

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-Profiles](#)

[Schritt 3: Konfigurieren des AMP-Profiles](#)

[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.

The screenshot shows the 'AMP for Endpoints' management console. At the top, there's a navigation bar with 'Dashboard', 'Analysis', 'Outbreak Control', 'Reports', 'Management', and 'Accounts'. A search bar is on the right. The main heading is 'Download Connector'. Below it, a 'Group' dropdown menu is set to 'Audit'. There are four connector options:

- FireAMP Windows** (Audit): No computers require updates. Audit Policy settings: Flash Scan on Install (checked), Redistributable (checked). Buttons: Show URL, Download.
- FireAMP Mac**: Audit Policy for FireAMP Mac. Flash Scan on Install (checked). Buttons: Show URL, Download.
- FireAMP Linux**: Audit Policy for FireAMP Li... Flash Scan on Install (checked). Buttons: Show GPG Public Key, Show URL, Download.
- FireAMP Android**: Default FireAMP Android. Activation Codes. Buttons: Show URL, Download.

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:

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionarys Conditions Results

File Conditions List > File_Condition

File Condition

* Name:

Description:

* Operating System:

Compliance Module: Any version

* File Type: ⓘ

* File Path: ⓘ

* File Operator:

- Authentication
- Authorization
- Profiling
- Posture
 - Anti-Malware Condition
 - Anti-Spyware Condition
 - Anti-Virus Condition
 - Application Condition
 - Compound Condition
 - Disk Encryption Condition
 - File Condition
 - Patch Management Condition
 - Registry Condition
 - Service Condition
 - USB Condition
 - Dictionary Simple Condition
 - Dictionary Compound Condition
- Guest
- Common

Diese Bedingung wird für eine Anforderung verwendet:

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionarys Conditions Results

Requirements

Name	Operating Systems	Compliance Module	Conditions	Remediation Actions
Any_AV_Installation_Win	for Windows All	using 3.x or earlier	met if ANY_av_win_inst	then Message Text Only
File_Requirement	for Windows All	using Any version	met if File_Condition	then Message Text Only
Any_AV_Definition_Win	for Windows All	using 3.x or earlier	met if ANY_av_win_def	then AnyAVDefRemediationWin
Any_AM_Installation_Mac	for Mac OSX	using 4.x or later	met if ANY_am_mac_inst	then Message Text Only
Any_AS_Installation_Win	for Windows All	using 3.x or earlier	met if ANY_as_win_inst	then Message Text Only
Any_AS_Definition_Win	for Windows All	using 3.x or earlier	met if ANY_as_win_def	then AnyASDefRemediationWin
Any_AV_Installation_Mac	for Mac OSX	using 3.x or earlier	met if ANY_av_mac_inst	then Message Text Only
Any_AV_Definition_Mac	for Mac OSX	using 3.x or earlier	met if ANY_av_mac_def	then AnyAVDefRemediationMac
Any_AS_Installation_Mac	for Mac OSX	using 3.x or earlier	met if ANY_as_mac_inst	then Message Text Only
Any_AS_Definition_Mac	for Mac OSX	using 3.x or earlier	met if ANY_as_mac_def	then AnyASDefRemediationMac
Any_AM_Installation_Win	for Windows All	using 4.x or later	met if ANY_am_win_inst	then Message Text Only
Any_AM_Definition_Win	for Windows All	using 4.x or later	met if ANY_am_win_def	then AnyAMDefRemediationWin
Any_AM_Definition_Mac	for Mac OSX	using 4.x or later	met if ANY_am_mac_def	then AnyAMDefRemediationMac
USB_Block	for Windows All	using 4.x or later	met if USB_Check	then USB_Block

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

Status	Rule Name	Identity Groups	Operating Systems	Compliance Module	Other Conditions	Requirements
<input checked="" type="checkbox"/>	Windows_Posture	Any	and Windows All	and Any version	and	then File_Requirement

Schritt 2: Konfigurieren des Status-Profiles

- 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

ISE Posture Agent Profile Settings > **New Profile**

Posture Agent Profile Settings

AnyConnect

* Name: AC Posture Profile

Description:

Agent Behavior

Parameter	Value	Notes
PRA retransmission time	120 secs	
Discovery host		
* Server name rules	*	need to be blank by default to force admin to enter a value. "*" means agent will connect to all

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

Posture Protocol

Parameter	Value	Notes
PRA retransmission time	120 secs	
Discovery host		
* Server name rules	*	need to be blank by default to force admin to enter a value. "*" means agent will connect to all

Schritt 3: Konfigurieren des AMP-Profiles

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.

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The breadcrumb trail is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Policy Elements > Client Provisioning > Results. The left sidebar shows a navigation menu with 'Client Provisioning' selected. The main content area is titled 'AMP Enabler Profile Settings > New Profile' and 'AMP Enabler Profile'. It contains the following fields and options:

- * Name: AMP Profile
- Description: (empty field)
- Install AMP Enabler Uninstall AMP Enabler
- Windows Installer: [https://win2012ek.example.com/Downloads/Audit_FireAMPSetup.](https://win2012ek.example.com/Downloads/Audit_FireAMPSetup)
- MAC Installer: <https://>
- Windows Settings:
 - Add to Start Menu
 - Add to Desktop
 - Add to Context Menu
- Buttons: Submit, Cancel

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**

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The navigation path is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Authentication > Authorization > Profiling > Posture > Client Provisioning > Policy Elements > Results. The main content area is titled 'Agent Resources From Local Disk' and shows a configuration form. The 'Category' dropdown is set to 'Cisco Provided Packages'. Below it, a 'Browse...' button is followed by the filename 'anyconnect-win-4.2.02075-k9.pkg'. A table titled 'AnyConnect Uploaded Resources' is visible, with the following data:

Name	Type	Version	Description
AnyConnectDesktopWindows 4.2.207...	AnyConnectDesktopWindows	4.2.2075.0	AnyConnect Secure Mobility Clie...

At the bottom of the form, there are 'Submit' and 'Cancel' buttons.

- 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.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The navigation path is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Authentication > Authorization > Profiling > Posture > Client Provisioning > Policy Elements > Results. The main content area is titled 'Agent Resources From Local Disk' and shows a configuration form. The 'Category' dropdown is set to 'Customer Created Packages'. The 'Type' dropdown is set to 'AnyConnect Profile'. The '* Name' field contains 'VPNDisable_ServiceProfile'. The 'Description' field is empty. Below it, a 'Browse...' button is followed by the filename 'VPNDisable_ServiceProfile.xml'. At the bottom of the form, there are 'Submit' and 'Cancel' buttons.

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**.

Download Remote Resources ✕

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	AgentCustomizationPackage 1.1.1.6	This is the NACAgent Customization Package v1.1.1.6 for Windows
<input type="checkbox"/>	AnyConnectComplianceModuleOSX 3.6.10591.2	AnyConnect OS X Compliance Module 3.6.10591.2
<input checked="" type="checkbox"/>	AnyConnectComplianceModuleWindows 3.6.10591.2	AnyConnect Windows Compliance Module 3.6.10591.2
<input type="checkbox"/>	ComplianceModule 3.6.10591.2	NACAgent ComplianceModule v3.6.10591.2 for Windows
<input type="checkbox"/>	MACComplianceModule 3.6.10591.2	MACAgent ComplianceModule v3.6.10591.2 for MAC OSX
<input type="checkbox"/>	MacOsXAgent 4.9.0.1006	NAC Posture Agent for Mac OSX (ISE 1.2 release)
<input type="checkbox"/>	MacOsXAgent 4.9.0.1007	NAC Posture Agent for Mac OSX v4.9.0.1007 (with CM 3.6.7873.2)- ISE
<input type="checkbox"/>	MacOsXAgent 4.9.0.655	NAC Posture Agent for Mac OSX (ISE 1.1.1 or later)
<input type="checkbox"/>	MacOsXAgent 4.9.0.661	NAC Posture Agent for Mac OS X v4.9.0.661 with CM v3.5.7371.2 (ISE
<input type="checkbox"/>	MacOsXAgent 4.9.4.3	NAC Posture Agent for Mac OSX v4.9.4.3 - ISE 1.2 , ISE 1.1.3 and Abov
<input type="checkbox"/>	MacOsXAgent 4.9.5.3	NAC Posture Agent for Mac OSX v4.9.5.3 - ISE 1.2 Patch 12, ISE 1.3 rel
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.18	Supplicant Provisioning Wizard for Mac OsX 1.0.0.18 (ISE 1.1.3 Release)
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.21	Supplicant Provisioning Wizard for Mac OsX 1.0.0.21 (for ISE 1.2 release
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.27	Supplicant Provisioning Wizard for Mac OsX 1.0.0.27 (for ISE 1.2 release
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.29	Supplicant Provisioning Wizard for Mac OsX 1.0.0.29 (for ISE 1.2 release
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.30	Supplicant Provisioning Wizard for Mac OsX 1.0.0.30 (for ISE 1.2 Patch
<input type="checkbox"/>	MacOsXSPWizard 1.0.0.36	Supplicant Provisioning Wizard for Mac OsX 1.0.0.36 (for ISE 1.2 Patch

For AnyConnect software, please download from <http://cisco.com/go/anyconnect>. Use the "Agent resource from local disk" add option, to import into ISE

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.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionary Conditions Results

Authentication

Authorization

Profiling

Posture

Client Provisioning

Resources

AnyConnect Configuration > AnyConnect Configuration AMP

* Select AnyConnect Package: AnyConnectDesktopWindows 4.2.2075.0

* Configuration Name: AnyConnect Configuration AMP

Description:

DescriptionValue

* Compliance Module: AnyConnectComplianceModuleWindows 3.6.10591.2

AnyConnect Module Selection

ISE Posture

VPN

Network Access Manager

Web Security

AMP Enabler

ASA Posture

Network Visibility

Start Before Logon

Diagnostic and Reporting Tool

Profile Selection

* ISE Posture: AC Posture Profile

VPN: VPNDisable_ServiceProfile

Network Access Manager

Web Security

AMP Enabler: AMP Profile

Network Visibility

Customer Feedback

Schritt 5: Konfigurieren von Client-Bereitstellungsregeln

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

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Client Provisioning Policy

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
 For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
 For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
<input checked="" type="checkbox"/> Windows_Posture_AMP	If Any	and Windows All	and Condition(s)	then AnyConnect Configuration AMP

Schritt 6: Autorisierungsrichtlinien konfigurieren

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

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionarys Conditions Results

Authentication

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

Authorization Profiles > AMP_Profile

Authorization Profile

* Name AMP_Profile

Description

* Access Type ACCESS_ACCEPT

Network Device Profile Cisco

Service Template

Track Movement

Passive Identity Tracking

Common Tasks

Web Redirection (CWA, MDM, NSP, CPP)

Client Provisioning (Posture) ACL ACL_WEBAUTH_REDIRECT Value Client Provisioning Portal (defa

Display Certificates Renewal Message

Static IP/Host name/FQDN

Advanced Attributes Settings

Select an item =

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

Authorization Policy

Define the Authorization Policy by configuring rules based on Identity groups and/or other conditions. Drag and drop rules to change the order. For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

First Matched Rule Applies

Exceptions (1)

Standard

Status	Rule Name	Conditions (Identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Wireless Black List Default	if Blacklist AND Wireless_Access	then Blackhole_Wireless_Access
<input checked="" type="checkbox"/>	Profiled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones
<input checked="" type="checkbox"/>	Profiled Non Cisco IP Phones	if Non_Cisco_Profiled_Phones	then Non_Cisco_IP_Phones
2. <input checked="" type="checkbox"/>	Compliant_Devices_Access	if (Network_Access_Authentication_Passed AND Compliant_Devices)	then PermitAccess
1. <input checked="" type="checkbox"/>	Non_Compliant_Devices_Access	if Session:PostureStatus NOT_EQUALS Compliant	then AMP_Profile
<input type="checkbox"/>	Employee_EAP-TLS	if (Wireless_802.1X AND BYOD_is_Registered AND EAP-TLS AND MAC_in_SAN)	then PermitAccess AND BYOD
<input type="checkbox"/>	Employee_Onboarding	if (Wireless_802.1X AND EAP-MSCHAPv2)	then NSP_Onboard AND BYOD
<input checked="" type="checkbox"/>	Wi-Fi_Guest_Access	if (Guest_Flow AND Wireless_MAB)	then PermitAccess AND Guests
<input checked="" type="checkbox"/>	Wi-Fi_Redirect_to_Guest_Login	if Wireless_MAB	then Cisco_WebAuth
<input checked="" type="checkbox"/>	Basic_Authenticated_Access	if Network_Access_Authentication_Passed	then VA_Scan
<input checked="" type="checkbox"/>	Default	if no matches, then	DenyAccess

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.

Deployment Nodes List > ISE21-3ek

Edit Node

General Settings Profiling Configuration

Hostname **ISE21-3ek**
 FQDN **ISE21-3ek.example.com**
 IP Address **10.62.145.25**
 Node Type **Identity Services Engine (ISE)**

Personas

- Administration Role **STANDALONE** Make Primary
- Monitoring Role **PRIMARY** Persons Other Monitoring Node
- Policy Service
 - Enable Session Services i Include Node in Node Group **None** i
 - Enable Profiling Service
 - Enable Threat Centric NAC Service i

Schritt 8: Konfigurieren des AMP-Adapters

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

Identity Services Engine Administration Work Centers
System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service PassiveID Threat Centric NAC

Third Party Vendors

Vendor Instances > New
Input fields marked with an asterisk (*) are required.

Vendor * AMP : THREAT

Instance Name * AMP_THREAT

Cancel Save

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

Identity Services Engine Administration Work Centers
System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service PassiveID Threat Centric NAC

Third Party Vendors

Vendor Instances
0 Selected

Refresh Add Trash Edit Filter Settings

<input type="checkbox"/>	Instance Name	Vendor Na...	Type	Hostname	Connectivity	Status
<input type="checkbox"/>	QualysVA	Qualys	VA	qualysguard.qg2.apps.qualys.com	Connected	Active
<input type="checkbox"/>	AMP_THREAT	AMP	THREAT		Disconnected	Ready to configure

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

Identity Services Engine Administration Work Centers
System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service PassiveID Threat Centric NAC

Third Party Vendors

Vendor Instances > AMP

Cloud
US Cloud

Which public cloud would you like to connect to

Cancel Next

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

Third Party Vendors

Vendor Instances > AMP

root

SAS External URL

Please click on the link below to open an external web page. Login as admin and approve the registration to complete configuration. You will be redirect back into IRF upon approval

https://api.amp.sourcefire.com/authorize?client_id=mbga79xvh3tq7aafywt7yhsb90ktz5p&response_type=code&redirect_uri=https://ise21-3ek.example.com/admin/vrfapi/62f6204b-751f-4ef5-9d93-e9f02500d842/authorize&scope=recv_events

Cancel

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

Applications

The AMP Adaptor 62f6204b-751f-4ef5-9d93-e9f02500d842 (IRF) Defense Center with URL of https://ise21-3ek.example.com/admin/vrfapi/62f6204b-751f-4ef5-9d93-e9f02500d842/authorize, is requesting the following authorizations:

Streaming event export.

Allow Deny

Event Export Groups All groups selected.

If you are going to authorize the request, please select which groups will have their events exported to this application:

Allow Deny

Applications external to FireAMP, such as Sourcefire's Defense Center, can be authorized to access your business' data.

Here an application is asking for your authorization to gain access to some specific services. Review the requested authorizations and approve or deny the request as appropriate.

Deny the request if you don't recognize the application or you did not initiate this request for integration from the application.

Authorization can always be revoked at a later time from the FireAMP web console, and the application completely deregistered from the system.

Search Groups

- Audit**
Audit Group for Cisco - ekomeyc
- Domain Controller**
Domain Controller Group for Cisco - ekomeyc
- Protect**
Protect Group for Cisco - ekomeyc
- Server**
Server Group for Cisco - ekomeyc
- Triage**

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.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service PassiveID Threat Centric NAC

Third Party Vendors

Vendor Instances

0 Selected

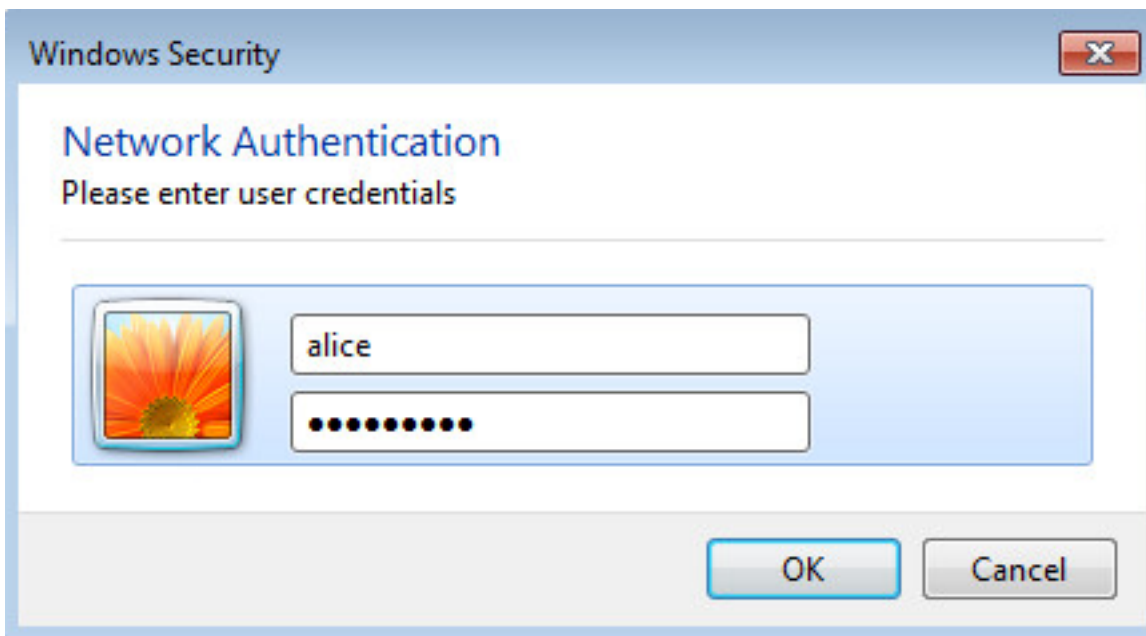
Refresh Add Trash Edit Filter Settings

Instance Name	Vendor Name	Type	Hostname	Connectivity	Status
AMP_THREAT	AMP	THREAT	https://api.amp.sourcefire.com	Connected	Active
QUALYS_VA	Qualys	VA	qualysguard.qg2.apps.qualys.com	Connected	Active

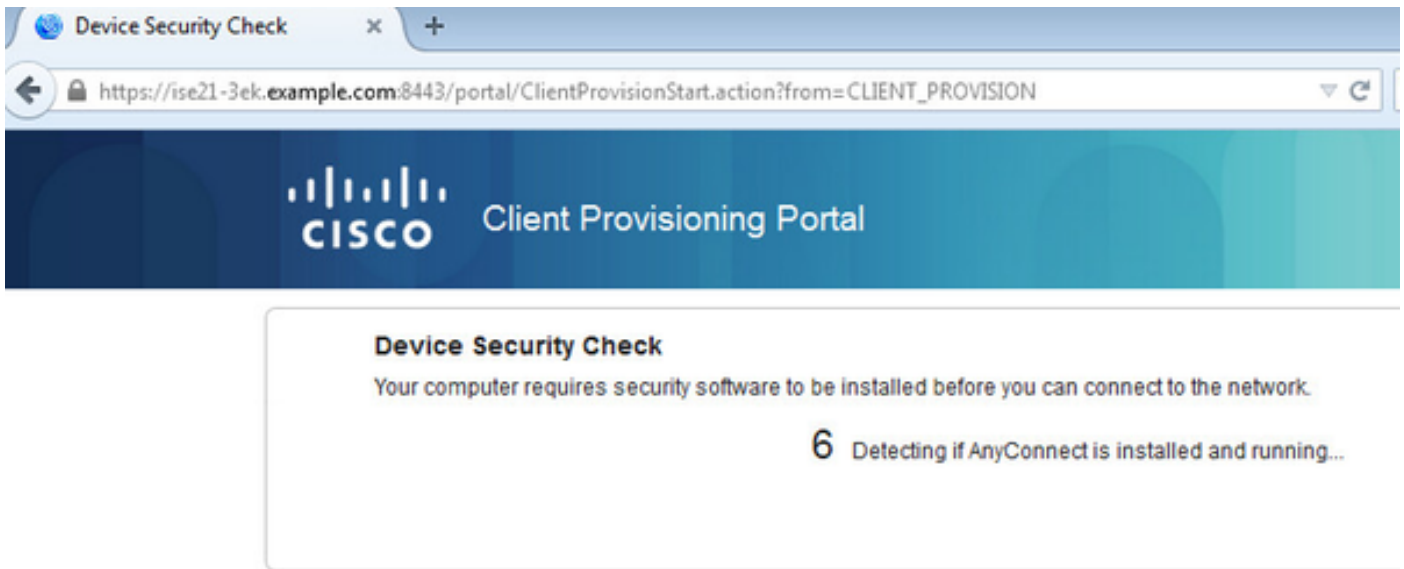
Überprüfen

Endpunkt

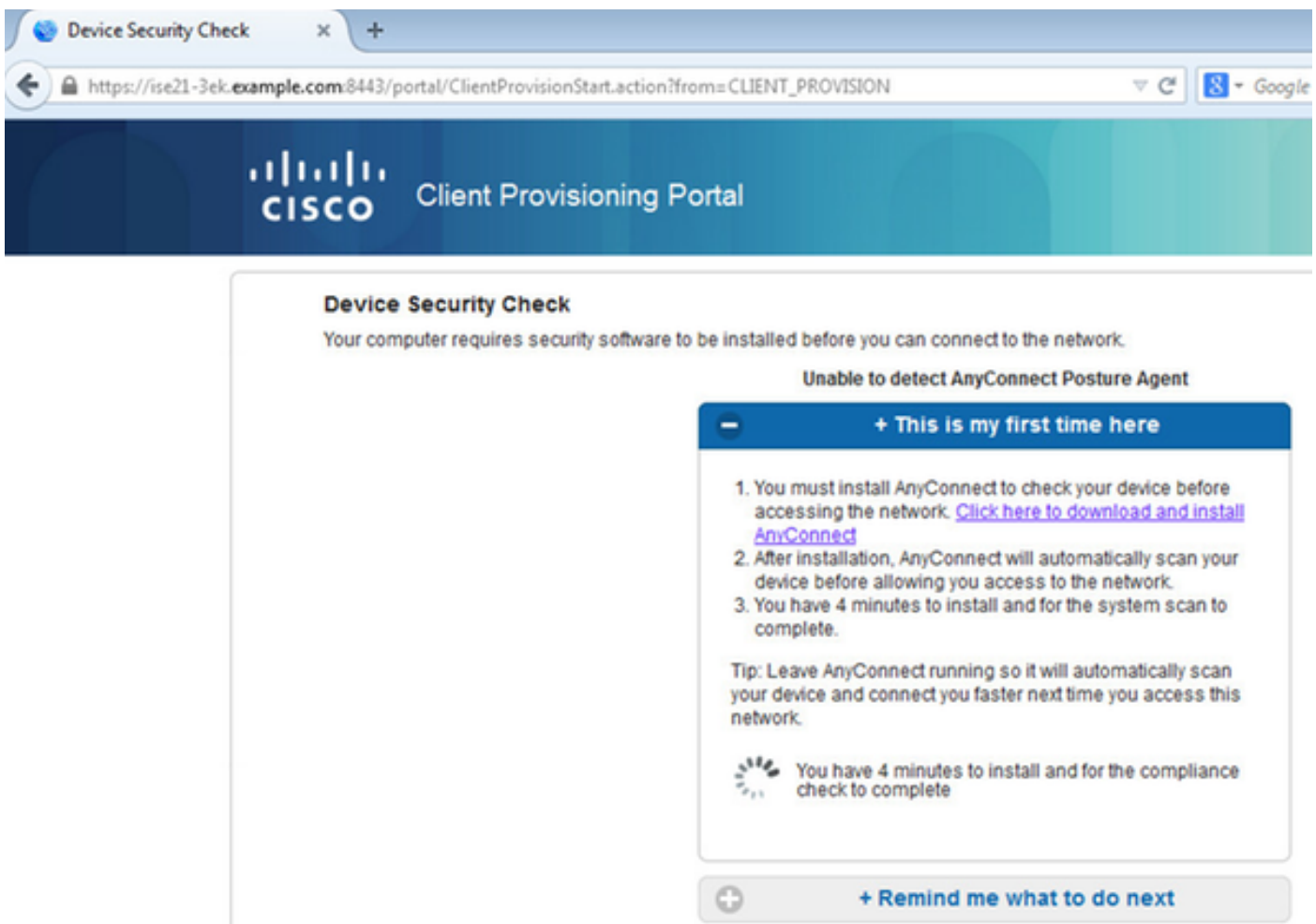
Herstellen einer Verbindung zum Wireless-Netzwerk über PEAP (MSCHAPv2).



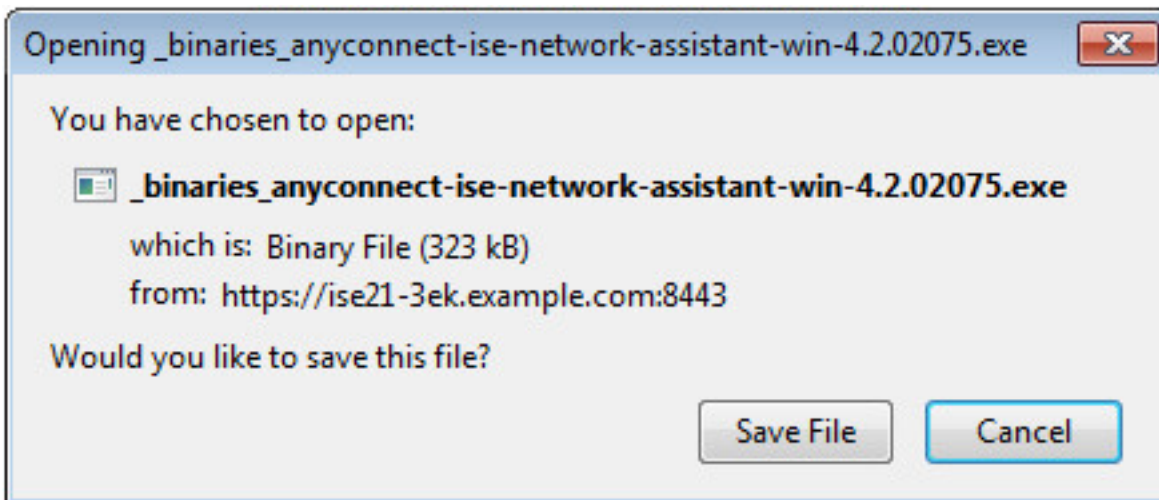
Nach dem Herstellen der Verbindung erfolgt die Umleitung zum Client Provisioning Portal.



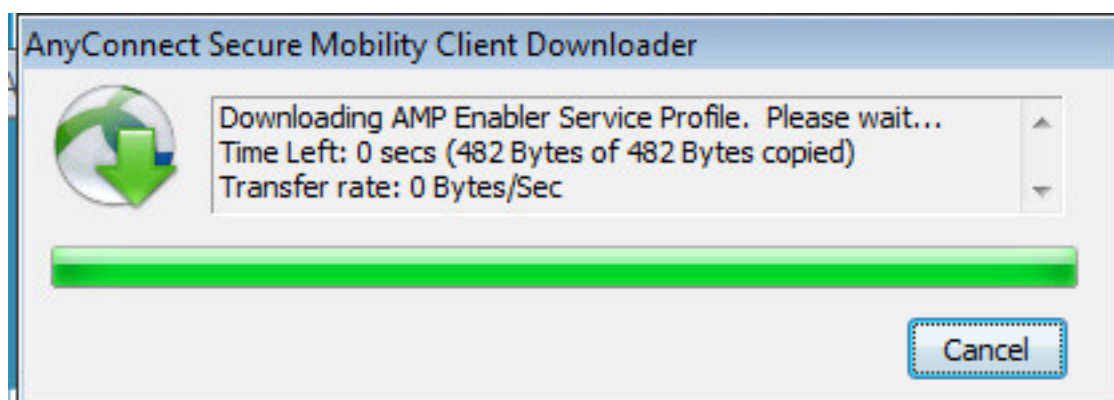
Da auf dem Client-Computer nichts installiert ist, fordert die ISE zur Installation des AnyConnect-Clients auf.

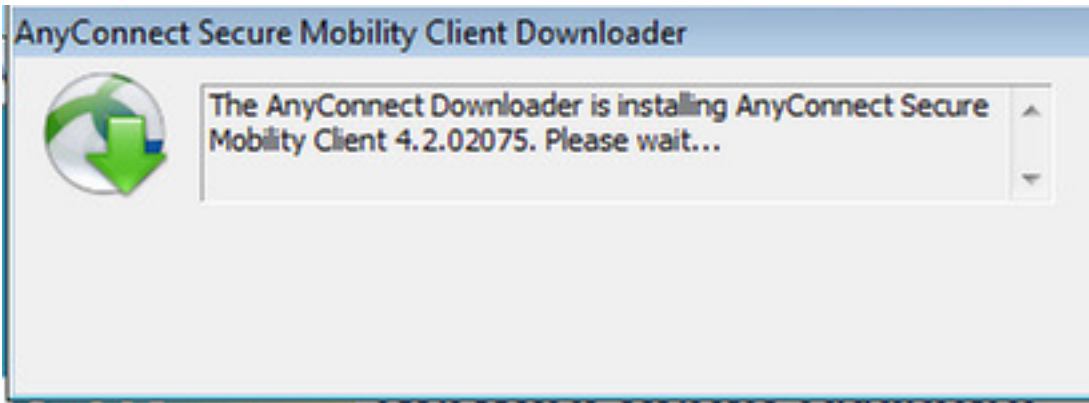


Die NSA-Anwendung (Network Setup Assistant) sollte vom Client-Computer heruntergeladen und ausgeführt werden.

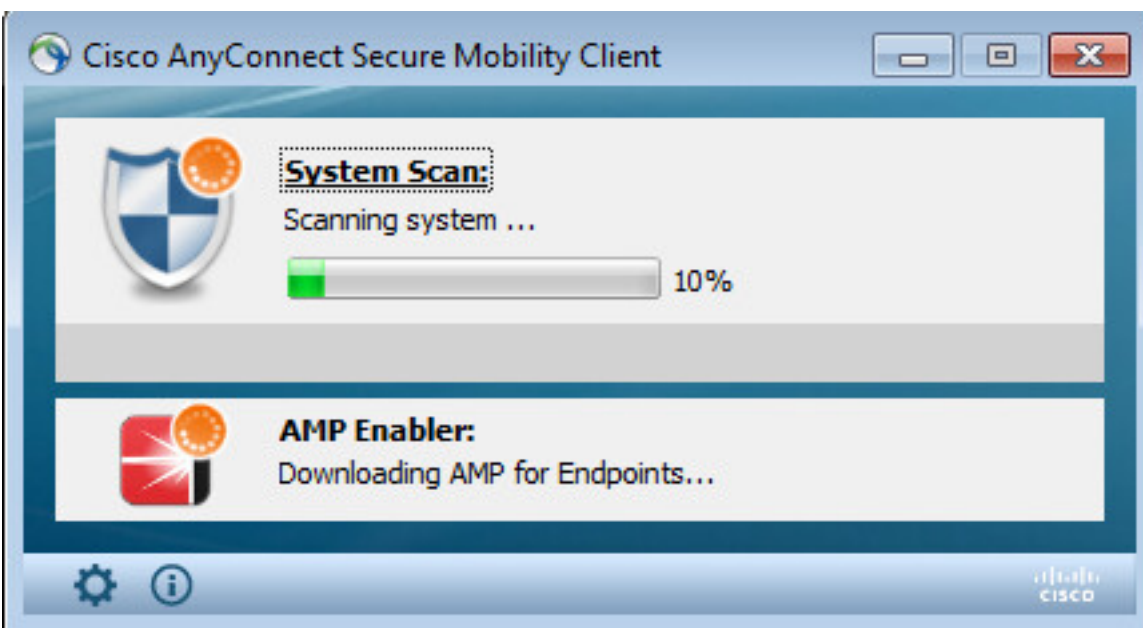
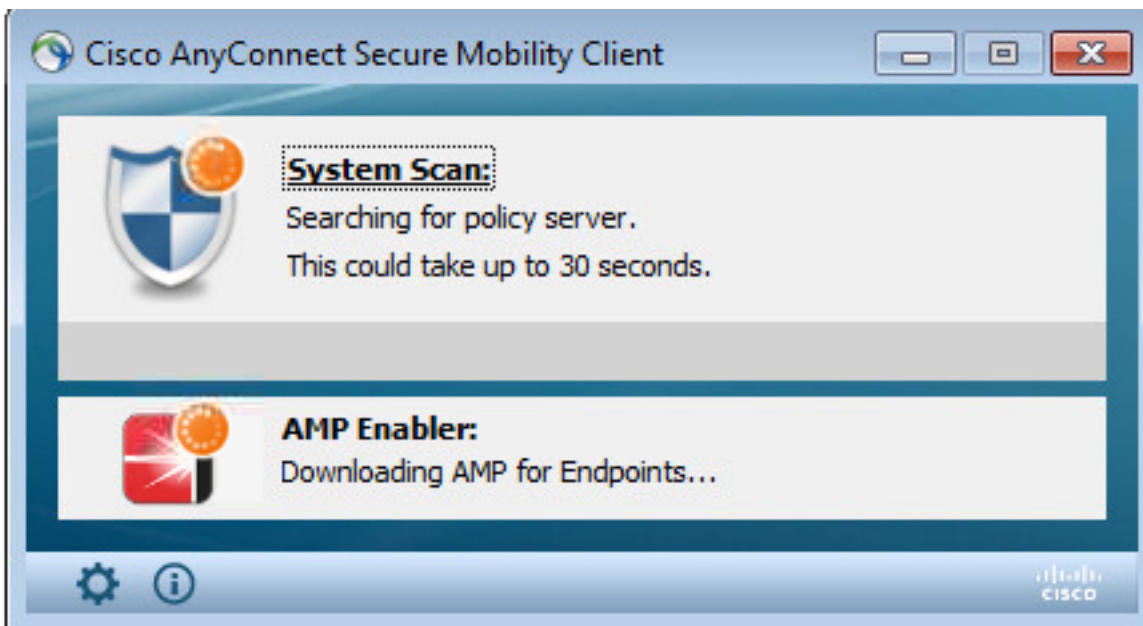


Die NSA übernimmt die Installation der erforderlichen Komponenten und Profile.

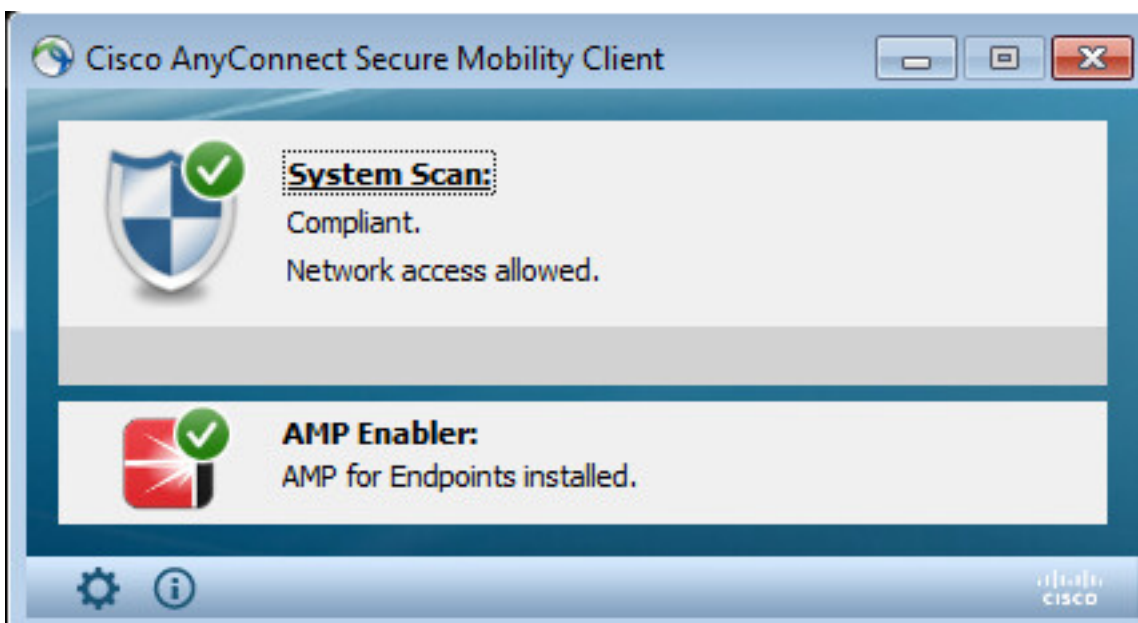
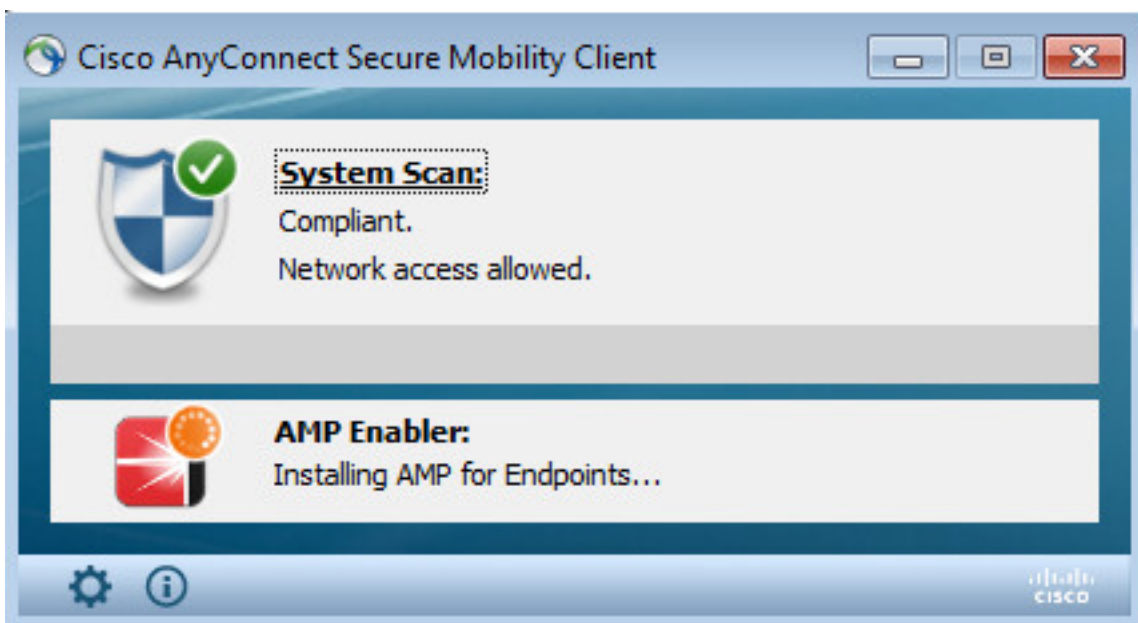
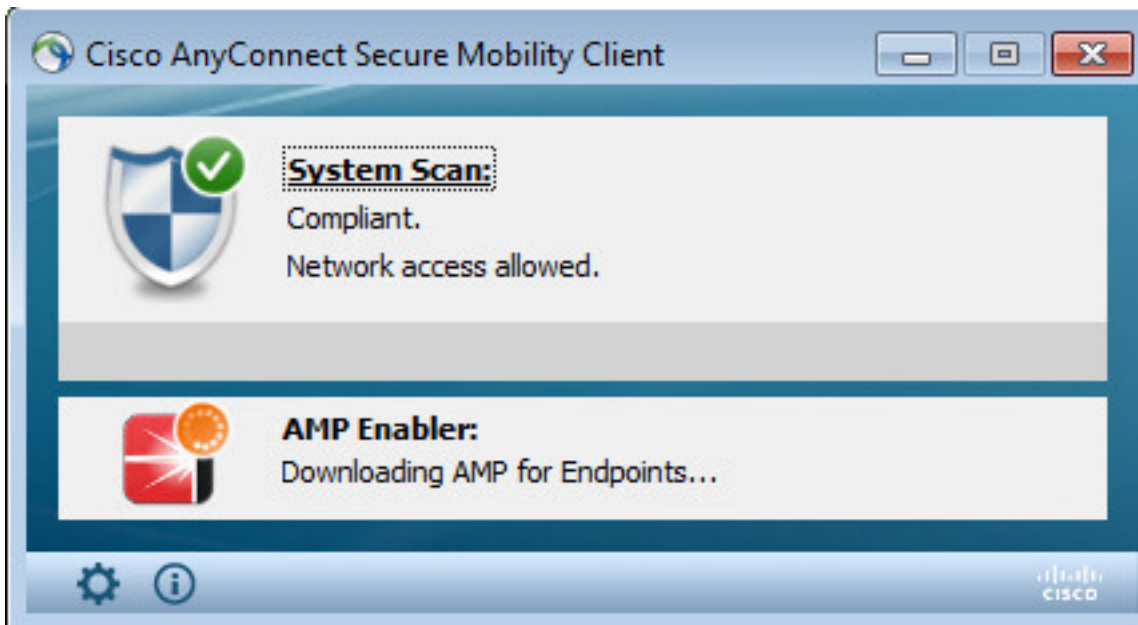




Nach Abschluss der Installation führt das AnyConnect Posture-Modul eine Compliance-Prüfung durch.



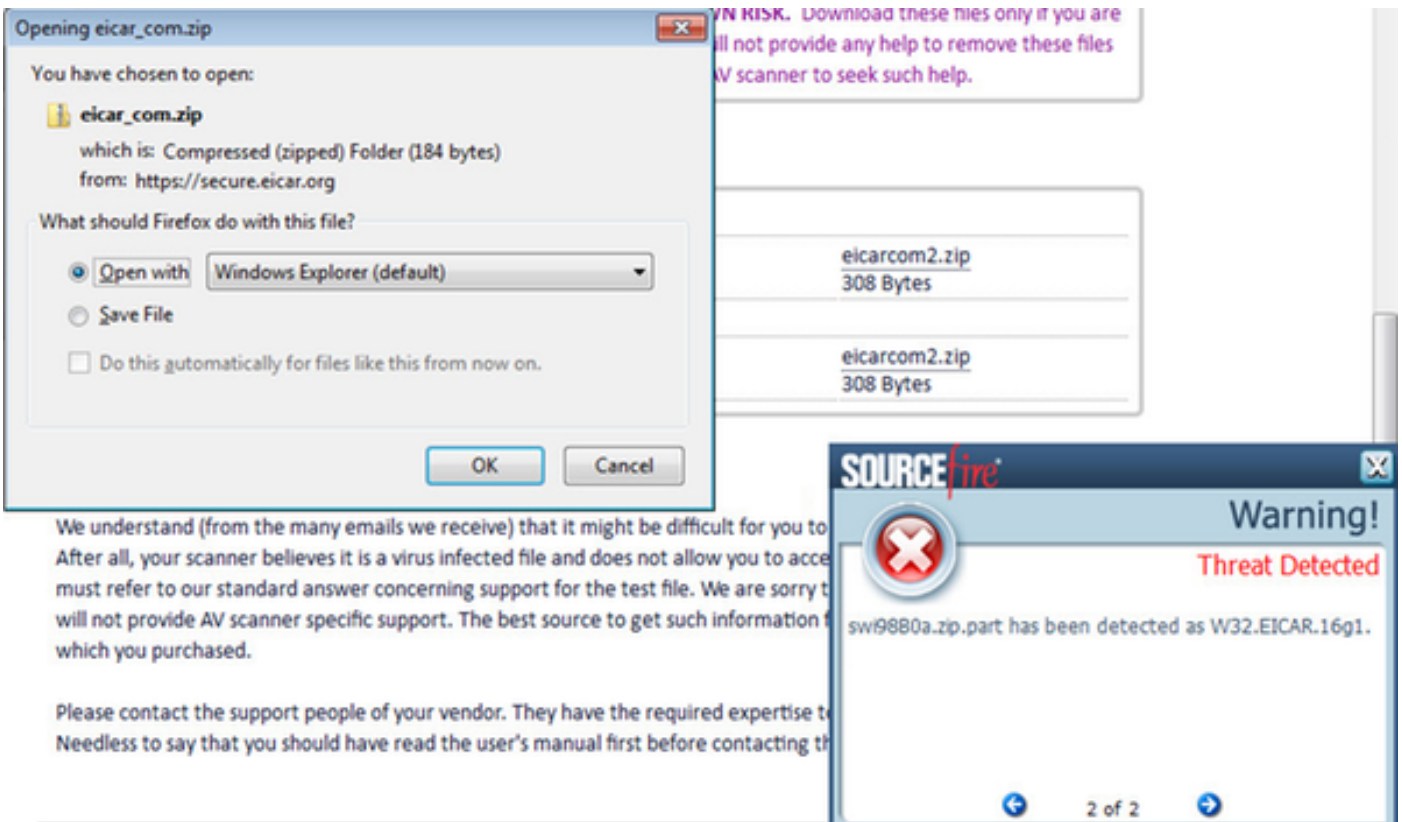
Wenn ein Endpunkt den Vorgaben entspricht, wird AMP über den zuvor im AMP-Profil angegebenen Webserver heruntergeladen und installiert.



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.

The dashboard displays the following data:

- Indications of Compromise:** ekorneyc-PC.example.com (Threat Detected)
- Hosts Detecting Malware (7 days):**

Computer	Count
ekorneyc-PC.example.com	4
HARISHA-PC.example.com	1
- Hosts Detecting Network Threats (7 days):** (No recent network threat detections to display)
- Malware Threats (7 days):**

Detection Name	Count
W32.EICAR.16g1	5
- Network Threats (7 days):** (No recent network threat detections to display)

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

The detailed view shows the following information:

- Event Type:** Threat Detected
- Filters:** Computer: e8c02e6a-a885-47ba-aeec-2ac03bea4241
- Sort:** Time
- Event Details:** ekorneyc-PC.example.com detected 0M90PRxO.zip.part as W32.EICAR.16g1
- Quarantine:** Not Seen
- Timestamp:** 2016-05-30 16:27:30 UTC
- File Detection Details:**

Field	Value
Detection	W32.EICAR.16g1
Fingerprint (SHA-256)	2546dcff...6e9eedad
Filename	0M90PRxO.zip.part
Filepath	C:\Users\admin\AppData\Local\Temp\0M90PRxO.zip.part
File Size (bytes)	184
Parent Fingerprint (SHA-256)	3147bd8...32d689c2
Parent Filename	Firefox.exe

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

Applications

AMP Adaptor 4d4047dc-4791-477d-955f-6a0f182ae65b IRF	Edit Deregister
AMP Adaptor fe80e16e-cde8-4d7f-a836-545416ae56f4 IRF	Edit Deregister

These are applications external to FireAMP, such as Sourcefire's Defense Center, that you have authorized to access your business' data.

Here you can deauthorize registered applications, thus revoking their access to specific functionality, or you can deregister the applications, thus deauthorizing them and completely removing them from the FireAMP system.

You can currently authorize Defense Center appliances to receive streaming FireAMP events for integration with the Defense Center.

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.

Summary Statistics:

- Misconfigured Supplicants: 0
- Misconfigured Network Devices: 0
- RADIUS Drops: 14
- Client Stopped Responding: 3
- Repeat Counter: 0

Time	Status	Details	Repeat	Identify	Endpoint ID	Endpoint P...	Authentication Policy	Authorization Policy	Authorization Profiles	IP Address
Jun 30, 2016 05:50:18.729 PM	●		0	alice	02-4A:00:14-8D-4B	Windows7...	Default >> Dot1X >> Default	Default >> Compliant_Device_A...	PermitAccess	10.62.148.26
Jun 30, 2016 05:49:26.479 PM	●			alice	02-4A:00:14-8D-4B	Windows7...	Default >> Dot1X >> Default	Default >> Compliant_Device_A...	PermitAccess	
Jun 30, 2016 05:49:34.437 PM	●			alice	02-4A:00:14-8D-4B	Windows7...	Default >> Dot1X >> Default	Default >> Non_Compliant_Devis...	AMP_Profile	
Jun 30, 2016 05:42:56.536 PM	●			alice	02-4A:00:14-8D-4B	Windows7...	Default >> Dot1X >> Default	Default >> Non_Compliant_Devis...	AMP_Profile	

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

COMPROMISED ENDPOINTS BY INCIDENTS

COMPROMISED ENDPOINTS BY INDICATORS

MAC Address	Username	IPv4 Address	Threats	Source	Threat Severity	Logical NAD Location	Connectivity
CO-4A:00:14-8D-4B	alice	10.62.148.26	Threat Detected	AMP	Painful	Location/FBI Locations	Connected

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

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Endpoints Network Devices

Endpoints > C0:4A:00:14:8D:4B

C0:4A:00:14:8D:4B

MAC Address: C0:4A:00:14:8D:4B
 Username: **alice**
 Endpoint Profile: **Windows7-Workstation**
 Current IP Address: **10.62.148.26**
 Location:

Attributes Authentication **Threats** Vulnerabilities

Threat Detected

Type: INCIDENT
 Severity: Painful
 Reported by: AMP
 Reported at: 2016-06-30 11:27:48

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.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Endpoints Network Devices

Authentication BYOD Compliance **Compromised Endpoints** Endpoint Classification Guest Vulnerable Endpoints

COMPROMISED ENDPOINTS BY INCIDENTS
 All endpoints | Connected | Disconnected

COMPROMISED ENDPOINTS BY INDICATORS
 All endpoints | Connected | Disconnected

1 Selected

Change Authorization

Source	Threat Severity	Logical NAD Location	Connectivity	Hostname	Identity Group	Endpoint OS
AMP	Painful	Location#A1 Locations	Disconnected		Workstation	
AMP	Painful	Location#A1 Locations	Connected		Workstation	

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**.

The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The breadcrumb navigation is: Administration > System > Logging > Debug Log Configuration. The page title is "Node List > ISE21-3ek.example.com Debug Level Configuration". There are two buttons: "Edit" and "Reset to Default". Below this is a table with columns "Component Name", "Log Level", and "Description". The table contains one entry: TC-NAC with Log Level set to DEBUG and Description "TC-NAC log messages".

Component Name	Log Level	Description
TC-NAC	DEBUG	TC-NAC log messages

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), amqpProperties=#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.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 Bedrohungseignis zum Senden an PAN - c0:4a:00:14:8d:4b  
{Incident={Impact_Qualification=Painful}, Zeitstempel=1467304068599, vendor=AMP, title=Threat  
Detected}
```