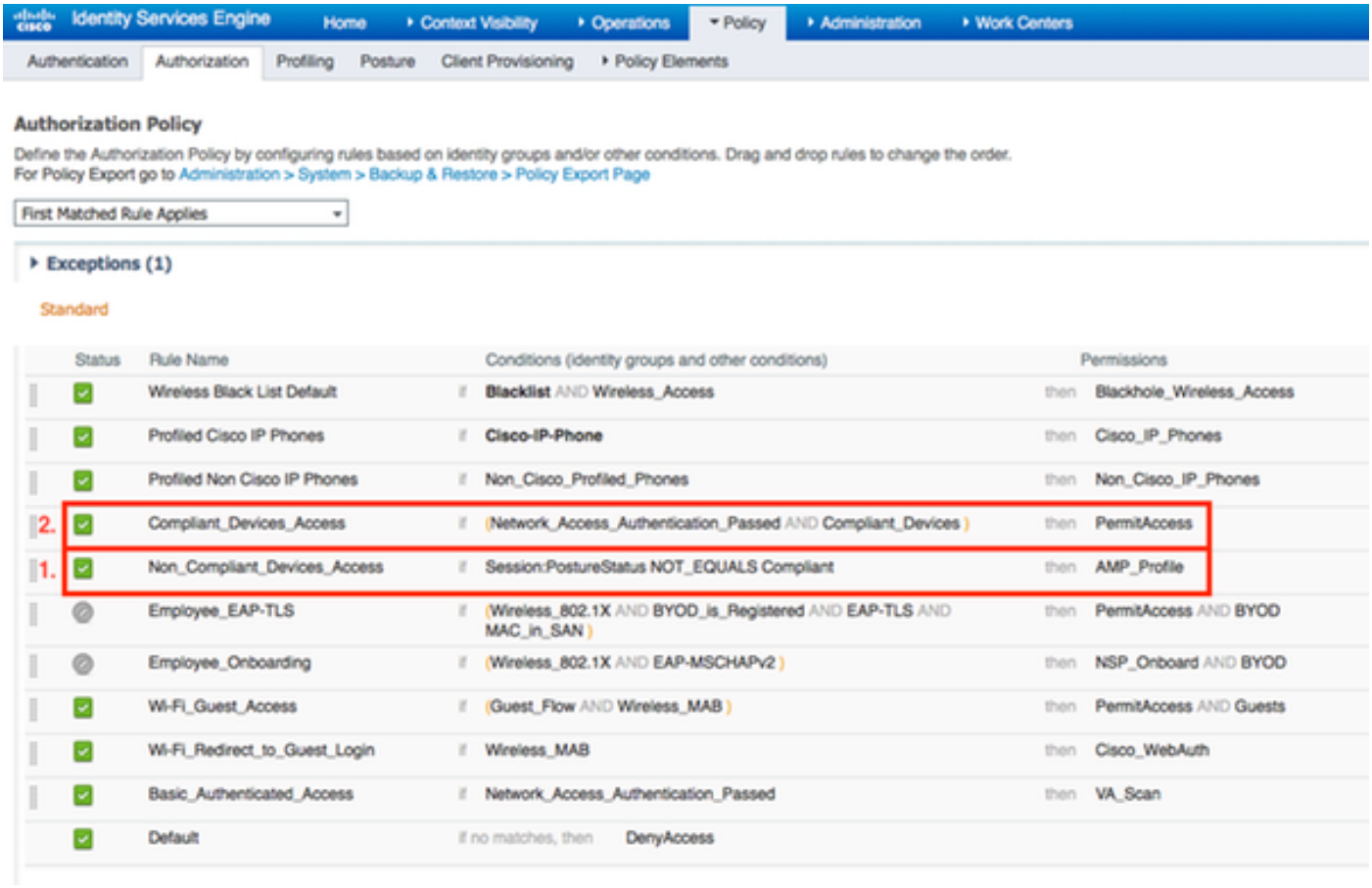


Schritt 6: Autorisierungsrichtlinien konfigurieren

Zunächst findet die Umleitung zum Client Provisioning Portal statt. Es werden standardmäßige Autorisierungsrichtlinien für den Status verwendet.

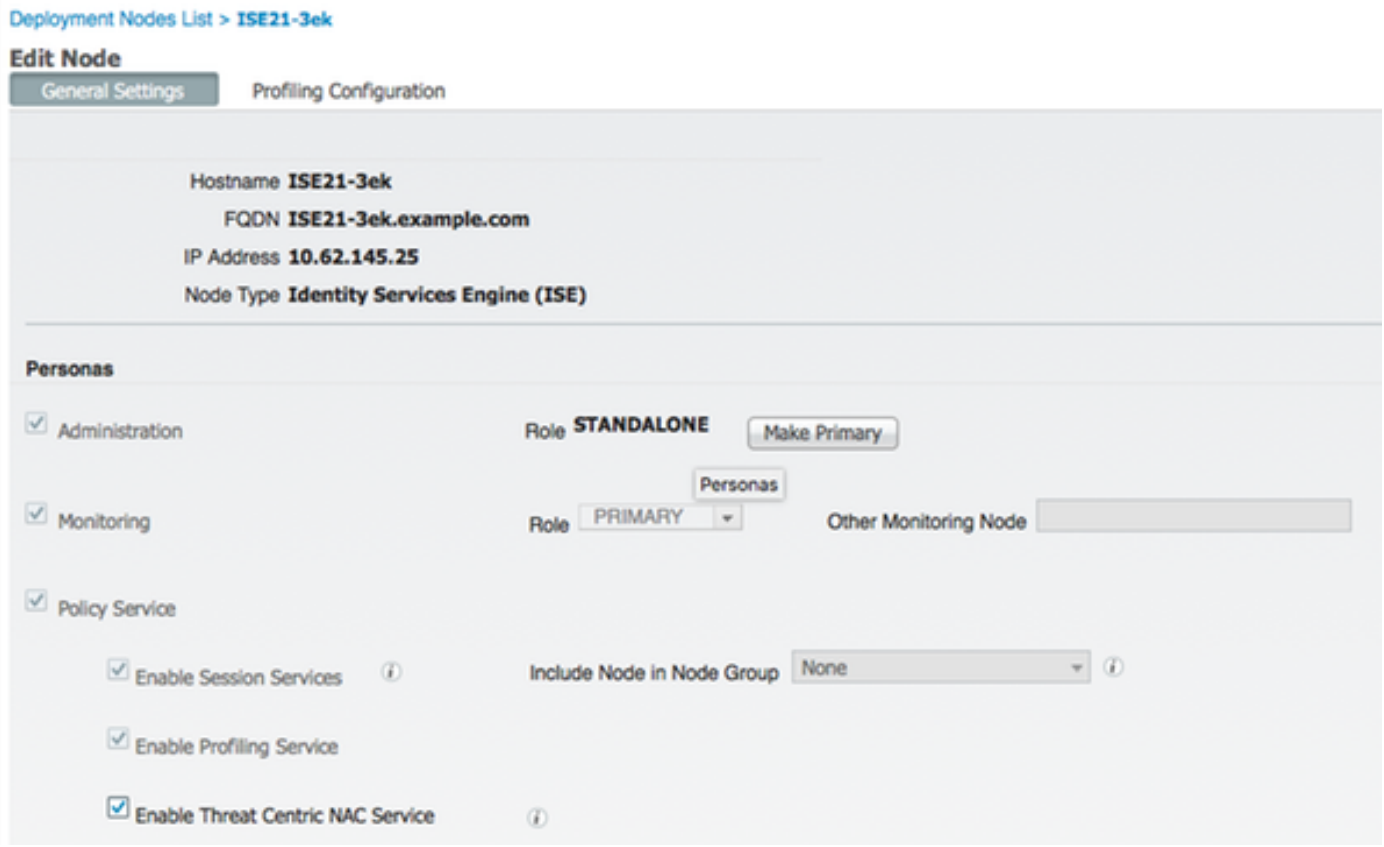


Anschließend wird der vollständige Zugriff zugewiesen, sobald die Vorgaben konform sind.



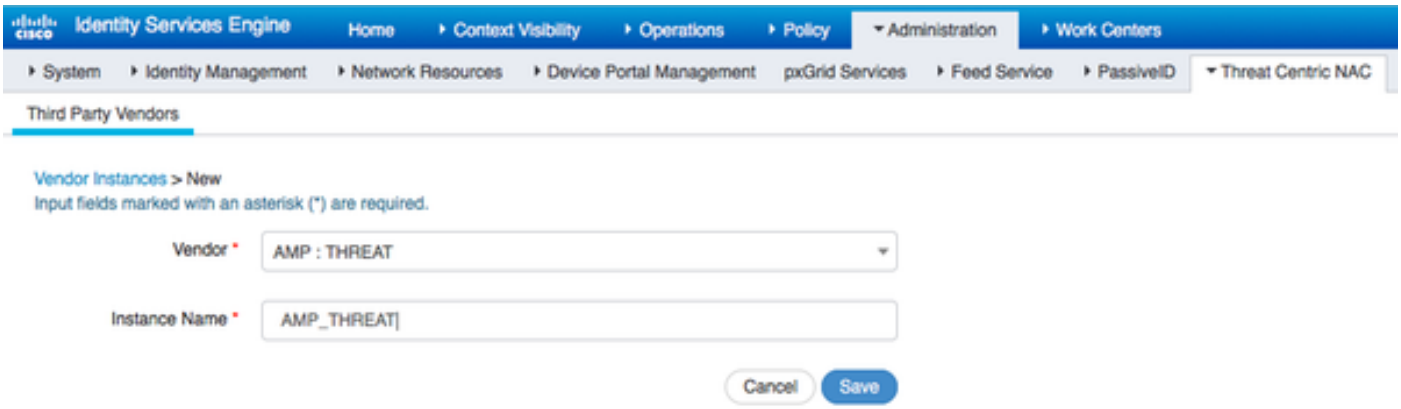
Schritt 7: Aktivieren von TC-NAC-Services

Aktivieren Sie TC-NAC Services unter Administration > Deployment > Edit Node. Aktivieren Sie das Kontrollkästchen **Threat Centric NAC Service aktivieren**.

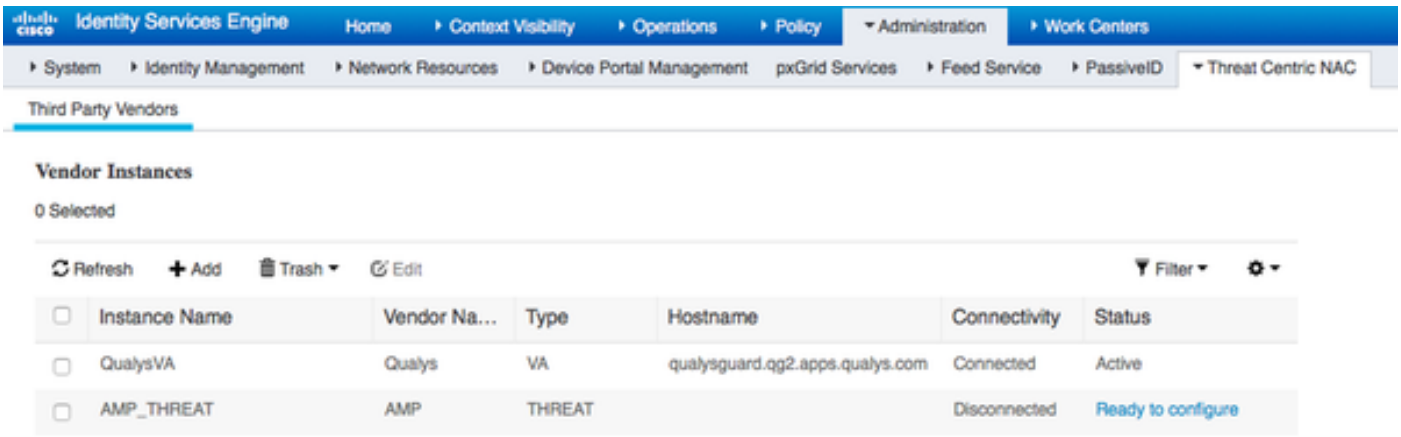


Schritt 8: Konfigurieren des AMP-Adapters

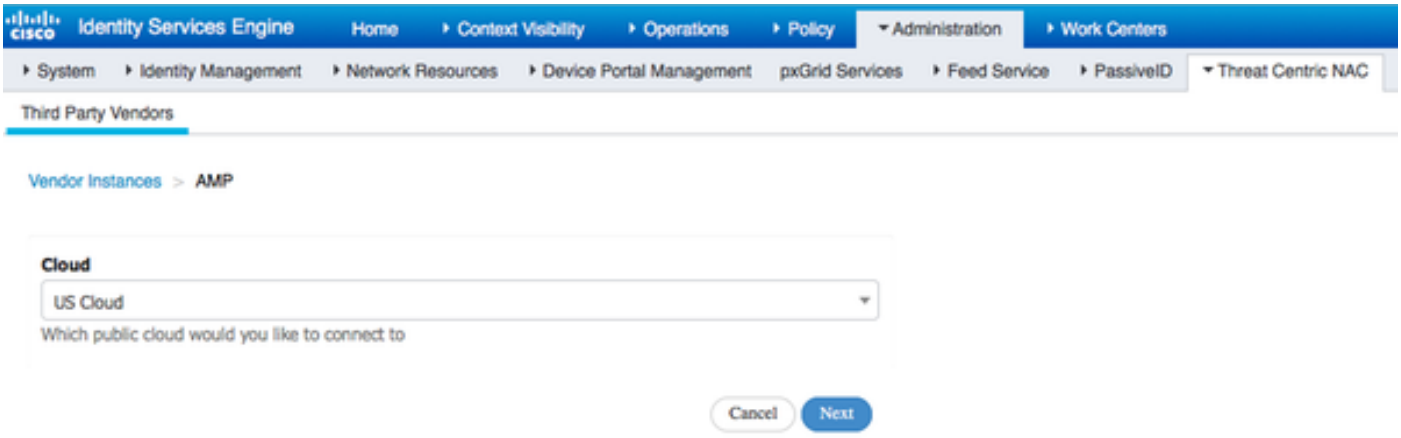
Navigieren Sie zu Administration > Threat Centric NAC > Third Party Vendors > Add. Klicken Sie auf **Speichern.**



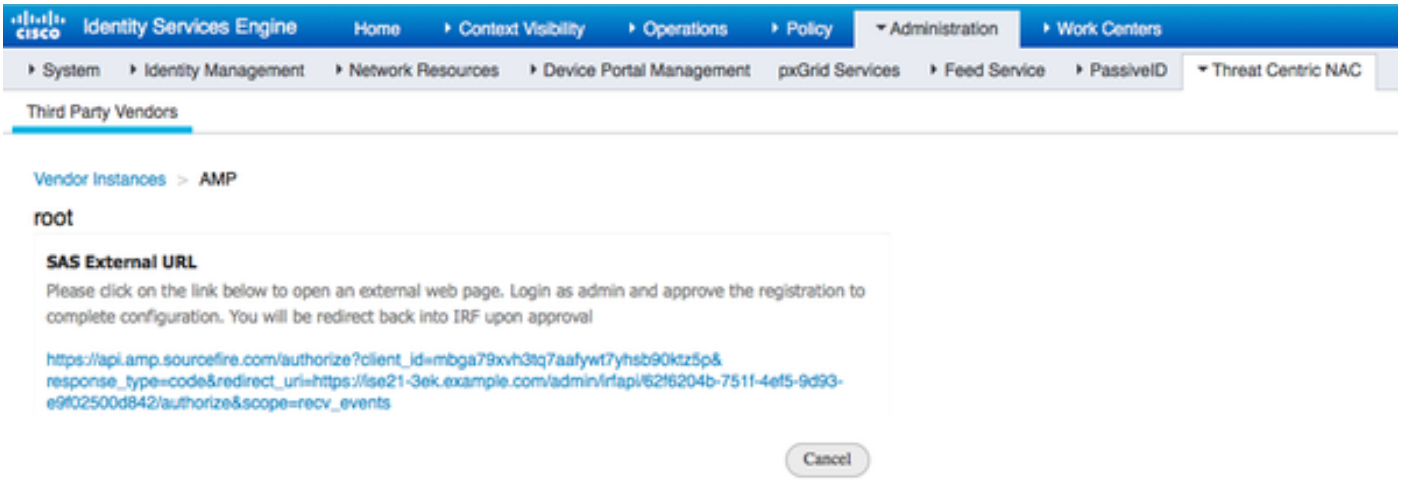
Sie sollte in den Status **Ready to Configure** (**Bereit zum Konfigurieren)** wechseln. Klicken Sie auf **Bereit zur Konfiguration.**



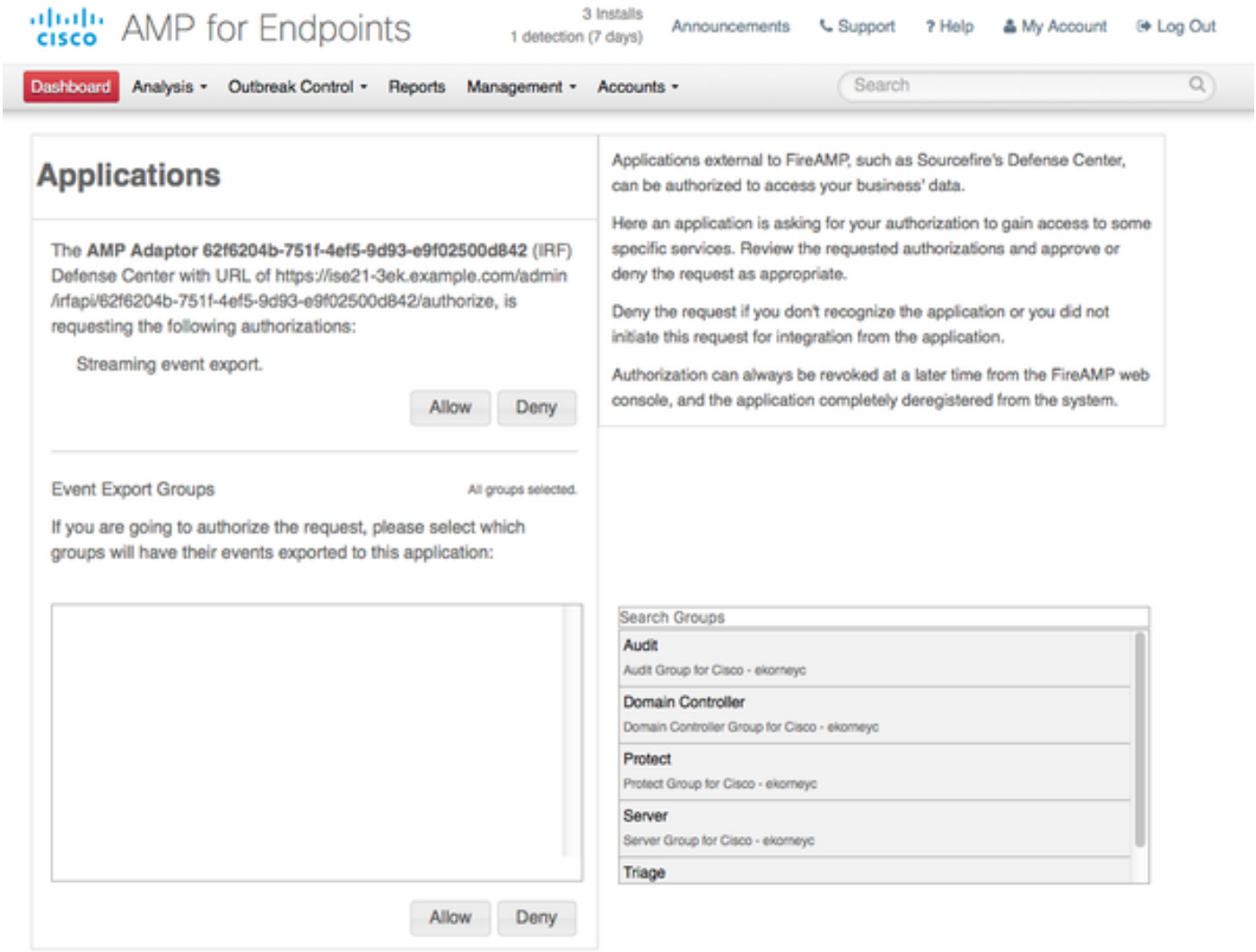
Wählen Sie **Cloud aus** und klicken Sie auf **Weiter**



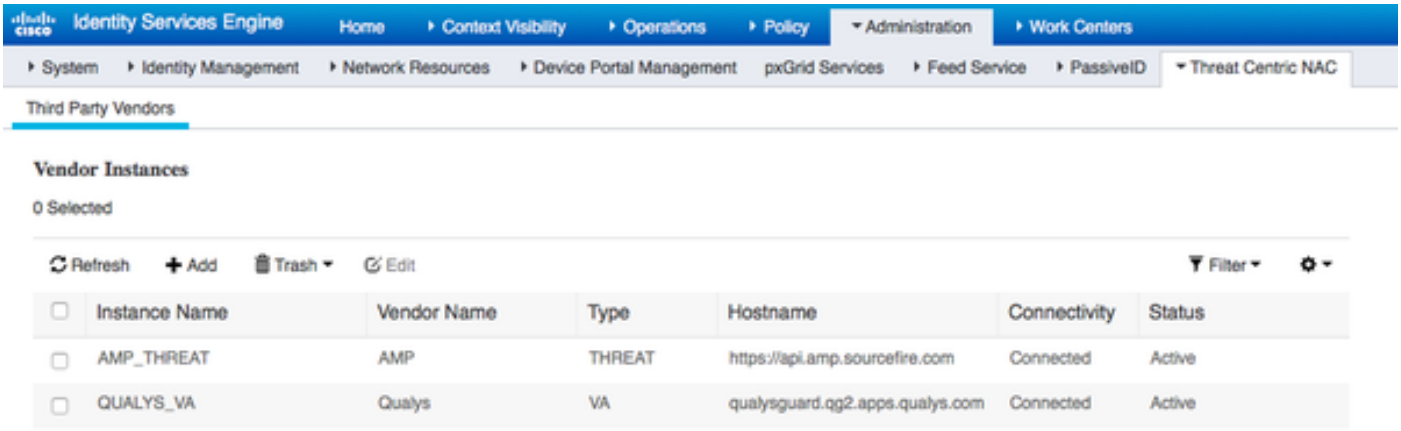
Klicken Sie auf den FireAMP-Link, und melden Sie sich als admin in FireAMP an.



Klicken Sie im Bereich **Anwendungen auf Zulassen**, um die Exportanforderung für Streaming-Ereignisse zu autorisieren. Danach werden Sie zurück zur Cisco ISE weitergeleitet.



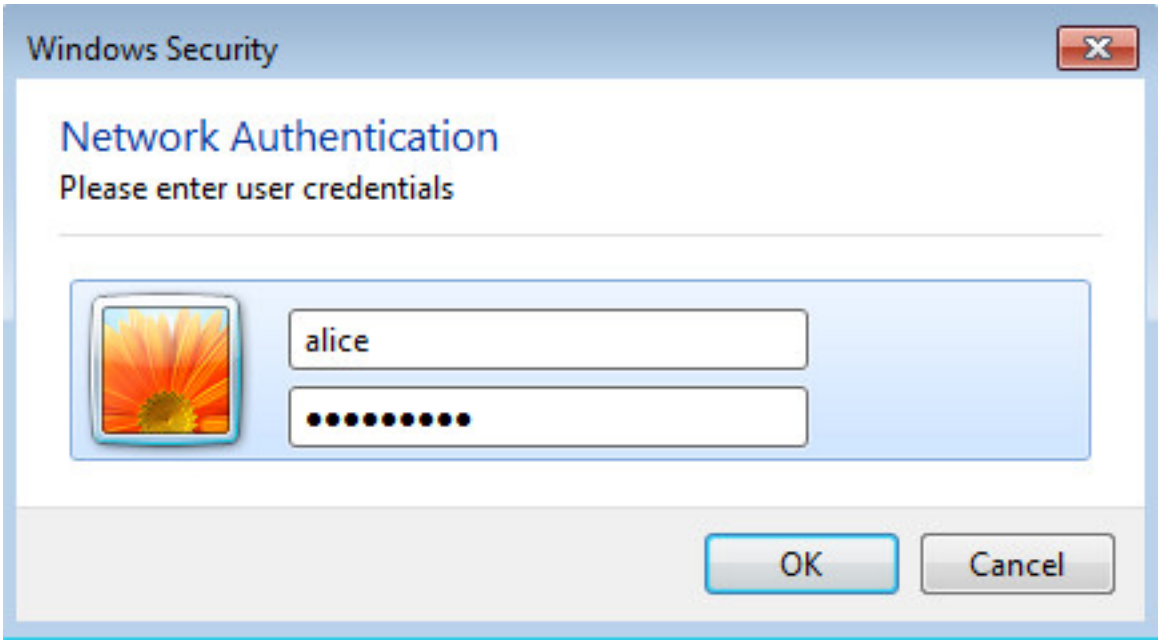
Wählen Sie die Ereignisse aus, die Sie überwachen möchten (z. B. verdächtiger Download, Verbindung zu verdächtiger Domäne, ausgeführte Malware, Java-Kompromittierung). Die Zusammenfassung der Adapterinstanzkonfiguration wird auf der Seite Konfigurationsübersicht angezeigt. Adapterinstanz wechselt in den Connected/Active State.



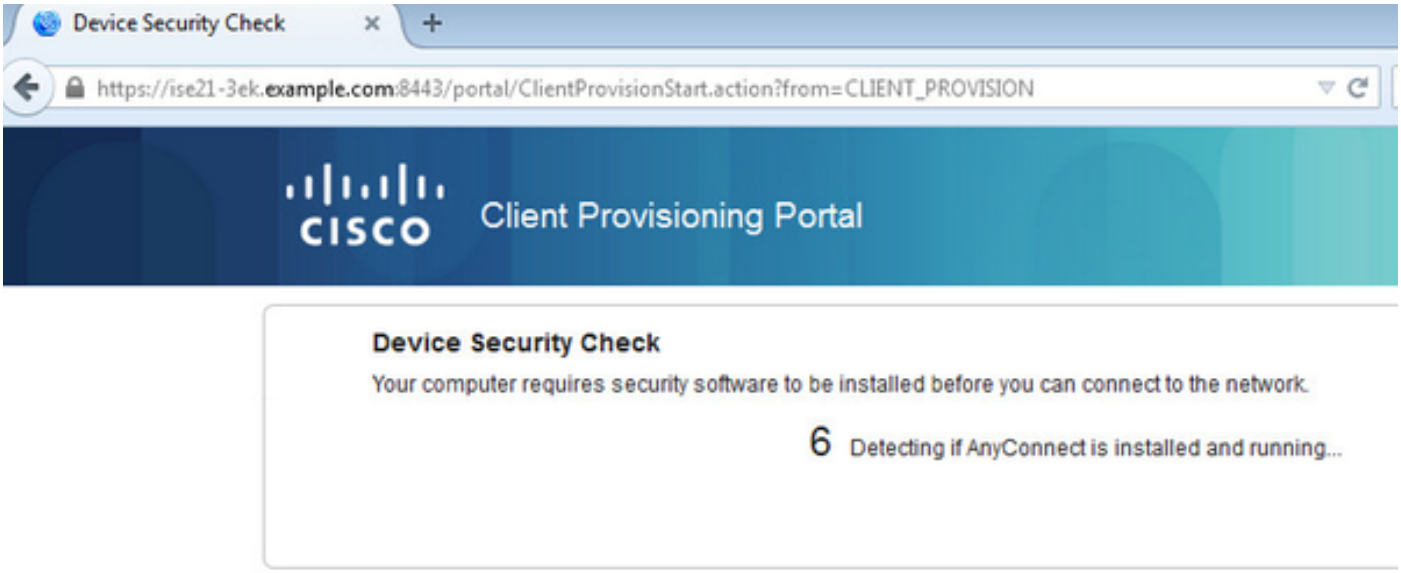
Überprüfen

Endpunkt

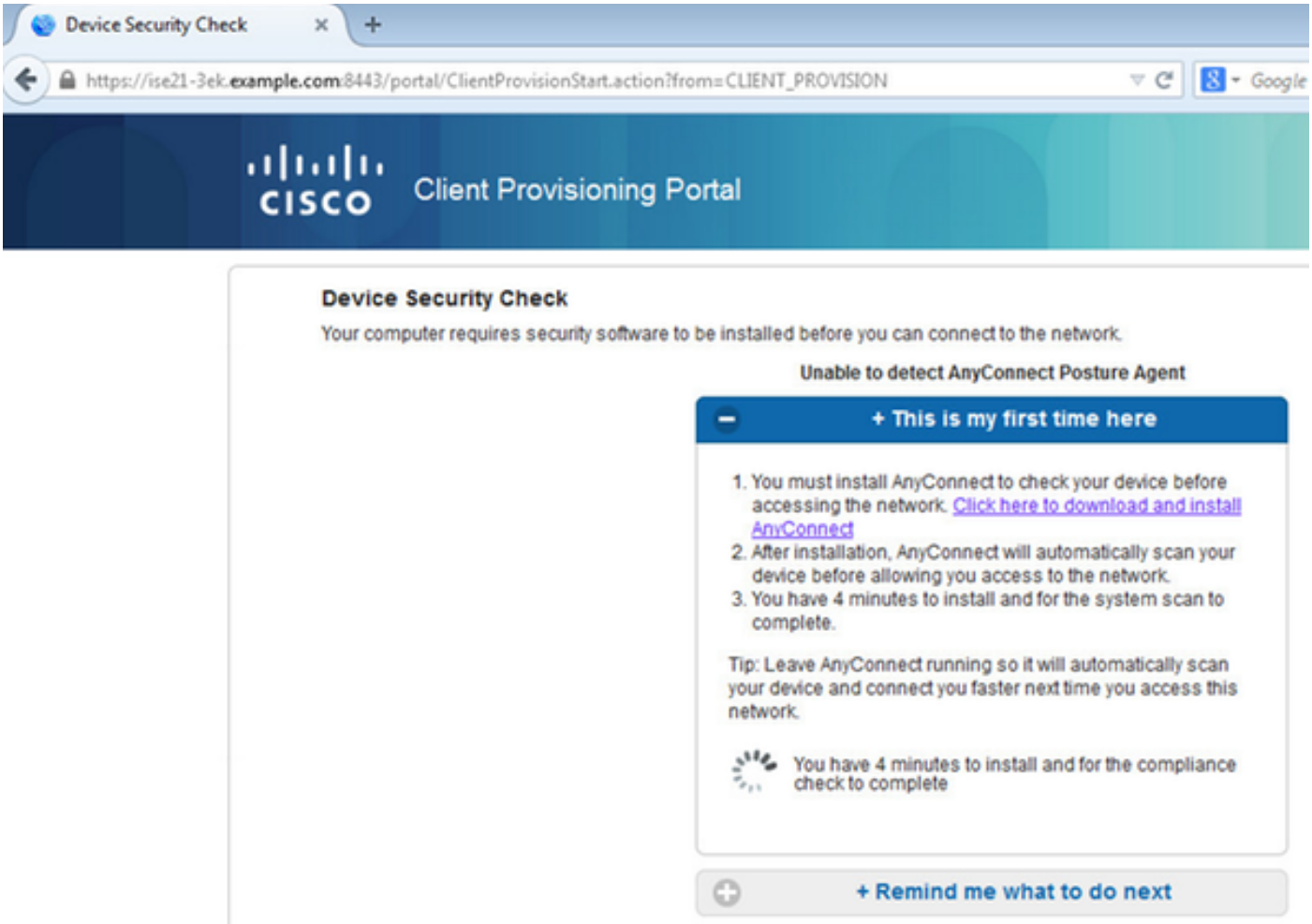
Herstellen einer Verbindung zum Wireless-Netzwerk über PEAP (MSCHAPv2).



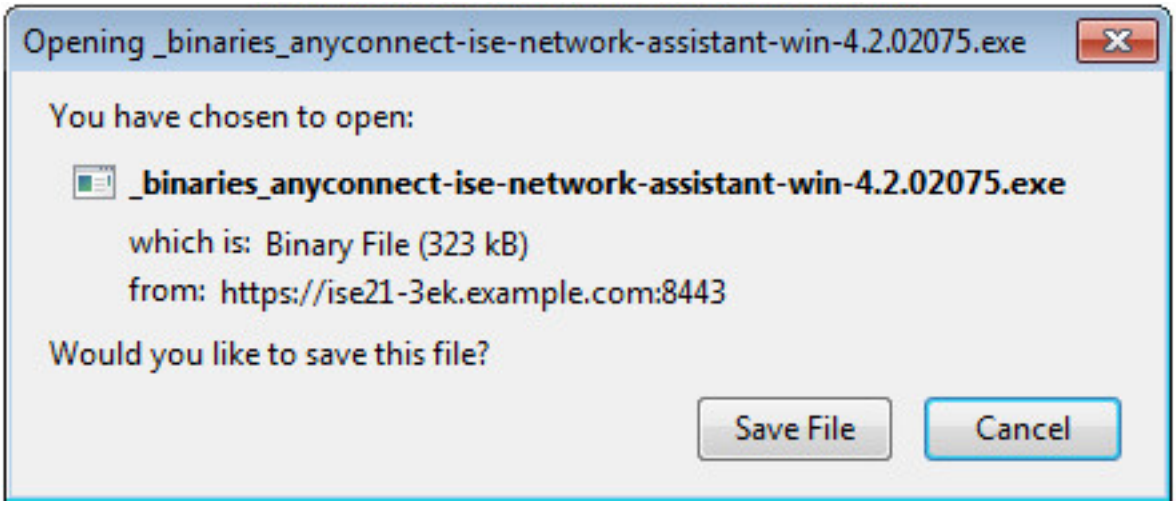
Nach dem Herstellen der Verbindung erfolgt die Umleitung zum Client Provisioning Portal.



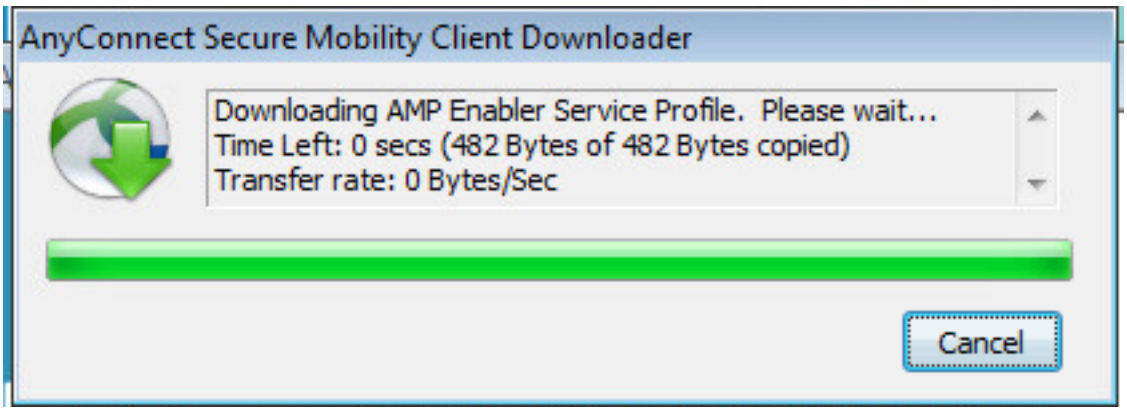
Da auf dem Client-Computer nichts installiert ist, fordert die ISE zur Installation des AnyConnect-Clients auf.

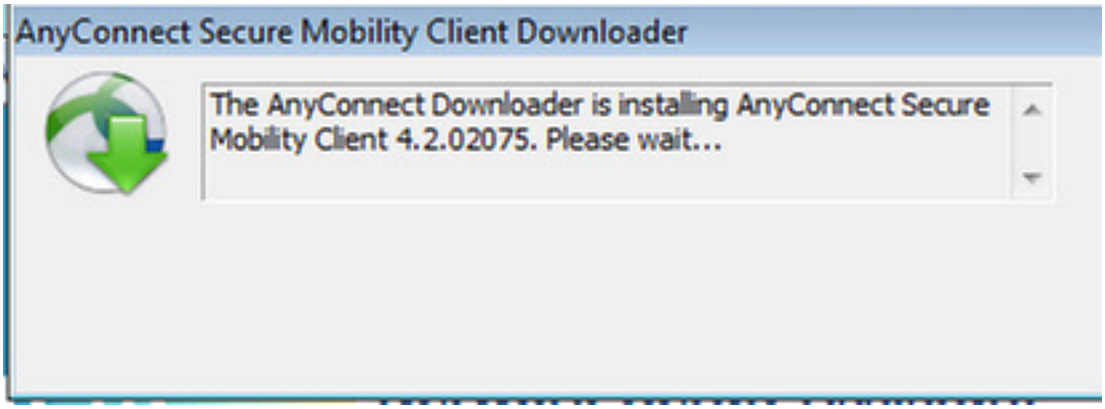


Die NSA-Anwendung (Network Setup Assistant) sollte vom Client-Computer heruntergeladen und ausgeführt werden.

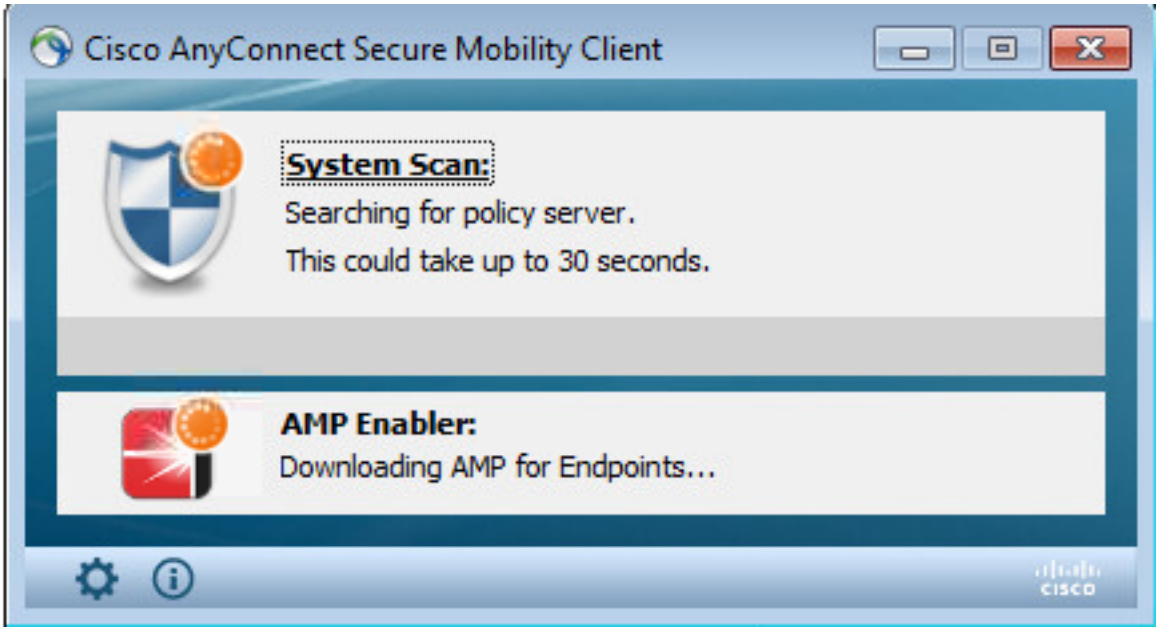


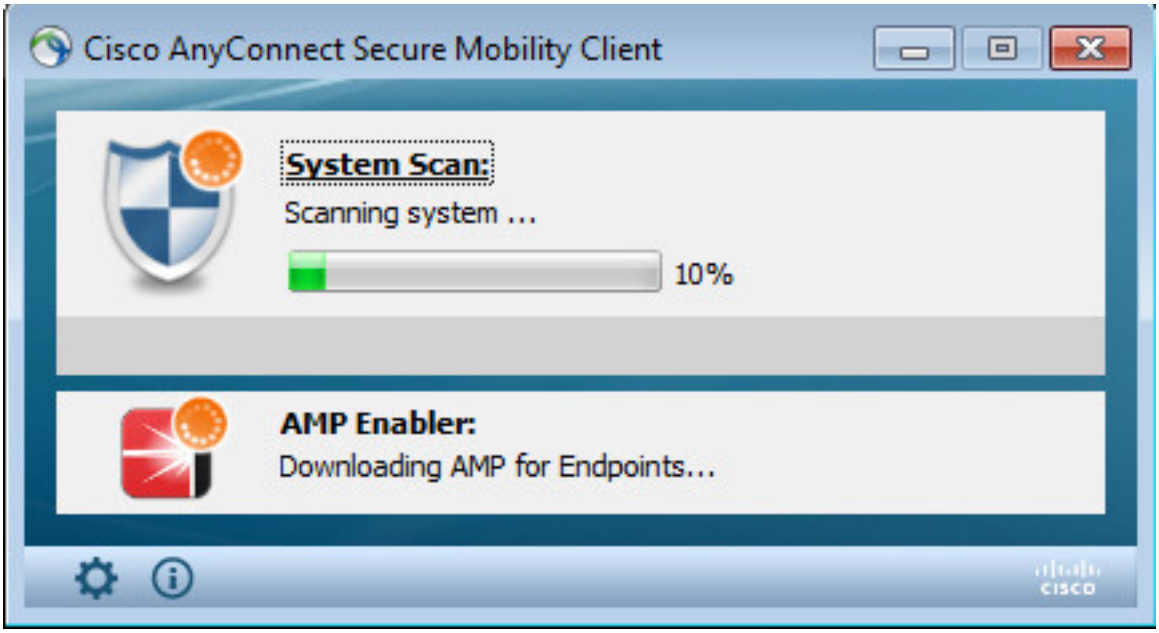
Die NSA übernimmt die Installation der erforderlichen Komponenten und Profile.



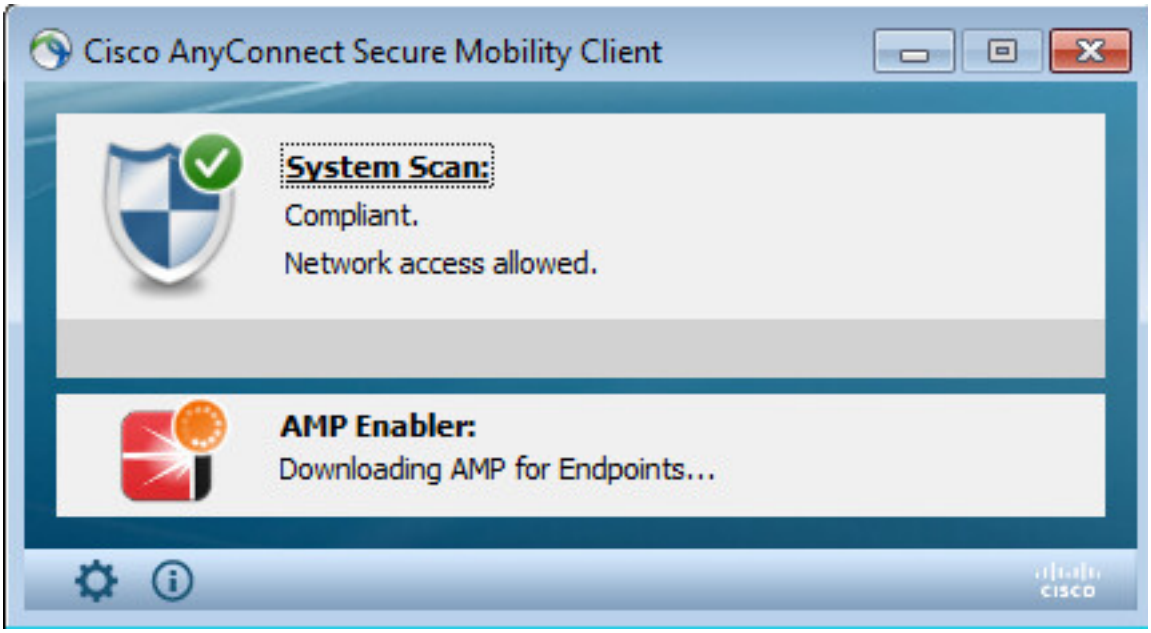


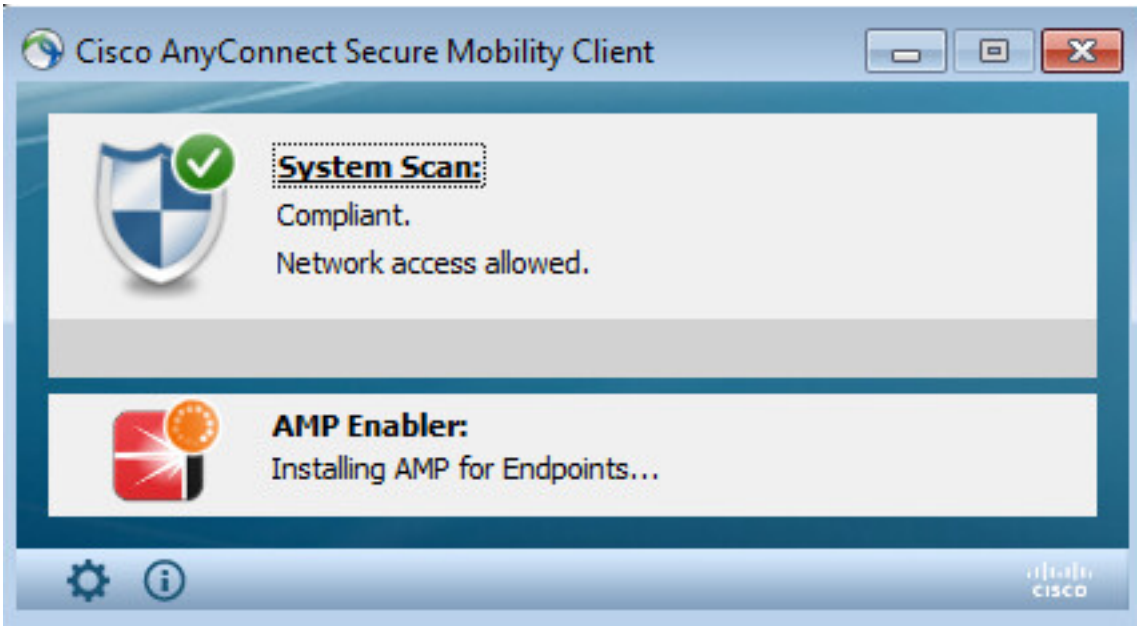
Nach Abschluss der Installation führt das AnyConnect Posture-Modul eine Compliance-Prüfung durch.

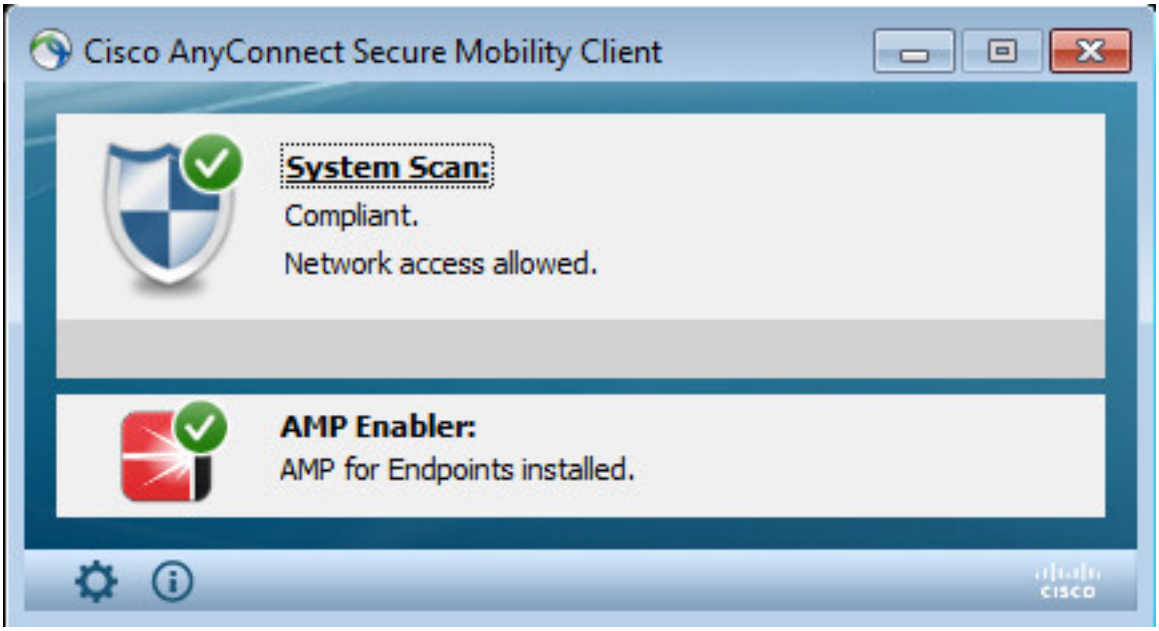




Wenn ein Endpunkt den Vorgaben entspricht, wird AMP über den zuvor im AMP-Profil angegebenen Webserver heruntergeladen und installiert.

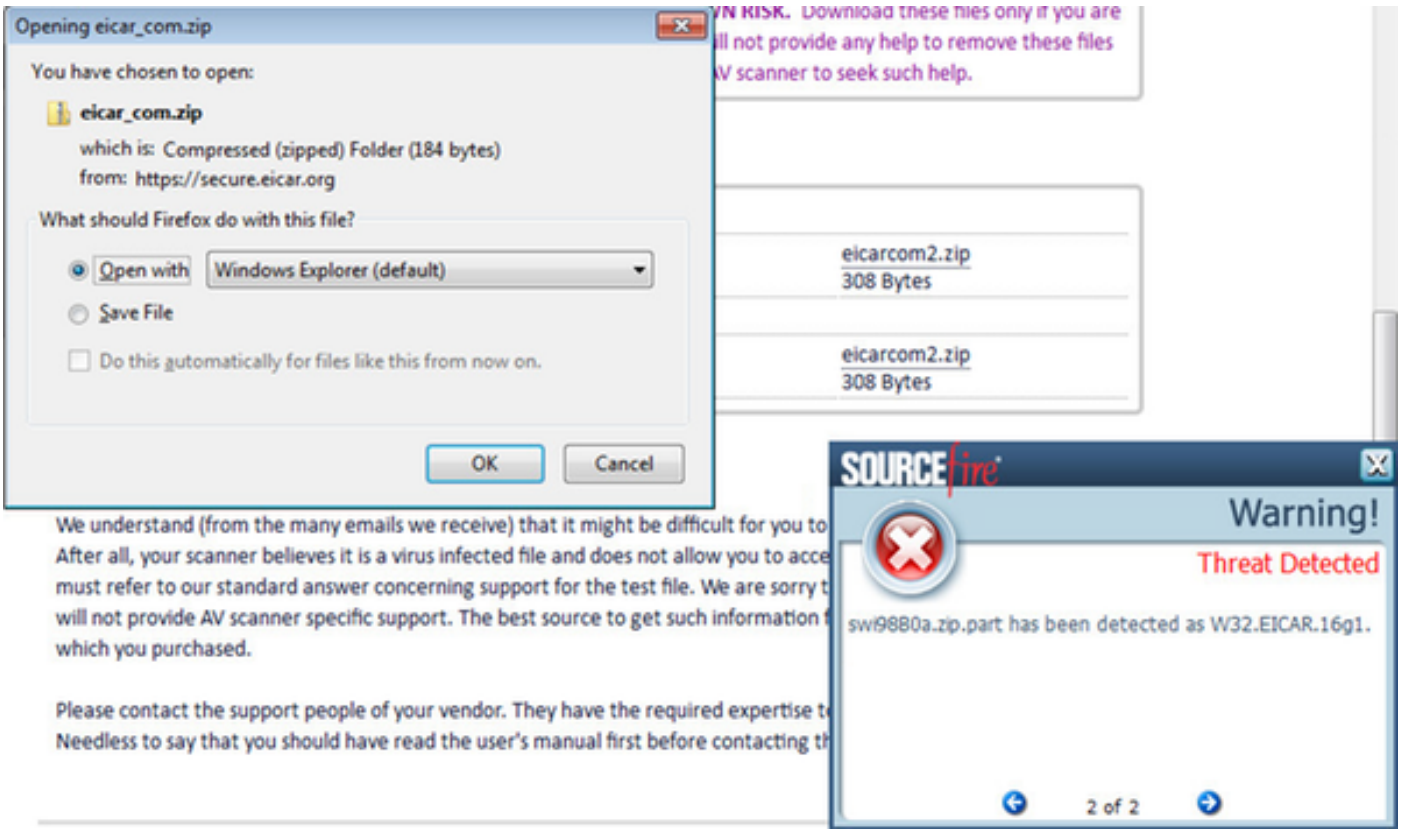






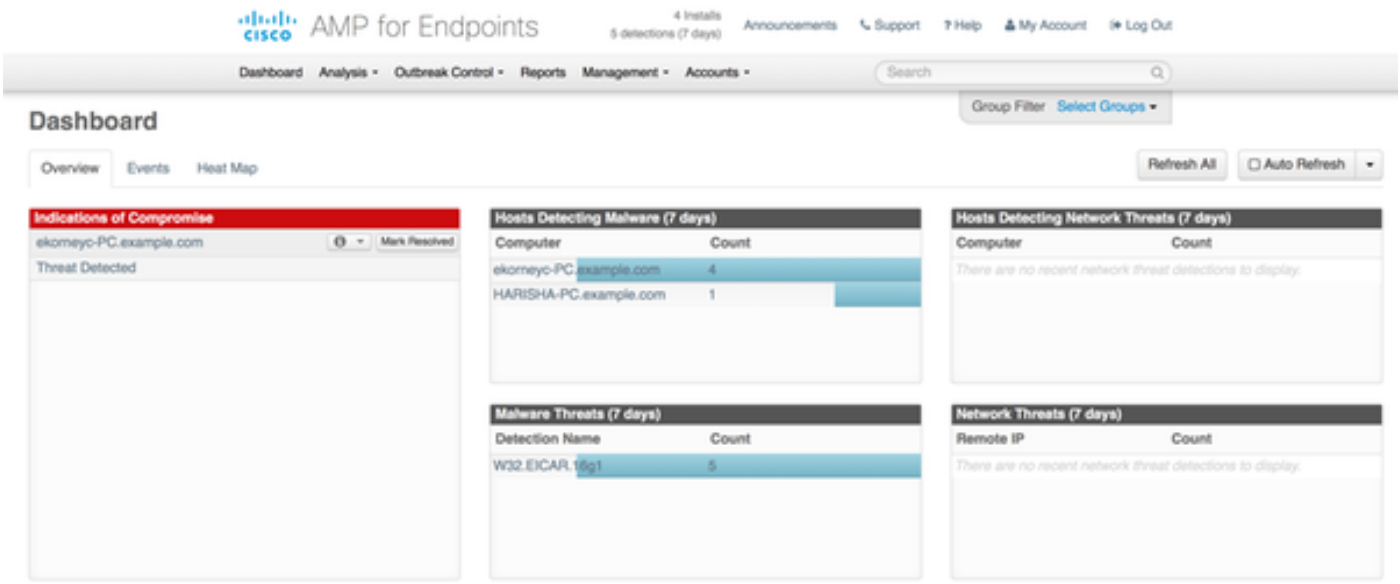
AMP Connector wird angezeigt.

Um AMP in Aktion zu testen, wird die in einer ZIP-Datei enthaltene Eicar-Zeichenfolge heruntergeladen. Die Bedrohung wird erkannt und an die AMP Cloud gemeldet.

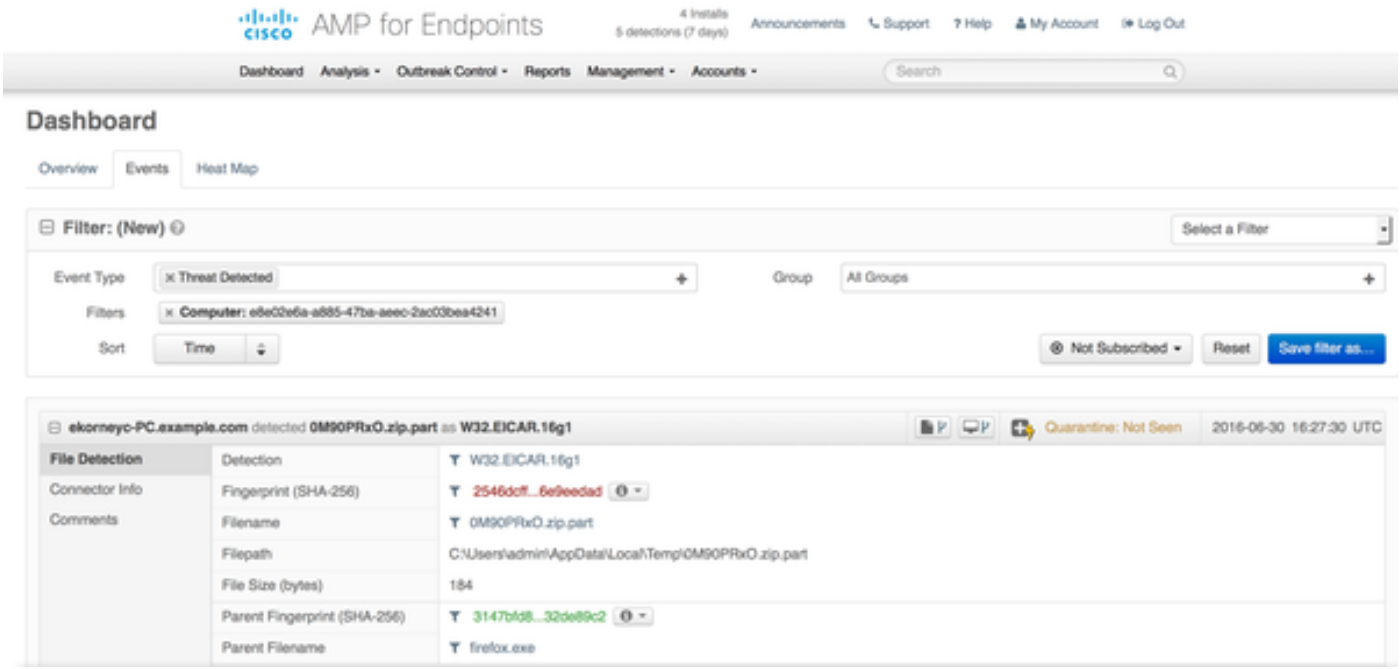


AMP-Cloud

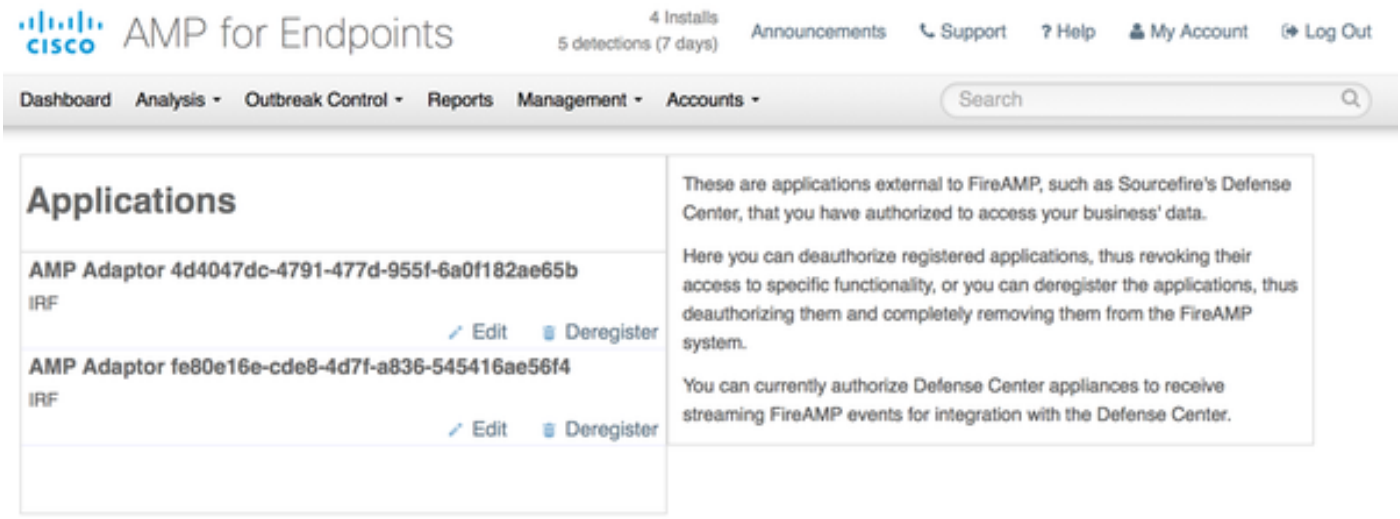
Die Details des Threat Dashboards der AMP-Cloud können überprüft werden.



Um weitere Informationen zu Bedrohung, Filepath und Fingerpints zu erhalten, können Sie auf den Host klicken, auf dem Malware erkannt wurde.

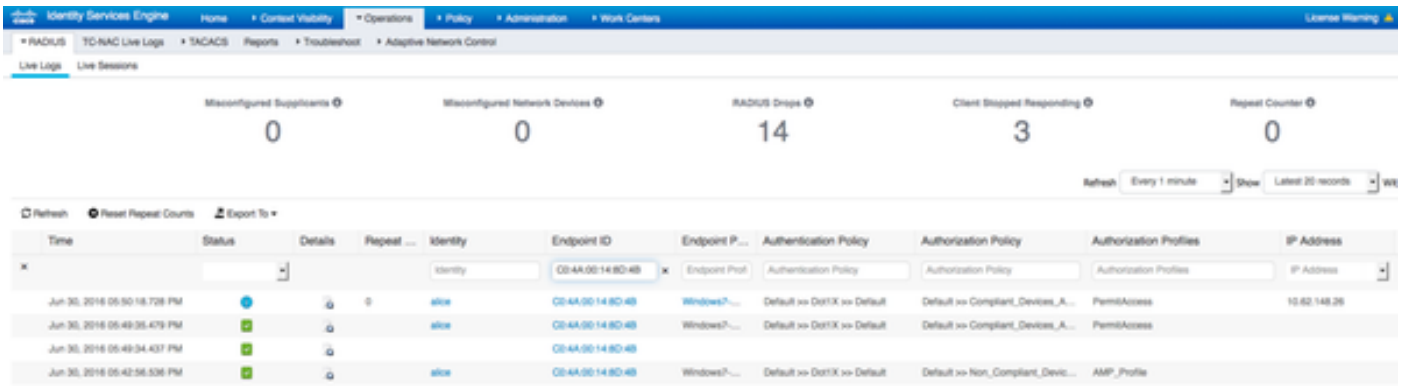


Um die ISE-Instanz anzuzeigen oder zu deaktivieren, können Sie zu Konten > Anwendungen navigieren.

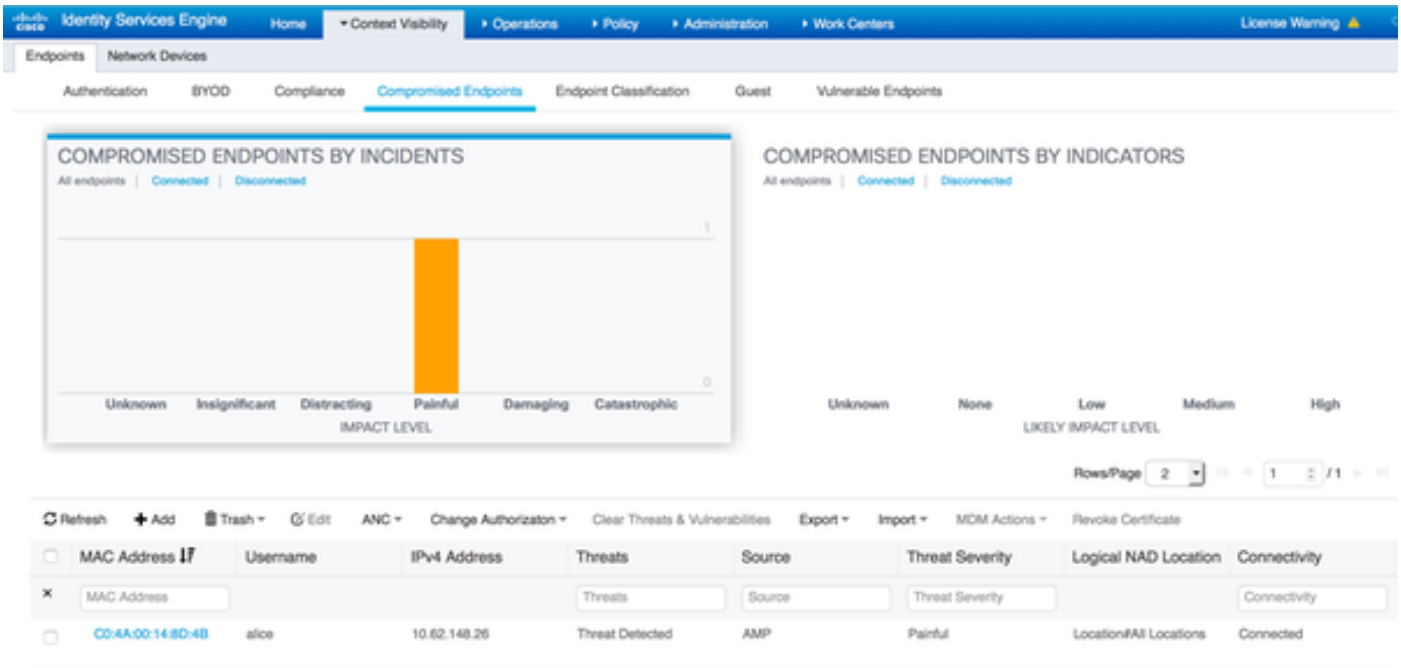


ISE

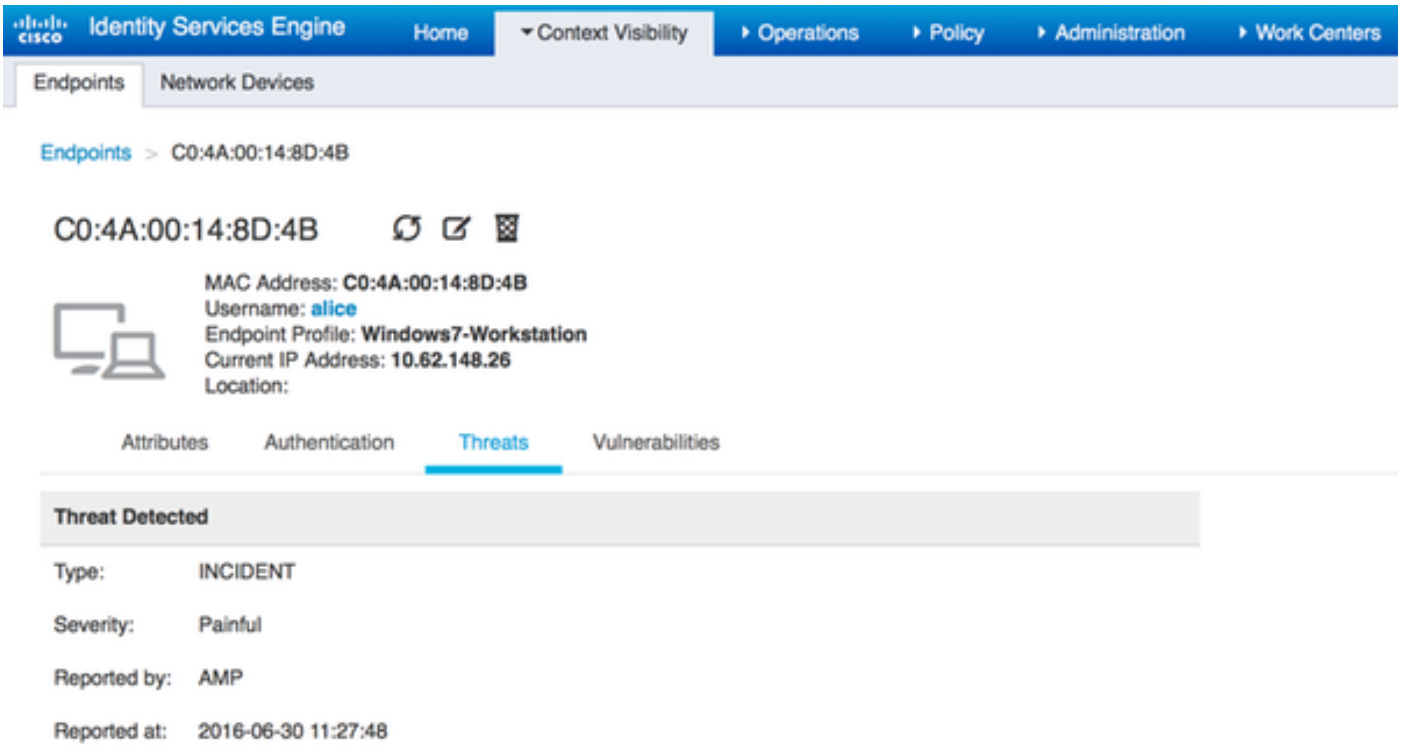
Bei der ISE selbst wird ein regelmäßiger Status-Flow erkannt. Die Umleitung erfolgt zuerst, um die Einhaltung der Netzwerkrichtlinien zu überprüfen. Sobald der Endpunkt kompatibel ist, wird CoA-Authentifizierung gesendet und ein neues Profil mit PermitAccess zugewiesen.



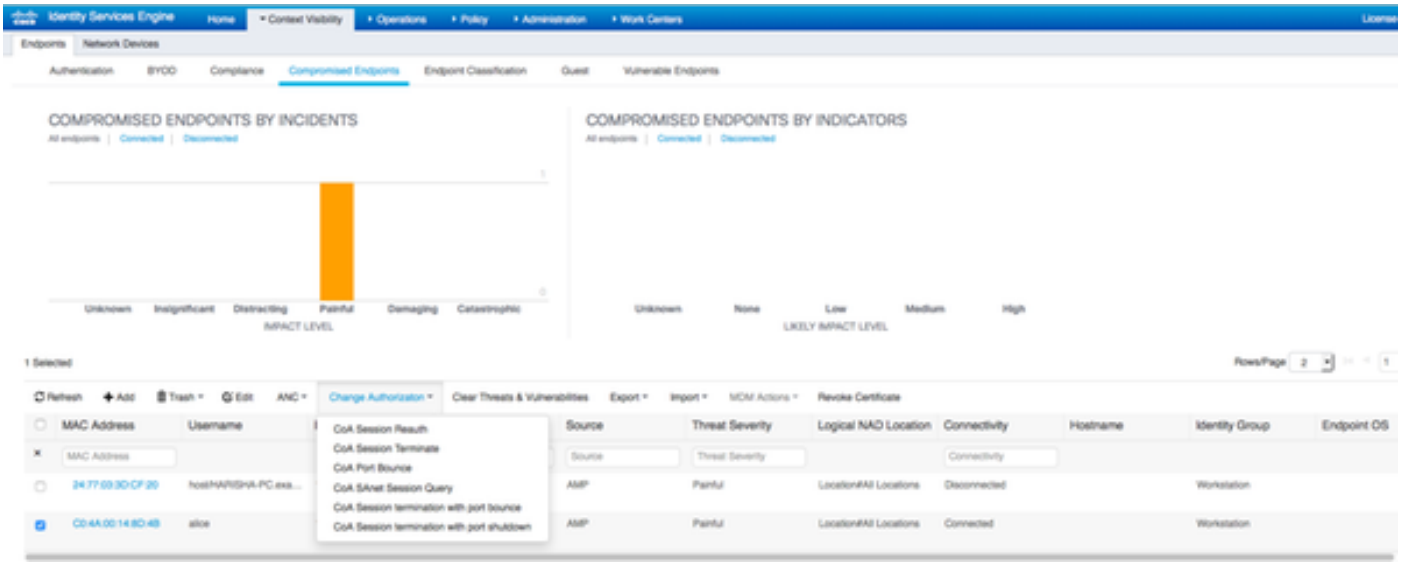
Um die erkannten Bedrohungen anzuzeigen, navigieren Sie zu Context Visibility > Endpoints > Compromise Endpoints.



Wenn Sie den Endpunkt auswählen und zur Registerkarte "Bedrohung" navigieren, werden weitere Details angezeigt.



Wenn ein Bedrohungsereignis für einen Endpunkt erkannt wird, können Sie die MAC-Adresse des Endpunkts auf der Seite "Kompromittierte Endgeräte" auswählen und eine ANC-Richtlinie anwenden (sofern konfiguriert, z. B. Quarantäne). Alternativ können Sie Change of Authorization (Autorisierungsänderung) ausgeben, um die Sitzung zu beenden.



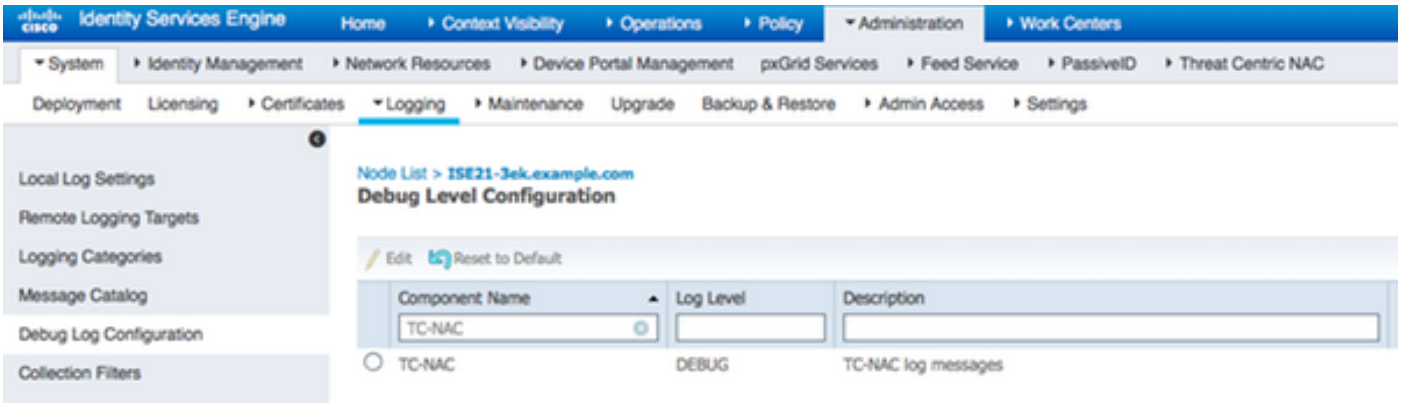
Wenn CoA Session Terminate ausgewählt ist, sendet die ISE CoA Disconnect, und der Client verliert den Zugriff auf das Netzwerk.

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

Fehlerbehebung

Um das Debuggen auf der ISE zu aktivieren, navigieren Sie zu Administration > System > Logging > Debug Log Configuration, wählen Sie TC-NAC Node aus, und ändern Sie die **Protokollstufe** der TC-NAC-Komponente in **DEBUG.**



Protokolle zu überprüfen - irf.log. Sie können sie direkt über die ISE-CLI entfernen:

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

Die AMP-Cloud bietet sogar eine Bedrohung

2016-06-30 18:27:48,617 DEBUG [IRF-AMQP-Dispatcher-Notification-0][]
cisco.cpm.irf.amqp.NotificationDispatcher:processDelivery:53 -::::- call notification handler
com.cisco.cpm irf.service.IrfNotificationHandler$MyNotificationHandler@3fac8043
Message{messageType=NOTIFICATION, messageId=THREAT_EVENT, content='{"**c0:4a:00:14:8d:4b**":
[{"Vorfall": {"Impact_Qualification": "Schmerzhaft"}, "Zeitstempel": 1467304068599, "Anbieter":
"AMP", "Titel": "**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.bedroht), amqqqqql pProperties=#contentHeader<basic>(content-
type=application/json, content-encoding=null, headers=null, Delivery-mode=null, priority=0,
Korrelations-id=null, reply-to=null, expiration=null, message-id=THREAT_EVENT, timestamp=null,
type=NOTIFICATION, user-id=null, app-id=fe80e 16e-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 -::::- Zur ausstehenden Warteschlange
hinzugefügt: Message{messageType=NOTIFICATION, messageId=THREAT_EVENT,
content='{"**c0:4a:00:14:8d:4b**": [{"Vorfall": {"Impact_Qualification": "**Schmerzhaft**"},
"Zeitstempel": 1467304068599, "Anbieter": "**AMP**", "Titel": "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.bedroht), amqpProperties#1
contentHeader<basic>(content-type=application/json, content-encoding=null, headers=null,
delivery-mode=null, priority=0, Korrelations-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 -::::-
Verarbeitungsbenachrichtigung: Umschlag(deliveryTag=79, redeliver=false,
exchange=irf.topic.events, routingKey=irf.events.bedroht) #contentHeader<basic>(content-
type=application/json, content-encoding=null, headers=null, Delivery-mode=null, priority=0,
Korrelations-id=null, reply-to=null, expiration=msid=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 -::::::- Analyse-Benachrichtigung:
Message{messageType=NOTIFICATION, messageId=THREAT_EVENT, content='{"c0:4a:00:14:8d:4b":
[{"Vorfall": {"Impact_Qualification": "Schmerzhaft"}, "Zeitstempel": 1467304068599, "Anbieter":
"AMP", "Titel": "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.bedroht), amqpProperties#1 contentHeader<basic>(content-
type=application/json, content-encoding=null, headers=null, delivery-mode=null, priority=0,
Korrelations-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)}

Informationen über die Bedrohung werden an den PAN gesendet

2016-06-30 18:27:48.724 DEBUG [IRF-EventProcessor-0][]
cisco.cpm.irf.service.IrfEventProcessor:storeEventsInES:366 -::::- **Hinzufügen von Informationen zum Bedrohungsereignis zum Senden an PAN - c0:4a:00:14:8d:4b**
{Incident={Impact_Qualification=Painful}, Zeitstempel=1467304068599, vendor=AMP, title=Threat
Detected}