

2.2 Client-Bereitstellung und -Anwendung konfigurieren

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Konfigurationen](#)

[Abschnitt 1: Konfigurieren der Client-Bereitstellung](#)

[Schritt 1: AnyConnect-Paket hochladen](#)

[Schritt 2: AnyConnect Compliance Module herunterladen](#)

[Schritt 3: Statusprofil erstellen](#)

[Schritt 4: AnyConnect-Konfiguration erstellen](#)

[Schritt 5: Konfigurieren von Client-Bereitstellungsrichtlinien](#)

[Schritt 6: Autorisierungsprofil für CP erstellen](#)

[Schritt 7: Autorisierungsrichtlinien konfigurieren](#)

[Abschnitt 2: Status konfigurieren](#)

[Schritt 1: Status aktualisieren](#)

[Schritt 2: Erstellen der Anwendungsbedingung](#)

[Schritt 3: Statusanforderung erstellen](#)

[Schritt 4: Statusrichtlinie erstellen](#)

[Schritt 5 \(optional\). Intervall für kontinuierliche Überwachung ändern](#)

[Schritt 6 \(optional\). Anwendungs-Compliance erstellen](#)

[Überprüfen](#)

[LiveLogs](#)

[Endpunkt](#)

[Richtlinienelemente für den Status](#)

[Berichte](#)

[Statusüberprüfung nach Zustand](#)

[Statusüberprüfung nach Endpunkt](#)

[Fehlerbehebung](#)

[Von ISE](#)

[Von AnyConnect](#)

[Häufige Probleme](#)

[AnyConnect kann ISE nicht erreichen](#)

[ISE löst beim Erstellen von Anwendungs-Compliance aus der EP-Ansicht den Fehler "Null" aus](#)

Einführung

In diesem Dokument wird beschrieben, wie die Anwendungstransparenz auf Identity Service

Engine (ISE) 2.2 konfiguriert und Fehler behoben werden. Mit Application Visibility (Anwendungstransparenz) können Sie Anwendungen überwachen, die auf Endpunkten installiert sind, auf diesen Informationen basierende Richtlinien erstellen und Anwendungen während Statusprüfungen abbuchen oder deinstallieren, wenn sie bestimmte Bedingungen erfüllen. AnyConnect sendet regelmäßig Informationen mit einer Liste installierter/ausgeführter Anwendungen und Prozesse an die ISE. AnyConnect kann Informationen über alle Anwendungen oder über Anwendungen bestimmter Kategorien (Browser, Verschlüsselung usw.) sammeln.

Voraussetzungen

Anforderungen

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

- Cisco Identity Service Engine
- Client-Bereitstellung
- ISE-Status

Verwendete Komponenten

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

- Cisco Identity Service Engine Version 2.2.0.470
- Cisco AnyConnect 4.4.00243
- AnyConnect Compliance Module 4.2.468.0
- Windows 7 Service Pack 1

Konfigurieren

Konfigurationen

Abschnitt 1: Konfigurieren der Client-Bereitstellung

Schritt 1: AnyConnect-Paket hochladen

1. Navigieren Sie zu **Richtlinien > Richtlinienelemente > Ergebnisse > Client Provisioning > Results** on ISE. Klicken Sie auf **Hinzufügen > Agent-Ressourcen von der lokalen Festplatte**:

2. Wählen Sie **Kategorie** als von Cisco bereitgestellte Pakete aus und **wählen Sie Datei** (AnyConnect-Paket):

Agent Resources From Local Disk

Category ⓘ

anyconnect-w...ploy-k9.pkg

AnyConnect Uploaded Resources

Name	Type	Version	Description
AnyConnectDesktopWindows 4.4.24...	AnyConnectDesktopWindows	4.4.243.0	AnyConnect Secure Mobility Clie...

Klicken Sie auf **Senden**, um die Änderungen zu speichern.

Sie sollten aufgefordert werden, die Prüfsummen des hochgeladenen Pakets zu bestätigen. Vergleichen Sie diese mit Prüfsummen, die auf einer Cisco Website bereitgestellt werden, um sicherzustellen, dass das Paket nicht beschädigt wird.

Schritt 2: AnyConnect Compliance Module herunterladen

Klicken Sie auf einer Ergebnisseite von Client Provisioning auf **Add > Agent resources from Cisco site**, sodass ein Fenster mit verfügbaren Modulen angezeigt wird. Wählen Sie das erforderliche **AnyConnect Compliance Module** für Windows aus, und klicken Sie auf **Speichern**.

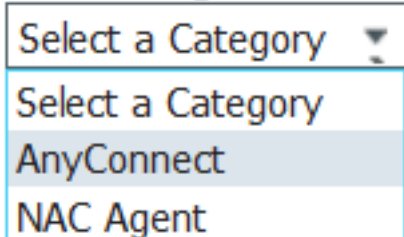
Wenn Sie keine Internetverbindung auf Ihrer ISE haben, können Sie das neueste Compliance-Modul von cisco.com herunterladen und auf dieselbe Weise wie das AnyConnect-Paket auf Ihre ISE hochladen.

Wenn Sie einen Proxy in Ihrem Netzwerk haben, konfigurieren Sie ihn unter **Administration > System > Settings > Proxy** page.

Schritt 3: Statusprofil erstellen

Im Ergebnisseite von Client Provisioning: Klicken Sie auf **Add > NAC Agent oder AnyConnect Posture Profile**, und wählen Sie **AnyConnect** aus Status Agent Profile Settings aus:

Posture Agent Profile Settings

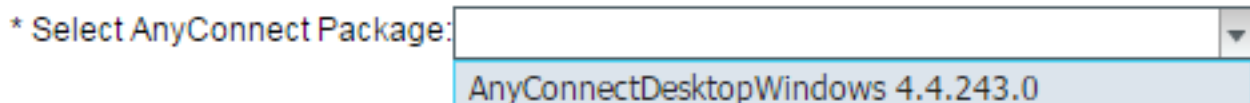


Select a Category ▼
Select a Category
AnyConnect
NAC Agent

Benennen Sie das Profil, und füllen Sie die erforderlichen Felder aus. Klicken Sie auf **Senden**, um das Profil zu speichern.

Schritt 4: AnyConnect-Konfiguration erstellen

Klicken Sie auf einer Ergebnisseite von Client Provisioning auf **Hinzufügen > AnyConnect Configuration**, und wählen Sie das in Schritt 1 hochgeladene Paket aus:



* Select AnyConnect Package: AnyConnectDesktopWindows 4.4.243.0

Zusätzliche Optionen müssen geladen werden. Füllen Sie alle erforderlichen Felder aus, und klicken Sie auf **Senden**, um die Änderungen zu speichern:

* Select AnyConnect Package: AnyConnectDesktopWindows 4.4.243.0
* Configuration Name: AnyConnect Configuration
Description:
DescriptionValue
* Compliance Module: AnyConnectComplianceModuleWindows 4.2.468.0

AnyConnect Module Selection

- ISE Posture
- VPN
- Network Access Manager
- Web Security
- AMP Enabler
- ASA Posture
- Network Visibility
- Umbrella Roaming Security
- Start Before Logon
- Diagnostic and Reporting Tool

Profile Selection

* ISE Posture: AnyConnect Posture
VPN
Network Access Manager
Web Security
AMP Enabler
Network Visibility
Umbrella Roaming Security
Customer Feedback

Customization Bundle
Localization Bundle

Konfigurationsname: Name der Konfiguration. Diese wird in der Client Provisioning-Richtlinie (nächster Schritt) verwendet.

Compliance Module: Wählen Sie Compliance-Modul aus, das in Schritt 2 heruntergeladen wurde.

ISE-Status: Wählen Sie das in Schritt 3 erstellte AnyConnect-Statusprofil aus.

Schritt 5: Konfigurieren von Client-Bereitstellungsrichtlinien

Navigieren Sie zu **Richtlinien > Client Provisioning**. Erstellen Sie eine neue Richtlinie, oder bearbeiten Sie eine vorhandene für Windows. Wählen Sie als Ergebnis erstellte AnyConnect-

Konfiguration aus:

	<input checked="" type="checkbox"/>	Windows	If	Any	and	Windows All	and	Condition(s)	then	AnyConnect Configuration
--	-------------------------------------	---------	----	-----	-----	-------------	-----	--------------	------	--------------------------

Schritt 6: Autorisierungsprofil für CP erstellen

Navigieren Sie zu **Richtlinien > Richtlinienelemente > Ergebnisse > Autorisierung > Autorisierungsprofile**, und klicken Sie auf **Hinzufügen**, um ein neues Profil zu erstellen. Konfigurieren Sie sie für die Umleitung zum Client Provisioning Portal:

Authorization Profiles > **New Authorization Profile**

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

Common Tasks

Web Redirection (CWA, MDM, NSP, CPP)

ACL Value

Static IP/Host name/FQDN

Auto Smart Port

Advanced Attributes Settings

=

Attributes Details

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = url-redirect-acl=ISE-REDIRECT
cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=4cb1f740-e371-11e6-92ce-005056873bd0&action=cpp
```

Klicken Sie auf **Senden**, um das Profil zu speichern.

Beachten Sie, dass die Umleitung-ACL (in diesem Beispiel **ISE-REDIRECT**) auf NAD (Network Access Device) erstellt werden muss, um eine ordnungsgemäße Umleitung zu erhalten. Grundlegende Umleitungskontrolllisten sollten den Datenverkehr zu und von ISE-PSN-Knoten, DNS und DHCP nicht abfangen. Außerdem sollte HTTP- und HTTPS-Datenverkehr umgeleitet werden. Beispiele für ACLs finden Sie in den folgenden Dokumenten: [Zentrale Webauthentifizierung im WLC- und ISE-Konfigurationsbeispiel](#) und [zentrale Webauthentifizierung mit einem Konfigurationsbeispiel für einen Switch und eine Identity Services Engine](#)

Schritt 7: Autorisierungsrichtlinien konfigurieren

Navigieren Sie zu **Richtlinie > Autorisierung**, und erstellen Sie zwei Richtlinien mit Statusüberprüfung:

<input checked="" type="checkbox"/>	POSTURED	if	Session:PostureStatus EQUALS Compliant	then	PermitAccess
<input checked="" type="checkbox"/>	CPP_REDIRECT	if	Session:PostureStatus NOT_EQUALS Compliant	then	CPP_REDIRECT

Wenn bei einer solchen Konfiguration auf einem Endpunkt noch kein AnyConnect installiert ist oder der Status noch nicht abgeschlossen wurde, wird er an das Client Provisioning Portal umgeleitet. Endbenutzer können AnyConnect von der ISE installieren, AnyConnect erkennt die ISE und überprüft die Schwachstelle.

Klicken Sie auf **Speichern**.

Abschnitt 2: Status konfigurieren

Schritt 1: Status aktualisieren

Navigieren Sie zu **Administration > Settings > Posture > Updates**, und klicken Sie auf **Jetzt aktualisieren**, um den Status zu aktualisieren. Sie enthält OPSWAT-Diagramme und -Definitionen für Anwendungen und ist für die Erstellung von Richtlinien erforderlich.

Wenn Sie auf Ihrer ISE keine Internetverbindung haben, können Sie die neuesten Statusaktualisierungen von <https://www.cisco.com/web/secure/pmbu/posture-offline.html> herunterladen. Navigieren Sie dann zu **Administration > System > Settings > Posture > Updates**, wählen Sie **Offline aus**, und wählen Sie die heruntergeladene Datei mit Statusaktualisierungen aus. Klicken Sie auf **Jetzt aktualisieren**, um die Datei hochzuladen und Statusaktualisierungen zu installieren.

Schritt 2: Erstellen der Anwendungsbedingung

AnyConnect erfasst Informationen zu installierten Anwendungen nur mit dem 4.x (oder höher) Compliance Module.

Bei der Version 3.x des Compliance Module können nur Prozessüberprüfungen durchgeführt werden (d. h., dass AnyConnect-Prüfungen durchführen kann, wenn der angegebene Prozess ausgeführt wird oder nicht).

Mit **Anwendungszustand** können diese Kombinationen konfiguriert werden:

- Installed + Running - AnyConnect sammelt Informationen zu aktuell ausgeführten Prozessen zusammen mit Installationsdaten.
- Installiert + nicht ausgeführt - AnyConnect sammelt nur Installationsdaten

Mit **Provision by** können diese ausgewählt werden: **Alles**, **Name** und **Kategorie**:

- Wenn **Alles** ausgewählt ist, versucht AnyConnect, Informationen über alle installierten Anwendungen zu sammeln.
- Wenn **Name** ausgewählt ist, kann eine bestimmte Anwendung für die Richtlinie ausgewählt werden. Beispiel:

Provision by

At least one category must be selected *

<input type="checkbox"/> Unclassified	<input type="checkbox"/> Data Loss Prevention	<input type="checkbox"/> Data Storage
<input type="checkbox"/> Browser	<input type="checkbox"/> Backup	<input type="checkbox"/> Patch Management
<input type="checkbox"/> Encryption	<input checked="" type="checkbox"/> Antiphishing	<input type="checkbox"/> VPN Client
<input type="checkbox"/> Anti-Malware	<input type="checkbox"/> Virtual Machine	<input type="checkbox"/> Firewall
<input type="checkbox"/> Messenger	<input type="checkbox"/> Public File Sharing	<input type="checkbox"/> Health Agent

Vendor *

At least one product must be selected *

| Selected Rows/Page 1 / 1 3 Total Rows

Refresh

Filter

<input type="checkbox"/>	Product Name	Version
<input checked="" type="checkbox"/>	Anvi Smart Defender	1.x
<input type="checkbox"/>	Anvi Smart Defender	2.x
<input type="checkbox"/>	Anvi Smart Defender	ANY

- Wenn **Kategorie** ausgewählt ist, sammelt AnyConnect Informationen über alle Anwendungen aus der angegebenen Kategorie. Beispiel:

Provision by

At least one category must be selected *

- | | | |
|--|---|---|
| <input type="checkbox"/> Unclassified | <input type="checkbox"/> Data Loss Prevention | <input type="checkbox"/> Data Storage |
| <input type="checkbox"/> Browser | <input type="checkbox"/> Backup | <input type="checkbox"/> Patch Management |
| <input type="checkbox"/> Encryption | <input type="checkbox"/> Antiphishing | <input type="checkbox"/> VPN Client |
| <input checked="" type="checkbox"/> Anti-Malware | <input type="checkbox"/> Virtual Machine | <input type="checkbox"/> Firewall |
| <input type="checkbox"/> Messenger | <input type="checkbox"/> Public File Sharing | <input type="checkbox"/> Health Agent |

Wenn Sie Informationen zu installierten und ausgeführten Anwendungen unter **Richtlinien > Richtlinienelemente > Bedingungen > Status > Anwendungsbedingung** sammeln möchten, klicken Sie auf **Hinzufügen**, um neue Bedingungen zu erstellen und die erforderlichen Felder wie folgt auszufüllen:

[Application Condition](#) > New

Name *	<input type="text" value="Apps_Collection"/>
Description	<input type="text" value="Condition for all applications"/>
Operating System *	<input type="text" value="Windows All"/> +
Compliance module	<input type="text" value="4.x or later"/>
Check By *	<input type="text" value="Application"/>
Application State *	<input checked="" type="checkbox"/> Installed <input checked="" type="checkbox"/> Running
Provision by	<input type="text" value="Everything"/>

Cancel

Submit

Schritt 3: Statusanforderung erstellen

Unter **Richtlinien > Richtlinienelemente > Ergebnisse > Status > Anforderungen** erstellen Sie mit der erstellten Anwendungsbedingung eine neue Anforderung:

Name	Operating Systems	Compliance Module	Stealth Mode	Conditions	Remediation Actions
USB_Block	for Windows All	using 4.x or later	using Disabled	met if USB_Check	then USB_Block
Apps_collection	for Windows All	using 4.x or later	using Disabled	met if Apps_Collection	then Message Text Only
Any_AV_Installation_Mac	for Mac OSX	using 3.x or earlier	using Disabled	met if ANY_av_mac_inst	then Message Text Only
Any_AV_Definition_Mac	for Mac OSX	using 3.x or earlier	using Disabled	met if ANY_av_mac_def	then AnyAVDefRemediationMac
Any_AS_Installation_Mac	for Mac OSX	using 3.x or earlier	using Disabled	met if ANY_as_mac_inst	then Message Text Only
Any_AS_Definition_Mac	for Mac OSX	using 3.x or earlier	using Disabled	met if ANY_as_mac_def	then AnyASDefRemediationMac

Schritt 4: Statusrichtlinie erstellen

Damit ISE und AnyConnect Informationen über Anwendungen sammeln können, sollte eine Anforderung mit einer Anwendungsbedingung in die Statusrichtlinie aufgenommen werden. Statusrichtlinien können unter **Richtlinien > Status** erstellt werden. Die Anforderung kann als **Audit** festgelegt werden, wenn Sie Informationen zur weiteren Verwendung sammeln möchten.

Posture Policy

Define the Posture Policy by configuring rules based on operating system and/or other conditions.

The screenshot shows a configuration window for a Posture Policy rule. The rule name is 'Apps'. The conditions are: 'Any' for 'Identify Groups', 'Windo...' for 'Operating Systems', '4.x or later' for 'Compliance Module', and 'Disabled' for 'Stealth mode'. The remediation action is 'Audit'. The 'Requirements' section on the right shows a tree view with 'Apps_collection' expanded, showing 'Mandatory', 'Optional', and 'Audit' options.

Schritt 5 (optional). Intervall für kontinuierliche Überwachung ändern

Mit der ISE können Sie festlegen, wie oft AnyConnect Updates über Anwendungen an die ISE senden soll. Standardmäßig ist das Intervall auf 5 Minuten festgelegt und kann unter **Administration > Settings > Posture > General Settings** geändert werden:

Posture General Settings

Remediation Timer Minutes *i*

Network Transition Delay Seconds *i*

Default Posture Status *i*

Automatically Close Login Success Screen After Seconds *i*

Continuous Monitoring Interval Minutes *i*

Acceptable Use Policy in Stealth Mode

Posture Lease

- Perform posture assessment every time a user connects to the network
- Perform posture assessment every Days *i*

Save

Reset

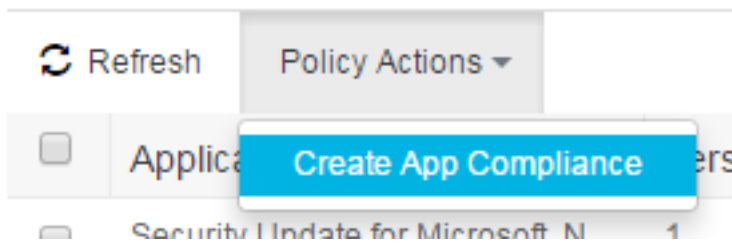
Schritt 6 (optional). Anwendungs-Compliance erstellen

Nachdem Daten vom Endpunkt gesammelt wurden, können Sie unter **Context Visibility > Endpoints > [ENDPOINT]** die Anwendungs-Compliance erstellen:

1. Wählen Sie eine Anwendung aus:

<input type="checkbox"/>	Windows Media Player	1.2.0.7001.23017	Microsoft Corporation	Unclassified	C:\Program Files\Windows...
<input checked="" type="checkbox"/>	FileZilla	3.8.1.0	FileZilla Project	FileShare	C:\Program Files (x86)...
<input type="checkbox"/>	Security Update for Microsoft N...	2	Microsoft Corporation	Unclassified	

2. Klicken Sie auf **Richtlinienaktionen > Anwendungs-Compliance erstellen**.



3. Füllen Sie die Felder in einem Popup-Fenster aus:

Create Posture Application Compliance

Application Names *

Version 3.8.1.0 ANY

Compliance Name *

Description

Operating System * MacOSX Windows

Compliance module

Condition

Application State * Installed Running

Remediation

Remediation Type

Interval *

Retry Count *

Remediation Option * Uninstall Kill Process

Note: By default the above Condition & Remediation would be linked as a requirement.

Posture Policy

Posture Policy will be defined by configuring rules based on operating system and/or other conditions.

Identity Groups *

4. Klicken Sie auf **Policy speichern**, diese Elemente sollten erstellt werden: Status-AnwendungsbedingungAktion zur Problembehebung für

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

LiveLogs

In RADIUS LiveLogs sieht der Fluss wie ein normaler Statusfluss aus: **Authentifizierung + Umleitung zum Bereitstellungsportal > Autorisierungsänderung (CoA) > Übereinstimmung mit konformen Statusrichtlinien**

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Posture St...	Endpoint P...	Authenticat...	Authorizati...	Authorizati...	IP Address
Jan 04, 2017 07:59:07.655 PM			1	cisco	C0-4A:00:15:75:C8	Compliant	Microsoft-W...	Default >> D...	Default >> p...	PermitAccess	10.62.148.162
Jan 04, 2017 07:19:16.732 PM				cisco	C0-4A:00:15:75:C8	Compliant	Microsoft-W...	Default >> D...	Default >> p...	PermitAccess	
Jan 04, 2017 07:19:16.097 PM					C0-4A:00:15:75:C8	Compliant					
Jan 04, 2017 07:19:02.205 PM				cisco	C0-4A:00:15:75:C8	Pending	Microsoft-W...	Default >> D...	Default >> C...	CPP	

Endpunkt

Nach der Client-Bereitstellung (wenn AnyConnect zuvor nicht bereitgestellt wurde) und der Konfiguration des Continuous Monitoring Interval (Intervall für die kontinuierliche Überwachung) kann der Prozess der Datenerfassung unter **Context Visibility > Endpoints** überprüft werden. Klicken Sie auf die MAC-Adresse des Endpunkts. Die Seite des Endpunkts sollte geöffnet werden. Sie enthält Informationen über Anwendungen, die auf dem Endpunkt selbst installiert sind:

Refresh Policy Actions Filter

Application Name	Version	Vendor	Running process	Category	Install Path
<input type="checkbox"/> Security Update for Microsoft .N...	1	Microsoft Corporation		Unclassified	
<input type="checkbox"/> Security Update for Microsoft .N...	1	Microsoft Corporation		Unclassified	
<input type="checkbox"/> Microsoft .NET Framework 4.6.1	4.6.01005	Microsoft Corporation		Unclassified	C:\Windows\Microsoft...
<input type="checkbox"/> Google Update Helper	1.3.24.15	Google Inc.		Unclassified	
<input type="checkbox"/> Windows Update Agent	7.6.7601.19161	Microsoft Corporation		PatchManagement	C:\Windows\System32\
<input type="checkbox"/> Cisco AnyConnect ISE Complia...	4.2.468.0	Cisco Systems, Inc		Unclassified	C:\Program Files (x86)...
<input type="checkbox"/> DAEMON Tools Lite	4.49.1.0356	Disc Soft Ltd		Unclassified	C:\Program Files (x86)...
<input type="checkbox"/> Tltpd32 Standalone Edition (re...	0.0			Unclassified	
<input type="checkbox"/> Security Update for Microsoft .N...	1	Microsoft Corporation		Unclassified	
<input type="checkbox"/> VMware Tools	9.4.15.2827462	VMware, Inc.	2	Unclassified	C:\Program Files\VMw...
<input type="checkbox"/> BitLocker Drive Encryption	6.1.7600.16385	Microsoft Corporation		DiskEncryption	C:\Windows\System32\
<input type="checkbox"/> Cisco AnyConnect Diagnostics ...	4.4.00209	Cisco Systems, Inc.		Unclassified	C:\Program Files (x86)...
<input type="checkbox"/> Cisco AnyConnect Secure Mobi...	4.4.00209	Cisco Systems, Inc.	5	Unclassified	C:\Program Files (x86)...
<input type="checkbox"/> Java Auto Updater	2.8.91.15	Oracle Corporation		Unclassified	
<input type="checkbox"/> Mozilla Firefox	47.0.2	Mozilla Corporation		AntiPhishing.Browser	C:\Program Files (x86)...
<input type="checkbox"/> Microsoft Visual C++ 2008 Redi...	9.0.30729.4148	Microsoft Corporation		Unclassified	
<input type="checkbox"/> Java 8 Update 91	8.0.910.15	Oracle Corporation		Unclassified	C:\Program Files (x86)...
<input type="checkbox"/> Google Chrome	55.0.2883.87	Google Inc.		AntiPhishing.Browser	C:\Program Files (x86)...
<input type="checkbox"/> Cisco AnyConnect Profile Editor	4.1.08005	Cisco Systems, Inc.		Unclassified	C:\Program Files (x86)...
<input type="checkbox"/> Java	8.0.910.15	Oracle Corporation		Unclassified	C:\Program Files (x86)...
<input type="checkbox"/> Internet Explorer	11.0.9600.18524	Microsoft Corporation		AntiPhishing.Browser	C:\Program Files\Inter...
<input type="checkbox"/> Wireshark	1.10.7	The Wireshark developer comm...		Unclassified	C:\Program Files (x86)...
<input type="checkbox"/> Windows Backup and Restore	6.1.7600.16385	Microsoft Corporation		BackupClient	C:\Windows\System32\
<input type="checkbox"/> Windows Media Player	12.0.7601.23517	Microsoft Corporation	1	Unclassified	C:\Program Files\Wind...
<input type="checkbox"/> FileZilla	3.8.1.0	FileZilla Project		FileShare	C:\Program Files (x86)...
<input type="checkbox"/> Security Update for Microsoft .N...	2	Microsoft Corporation		Unclassified	
<input type="checkbox"/> Java 7 Update 79	7.0.790	Oracle		Unclassified	C:\Program Files (x86)...

Aufgrund von [CSCve82743](#) müssen Sie zweimal auf den Endpunkt zugreifen und auf Aktualisieren klicken, um die Anwendungstabelle wiederzugeben.

Richtlinienelemente für den Status

Diese Elemente sollten mit der Option **Create App Compliance** erstellt werden:

- Status-Anwendungsbedingung
- Aktion zur Problembeseitigung für Statusanwendungen
- Statusanforderung
- Statusrichtlinie

Jede dieser Optionen kann über die ISE-GUI verifiziert werden. Die Bedingungen finden Sie unter **Richtlinien > Richtlinienelemente > Bedingungen > Status > Anwendungsbedingung**:

Application Condition

Rows/Page 25 1 / 1 Go 11 Total Rows

Name	Description	Application State	Compliance module	Categories	Check
Apps_Collection		Installed	4.x or later	Anti-Malware	APPLIC
FileZilla-Uninstall		Installed	4.x or later	Public File Sharing	APPLIC
Notepadplus		Installed and Running	4.x or later	Unclassified	APPLIC

Sie finden die Problembhebungen unter **Richtlinien > Richtlinienelemente > Ergebnisse > Status > Remediation Actions > Application Remediations**:

Application Remediation

Rows/Page 2 1 / 1 Go 2 Total Rows

Name	Description	Application State	Compliance module	Categories
Notepadplus_Remediation			4.x or later	
FileZilla-Uninstall_Remediation			4.x or later	

Die Anforderungen finden Sie unter **Richtlinien > Richtlinienelemente > Ergebnisse > Status > Anforderungen**:

FileZilla-Uninstall_Requirement	for Windows All	using 4.x or later	using Standard	met if FileZilla-Uninstall	then FileZilla-Uninstall_Remediation	Edit
---------------------------------	-----------------	--------------------	----------------	----------------------------	--------------------------------------	------

Die Richtlinien finden Sie unter **Richtlinien > Status**:

Posture Policy

Define the Posture Policy by configuring rules based on operating system and/or other conditions.

Status	Rule Name	Identity Groups	Operating Systems	Compliance Module	Stealth mode	Other Conditions	Requirements
✓	FileZilla-Uninstall_Policy	Any	and Windows All	and 4.x or later	and Disabled	and	then FileZilla-Uninstall_Requirement
✓	Minimale Online	Any	and Windows All	and 4.x or later	and Disabled	and	then Minimale Online

Berichte

Jeder Status-Bericht von jedem Endpunkt wird auf der ISE gespeichert und kann über **Operations > Reports** überprüft werden. Es gibt zwei Varianten von Statusberichten:

- Statusüberprüfung nach Endpunkt - Es enthält Details zur Statuskonformität für ein bestimmtes Endgerät.
- Statusüberprüfung nach Bedingung: Sie enthält Details zu Statusrichtlinienbedingungen. Es zeigt, welche Bedingungen fehlgeschlagen sind und welche erfolgreich waren. Es werden nur obligatorische und optionale Bedingungen angezeigt.

Statusüberprüfung nach Zustand

Statusüberprüfung nach Zustand sieht wie gezeigt aus. In diesem Beispiel schlägt eine der obligatorischen Bedingungen fehl, sodass der Status auf "Nicht konform" lautet:

Timestamp	Status	User	IP	Result	Condition	IP	Location
2017-01-24 17:20:57...	●	alice	C0:4A:00:15:75:C8	Passed	uc_visRun_v4_Notepad_ANY	10.62.148.136	All Locations
2017-01-24 17:05:59...	●	alice	C0:4A:00:15:75:C8	Failed	fs_visInst_v4_FileZilla_ANY	10.62.148.136	All Locations
2017-01-24 17:05:59...	●	alice	C0:4A:00:15:75:C8	Passed	uc_visRun_v4_Notepad_ANY	10.62.148.136	All Locations
2017-01-24 17:01:22...	●	alice	C0:4A:00:15:75:C8	Failed	fs_visInst_v4_FileZilla_ANY	10.62.148.136	All Locations
2017-01-24 17:01:22...	●	alice	C0:4A:00:15:75:C8	Passed	uc_visRun_v4_Notepad_ANY	10.62.148.136	All Locations
2017-01-24 16:56:44...	●	alice	C0:4A:00:15:75:C8	Failed	fs_visInst_v4_FileZilla_ANY	10.62.148.136	All Locations
2017-01-24 16:56:44...	●	alice	C0:4A:00:15:75:C8	Passed	uc_visRun_v4_Notepad_ANY	10.62.148.136	All Locations
2017-01-24 16:52:08.77	●	alice	C0:4A:00:15:75:C8	Failed	fs_visInst_v4_FileZilla_ANY	10.62.148.136	All Locations
2017-01-24 16:52:08.77	●	alice	C0:4A:00:15:75:C8	Passed	uc_visRun_v4_Notepad_ANY	10.62.148.136	All Locations
2017-01-24 16:17:24.78	■	alice	C0:4A:00:15:75:C8	Passed	uc_visRun_v4_Notepad_ANY	10.62.148.136	All Locations
2017-01-24 15:46:33.24	■	alice	C0:4A:00:15:75:C8	Passed	uc_visRun_v4_Notepad_ANY	10.62.148.136	All Locations
2017-01-24 15:45:57...	■	alice	C0:4A:00:15:75:C8	Passed	uc_visRun_v4_Notepad_ANY	10.62.148.136	All Locations
2017-01-24 13:45:04...	■	alice	C0:4A:00:15:75:C8	Passed	uc_visRun_v4_Notepad_ANY	10.62.148.136	All Locations
2017-01-24 12:43:45...	■	alice	C0:4A:00:15:75:C8	Passed	uc_visRun_v4_Notepad_ANY	10.62.148.136	All Locations
2017-01-24 12:43:10...	■	alice	C0:4A:00:15:75:C8	Passed	uc_visRun_v4_Notepad_ANY	10.62.148.136	All Locations
2017-01-24 12:42:35...	■	alice	C0:4A:00:15:75:C8	Passed	uc_visRun_v4_Notepad_ANY	10.62.148.136	All Locations
2017-01-24 12:41:59.22	■	alice	C0:4A:00:15:75:C8	Passed	uc_visRun_v4_Notepad_ANY	10.62.148.136	All Locations
2017-01-24 11:41:14...	■	alice	C0:4A:00:15:75:C8	Passed	uc_visRun_v4_Notepad_ANY	10.62.148.136	All Locations


Rows/Page: 100 / 11 / 12 / Go 1116 Total Rows

Statusüberprüfung nach Endpunkt

Statusüberprüfung nach Endpunkt:

Timestamp	Status	User	IP	Result	Condition	IP	Location
2017-01-24 18:17:40.993	●	N/A	alice		C0:4A:00:15:75:C8	10.62.148.136	Windows 7 Enterprise 64-bit
2017-01-24 18:10:44.127	●	N/A	alice		C0:4A:00:15:75:C8	10.62.148.136	Windows 7 Enterprise 64-bit
2017-01-24 18:00:57.393	●	N/A	alice		C0:4A:00:15:75:C8	10.62.148.136	Windows 7 Enterprise 64-bit
2017-01-24 17:55:39.642	●	N/A	alice		C0:4A:00:15:75:C8	10.62.148.136	Windows 7 Enterprise 64-bit
2017-01-24 17:46:25.969	●	N/A	alice		C0:4A:00:15:75:C8	10.62.148.136	Windows 7 Enterprise 64-bit
2017-01-24 17:40:35.05	●	N/A	alice		C0:4A:00:15:75:C8	10.62.148.136	Windows 7 Enterprise 64-bit
2017-01-24 17:25:38.766	●	N/A	alice		C0:4A:00:15:75:C8	10.62.148.136	Windows 7 Enterprise 64-bit
2017-01-24 17:20:57.331	●	N/A	alice		C0:4A:00:15:75:C8	10.62.148.136	Windows 7 Enterprise 64-bit
2017-01-24 17:05:59.534	●	N/A	alice		C0:4A:00:15:75:C8	10.62.148.136	Windows 7 Enterprise 64-bit
2017-01-24 17:01:22.737	●	N/A	alice		C0:4A:00:15:75:C8	10.62.148.136	Windows 7 Enterprise 64-bit
2017-01-24 16:56:44.516	●	N/A	alice		C0:4A:00:15:75:C8	10.62.148.136	Windows 7 Enterprise 64-bit
2017-01-24 16:52:08.77	●	N/A	alice		C0:4A:00:15:75:C8	10.62.148.136	Windows 7 Enterprise 64-bit
2017-01-24 16:17:24.78	■	N/A	alice		C0:4A:00:15:75:C8	10.62.148.136	Windows 7 Enterprise 64-bit
2017-01-24 15:46:33.24	■	N/A	alice		C0:4A:00:15:75:C8	10.62.148.136	Windows 7 Enterprise 64-bit
2017-01-24 15:45:57.783	■	N/A	alice		C0:4A:00:15:75:C8	10.62.148.136	Windows 7 Enterprise 64-bit
2017-01-24 13:45:04.109	■	N/A	alice		C0:4A:00:15:75:C8	10.62.148.136	Windows 7 Enterprise 64-bit
2017-01-24 12:43:45.326	■	N/A	alice		C0:4A:00:15:75:C8	10.62.148.136	Windows 7 Enterprise 64-bit
2017-01-24 12:43:10.551	■	N/A	alice		C0:4A:00:15:75:C8	10.62.148.136	Windows 7 Enterprise 64-bit

Rows/Page: 100 / 6 / Go 580 Total Rows

Details zu den einzelnen Statusprüfungen können durch Klicken auf das Symbol **Details Report** (Detailbericht) überprüft werden. 

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Von ISE

ise-psc.log enthält alle Informationen zum Status, einschließlich Debugging. Statusdebugs können unter **Administration > System > Logging > Debug Log Configuration** aktiviert werden.

Komponentenname ist **Status**:

- Local Log Settings
- Remote Logging Targets
- Logging Categories
- Message Catalog
- Debug Log Configuration
- Collection Filters

Node List > ise22-pri.example.com
Debug Level Configuration

Component Name	Log Level	Description
PassiveID	INFO	PassiveID events and messages
policy-engine	INFO	Policy Engine 2.0 related messages
portal	INFO	Portal (Guest, Hotspot, BYOD, CP) debug messages
portal-session-manager	INFO	Portal Session Manager debug messages
portal-web-action	INFO	Base Portal debug messages
posture	DEBUG	Posture debug messages
previewportal	INFO	Preview Portal debug messages

Wenn ein Endpunkt mit dem Netzwerk verbunden ist und AnyConnect sich mit der ISE in Verbindung setzt, prüft die ISE, ob EP mit konfigurierten Statusüberprüfungen abgeglichen werden soll. Außerdem erkennt die ISE Version des Compliance Module, das auf dem EP installiert ist. Basierend auf gesammelten Informationen generiert die ISE Statusabfrage für den EP - **NAC Agent xml** und verschlüsselt diese. Später sendet die ISE diese Abfrage an AnyConnect.

```

2017-01-04 19:19:13,686 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.runtime.PostureHandlerImpl -:cisco::- About to query posture policy for user
cisco with endpoint mac C0-4A-00-15-75-C8
2017-01-04 19:19:13,687 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.runtime.PostureManager -:cisco::- agentCMVersion=4.2.468.0,
agentType=AnyConnect Posture Agent, groupName=OESIS_V4_Agents -> found agent group with
displayName=4.x or later
2017-01-04 19:19:13,687 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.runtime.PosturePolicyUtil -:cisco::- User cisco belongs to groups NAC
Group:NAC:IdentityGroups:Endpoint Identity Groups:Profiled:Workstation,NAC
Group:NAC:IdentityGroups:Any
2017-01-04 19:19:13,687 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.runtime.PosturePolicyUtil -:cisco::- About to retrieve posture policy
resources for os 7 Enterprise, agent group 4.x or later and identity groups [NAC
Group:NAC:IdentityGroups:Endpoint Identity Groups:Profiled:Workstation, NAC
Group:NAC:IdentityGroups:Any]
2017-01-04 19:19:13,687 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.runtime.PosturePolicyUtil -:cisco::- Evaluate resourceId NAC
Group:NAC:Posture:PosturePolicies:Apps by agent group with FQN NAC
Group:NAC:AgentGroupRoot:ALL:OESIS_V4_Agents
2017-01-04 19:19:13,688 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.runtime.PosturePolicyUtil -:cisco::- The evaluation result by agent group for
resourceId NAC Group:NAC:Posture:PosturePolicies:Apps is Permit
2017-01-04 19:19:13,688 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.runtime.PosturePolicyUtil -:cisco::- Evaluate resourceId NAC
Group:NAC:Posture:PosturePolicies:Apps by OS group with FQN NAC
Group:NAC:OsGroupRoot:ALL:WINDOWS_ALL:WINDOWS_7_ALL:WINDOWS_7_ENTERPRISE_ALL
2017-01-04 19:19:13,688 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.runtime.PosturePolicyUtil -:cisco::- stealth mode is 0
2017-01-04 19:19:13,688 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.runtime.PosturePolicyUtil -:cisco::- The evaluation result by os group for
resourceId NAC Group:NAC:Posture:PosturePolicies:Apps is Permit
2017-01-04 19:19:13,688 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.runtime.PosturePolicyUtil -:cisco::- Evaluate resourceId NAC
Group:NAC:Posture:PosturePolicies:Apps by Stealth mode NSF group with FQN NAC
Group:NAC:StealthModeStandard
2017-01-04 19:19:13,688 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.runtime.PosturePolicyUtil -:cisco::- Procesing obligation with posture policy
resource with id NAC Group:NAC:Posture:PosturePolicies:Apps
2017-01-04 19:19:13,688 DEBUG [http-bio-10.48.26.60-8443-exec-9][]

```



```
cisco.cpm.posture.runtime.PosturePolicyUtil -:cisco::- Found obligation id
urn:cisco:cepm:3.3:xacml:response-qualifier for posture policy resource with id NAC
Group:NAC:Posture:PosturePolicies:Apps
2017-01-04 19:19:13,688 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.runtime.PosturePolicyUtil -:cisco::- Found obligation id PostureReqs for
posture policy resource with id NAC Group:NAC:Posture:PosturePolicies:Apps
2017-01-04 19:19:13,688 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.runtime.PosturePolicyUtil -:cisco::- Posture policy resource id Apps has
following associated requirements []
2017-01-04 19:19:13,720 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cpm.posture.runtime.agent.AgentXmlGenerator -:cisco::- policy enforceemnt is 2
2017-01-04 19:19:13,720 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cpm.posture.runtime.agent.AgentXmlGenerator -:cisco::- simple condition: [Name=Apps_Collection,
Description=null, Application State =installed,running, Provision By =Everything, monitory
Categories = []]
2017-01-04 19:19:13,720 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cpm.posture.runtime.agent.AgentXmlGenerator -:cisco::- check type is ApplicationVisibility
2017-01-04 19:19:13,800 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.runtime.PostureHandlerImpl -:cisco::- NAC agent xml <?xml version="1.0"
encoding="UTF-8"?><cleanmachines>
  <version>ISE: 2.2.0.423</version>
  <encryption>0</encryption>
  <package>
    <id>12</id>
    <name>Apps_collection</name>
    <description>Apps Check</description>
    <version/>
    <type>3</type>
    <optional>2</optional>
    <action>3</action>
    <check>
      <id>Apps_Collection</id>
      <category>12</category>
      <type>1202</type>
      <monitor>ALL</monitor>
      <evaluation>periodic</evaluation>
    </check>
    <criteria>(Apps_Collection)</criteria>
  </package>
</cleanmachines>
```

```
2017-01-04 19:19:13,800 INFO [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.util.StatusUtil -:cisco::- StatusUtil - getPosturePolicyHTML
[<cleanmachines><version>ISE:
2.2.0.423</version><encryption>0</encryption><package><id>12</id><name>Apps_collection</name><de
scription>Apps
Check</description><version/><type>3</type><optional>2</optional><action>3</action><check><id>Ap
ps_Collection</id><category>12</category><type>1202</type><monitor>ALL</monitor><evaluation>peri
odic</evaluation></check><criteria>(Apps_Collection)</criteria></package></cleanmachines>]
2017-01-04 19:19:13,800 INFO [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.util.StatusUtil -:cisco::- StatusUtil -getPosturePolicyHTML - do encrypt
2017-01-04 19:19:13,800 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.util.StatusUtil -:cisco::- Encrypting policy using AES key.
2017-01-04 19:19:13,800 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.util.CipherUtil -:cisco::- Encrypting message using AES.
2017-01-04 19:19:13,800 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.util.StatusUtil -:cisco::- IV Base 64: AeUQGbj6CP/jMB+cTIGIGQ==
2017-01-04 19:19:13,801 DEBUG [http-bio-10.48.26.60-8443-exec-9][]
cisco.cpm.posture.util.StatusUtil -:cisco::- StatusUtil.getPosturePolicyHTML() returns <!--X-
Perfigo-UserKey=--><!--X-Perfigo-Provider=Device Filter--><!--X-Perfigo-UserName=cisco--><!--
error=1010--><!--X-Perfigo-DM-Error=1010--><!--user role=--><!--X-Perfigo-OrigRole=--><!--X-
Perfigo-DM-Scan-Req=0--><!--X-ISE-IV=AeUQGbj6CP/jMB+cTIGIGQ==--><!--X-Perfigo-DM-Software-
List=f5aGq8rU5wx7hFS9WnugNhy/6HaSxNtKesoqAjYkecEk56t+I/J93PtAYU0XLq451NXQhReuFktImYEPENWwOslbV5o
OTuTsY3kEbcuR4p5Sp0cfz/j98YEubNtSKDCUGt5U8dhpOJqMYTV4UcaSP/D0FXym10gFEjPxpPghyWcplzYwcpehIX+2vOY
```

OSzPTEvM2kDdHTkof+/UYvBfGv8Y7YkK9P6lupfSedIqdynyxUbeqknXkoCaWvUawJLVWiXAJs2atsCwJjXitwNHyzCuH/mBz/Y9AUvblCB/cutCeyVCl7ij8wtXUAt2NpKqeEj0CO0xnp5B35JTBfOSXhfVjL29E5JALaun6RR8yJlkd4apk7qflnjsu451CHY/SbKTMnqjV5bNwXfuCBf++X6X/mh0nwk+r2iWhJJFyqmNxBm2BvcJAJXOKOV7xHIhgmLj+etF4Sss/zwnFT4+WTzKI+PbrVdnZjUP7+uvbQbIPtRFqJVI5StjZlIP4vLzFWKbWwXI+itTX6hjgvNhiT2zkwktvIboUZxAbV6yS5/+5cYMU3+EhWxIx/UVO0o7sX--><!--X-Perfigo-DM-Session-Time=240-->

2017-01-04 19:19:13,801 DEBUG [http-bio-10.48.26.60-8443-exec-9][[]

cisco.cpm.posture.runtime.PosturePolicyUtil --:cisco:::- User cisco belongs to groups NAC
Group:NAC:IdentityGroups:Endpoint Identity Groups:Profiled:Workstation,NAC
Group:NAC:IdentityGroups:Any

2017-01-04 19:19:13,801 DEBUG [http-bio-10.48.26.60-8443-exec-9][[]

cisco.cpm.posture.runtime.PostureHandlerImpl --:cisco:::- **Sending response to endpoint** C0-4A-00-15-75-C8 http response [[<!--X-Perfigo-UserKey=--><!--X-Perfigo-Provider=Device Filter--><!--X-Perfigo-UserName=cisco--><!--error=1010--><!--X-Perfigo-DM-Error=1010--><!--user role=--><!--X-Perfigo-OrigRole=--><!--X-Perfigo-DM-Scan-Req=0--><!--X-ISE-IV=AeUQGbj6CP/jMB+cTIGIGQ=--><!--X-Perfigo-DM-Software-

List=f5aGq8rU5wx7hFS9WnugNhy/6HaSxNtKesoqAjYkecEk56t+I/J93PtAYU0XLq451NXQhReuFktImYEPENWwOs1bV5oOTuTsY3kEbcuR4p5Sp0cfz/j98YEubNtSKDCUGt5U8dhpOJqMYTV4UcaSP/D0FXym10gFEjPxpPghyWcplzYwcpehIX+2vOYOSzPTEvM2kDdHTkof+/UYvBfGv8Y7YkK9P6lupfSedIqdynyxUbeqknXkoCaWvUawJLVWiXAJs2atsCwJjXitwNHyzCuH/mBz/Y9AUvblCB/cutCeyVCl7ij8wtXUAt2NpKqeEj0CO0xnp5B35JTBfOSXhfVjL29E5JALaun6RR8yJlkd4apk7qflnjsu451CHY/SbKTMnqjV5bNwXfuCBf++X6X/mh0nwk+r2iWhJJFyqmNxBm2BvcJAJXOKOV7xHIhgmLj+etF4Sss/zwnFT4+WTzKI+PbrVdnZjUP7+uvbQbIPtRFqJVI5StjZlIP4vLzFWKbWwXI+itTX6hjgvNhiT2zkwktvIboUZxAbV6yS5/+5cYMU3+EhWxIx/UVO0o7sX--><!--X-Perfigo-DM-Session-Time=240-->]]

2017-01-04 19:19:13,959 DEBUG [http-bio-10.48.26.60-8443-exec-5][[]

cisco.cpm.posture.runtime.PostureHandlerImpl -:::- receiving request from client
C0:4A:00:15:75:C8 10.62.148.162 bcu5ksw0

2017-01-04 19:19:13,966 DEBUG [http-bio-10.48.26.60-8443-exec-5][[]

cisco.cpm.posture.runtime.PostureHandlerImpl -:::- Found the ipAddress that matched the http request remote address 10.62.148.162 and corresponding client mac address C0-4A-00-15-75-C8

2017-01-04 19:19:13,966 DEBUG [http-bio-10.48.26.60-8443-exec-5][[]

cisco.cpm.posture.runtime.PostureRuntimeFactory -:::- looking for Radius session with input values : sessionId: 0a3e94650000066586d3c42, MacAddr: C0-4A-00-15-75-C8, ipAddr: 10.62.148.162

2017-01-04 19:19:13,966 DEBUG [http-bio-10.48.26.60-8443-exec-5][[]

cisco.cpm.posture.runtime.PostureRuntimeFactory -:::- looking for session using session ID: 0a3e94650000066586d3c42, IP addrs: [10.62.148.162], mac Addrs [C0-4A-00-15-75-C8]

2017-01-04 19:19:13,966 DEBUG [http-bio-10.48.26.60-8443-exec-5][[]

cisco.cpm.posture.runtime.PostureRuntimeFactory -:::- Found session using sessionId 0a3e94650000066586d3c42

Der vollständige Bericht von AnyConnect. Dieser Bericht enthält Informationen zu allen gefundenen Anwendungen, die mit der konfigurierten Anwendungsbedingung übereinstimmen.

2017-01-04 19:19:37,358 DEBUG [http-bio-10.48.26.60-8443-exec-3][[]

cisco.cpm.posture.runtime.PostureHandlerImpl -:::- UDID is 766bb955e51e4ab063fd478c63acee81260ca592 for end point C0-4A-00-15-75-C8

2017-01-04 19:19:37,358 DEBUG [http-bio-10.48.26.60-8443-exec-3][[]

cisco.cpm.posture.runtime.PostureHandlerImpl -:::- os version from user agent is 1.2.1.6.1.4

2017-01-04 19:19:37,358 DEBUG [http-bio-10.48.26.60-8443-exec-3][[]

cisco.cpm.posture.runtime.PostureHandlerImpl -:::- Received posture request [parameters: reqtype=, userip=10.62.148.162, clientmac=C0-4A-00-15-75-C8, os=, osVerison=1.2.1.6.1.4, architecture=, provider=, state=, userAgent=Mozilla/4.0 (compatible; WINDOWS; 1.2.1.6.1.4; AnyConnect Posture Agent v.4.4.00209), session_id=

2017-01-04 19:19:37,358 DEBUG [http-bio-10.48.26.60-8443-exec-3][[]

cisco.cpm.posture.runtime.PostureHandlerImpl -:::- Found a session info for endpoint C0-4A-00-15-75-C8 cisco

2017-01-04 19:19:37,358 DEBUG [http-bio-10.48.26.60-8443-exec-3][[]

cisco.cpm.posture.runtime.PostureHandlerImpl -:::- Got userid cisco from cache for endpoint C0-4A-00-15-75-C8/

2017-01-04 19:19:37,358 DEBUG [http-bio-10.48.26.60-8443-exec-3][[]

cisco.cpm.posture.runtime.PostureHandlerImpl -:::- Report IV in Base64: JjneGgZcJbmjqMKQcy8kJg==

2017-01-04 19:19:37,359 DEBUG [http-bio-10.48.26.60-8443-exec-3][[]

cisco.cpm.posture.runtime.PostureHandlerImpl -:::- Using AES shared secret to decrypt report.

2017-01-04 19:19:37,359 DEBUG [http-bio-10.48.26.60-8443-exec-3][[]

```
cisco.cpm.posture.util.CipherUtil -::::- Decrypting message using AES.
2017-01-04 19:19:37,359 DEBUG [http-bio-10.48.26.60-8443-exec-3][]
cisco.cpm.posture.runtime.PostureHandlerImpl -::::- Decrypted report [[
<report><version>1000</version><package><id>12</id><status>1</status><check><chk_id>Apps_Collect
ion</chk_id><diff>0</diff><application><diff>0</diff><id></id><name>Adobe Flash Player 23
NPAPI</name><vendor>Adobe Systems
Incorporated</vendor><version>23.0.0.207</version><category>Unclassified</category></application
><application><diff>0</diff><id>104</id><name>Adobe Flash Player</name><vendor>Adobe Systems
Inc.</vendor><version>23.0.0.207</version><path>C:\Windows\SysWOW64\Macromed\FIash</path><categ
ory>Unclassified</category></application><application><diff>0</diff><id>873</id><name>BitLocker
Drive Encryption</name><vendor>Microsoft
Corporation</vendor><version>6.1.7600.16385</version><path>C:\Windows\System32</path><category>
DiskEncryption</category></application><application><diff>0</diff><id></id><name>Cisco
AnyConnect Diagnostics and Reporting Tool</name><vendor>Cisco Systems,
Inc.</vendor><version>4.4.00209</version><path>C:\Program Files (x86)\Cisco\Cisco AnyConnect
Secure Mobility
Client\DART</path><category>Unclassified</category></application><application><diff>0</diff><id
></id><name>Cisco AnyConnect ISE Compliance Module</name><vendor>Cisco Systems,
Inc.</vendor><version>4.2.468.0</version><path>C:\Program Files (x86)\Cisco\Cisco AnyConnect
Secure Mobility
Client\opswat</path><category>Unclassified</category></application><application><diff>0</diff><
id></id><name>Cisco AnyConnect ISE Posture Module</name><vendor>Cisco Systems,
Inc.</vendor><version>4.4.00209</version><path>C:\Program Files (x86)\Cisco\Cisco AnyConnect
Secure Mobility
Client</path><category>Unclassified</category><process><diff>0</diff><pid>704</pid><path>c:\pro
gram files (x86)\cisco\cisco anyconnect secure mobility
client\vpnagent.exe</path><hash>7D7502DE53F0282A7AFC98BE89F54D39FDEC3FAC2A1F32674C76967ADC695E09
</hash></process><process><diff>0</diff><pid>1296</pid><path>c:\program files (x86)\cisco\cisco
anyconnect secure mobility
client\aciseagent.exe</path><hash>7E156520C184334D473506FFE8A482997581ACF6ABD34231FDEDC2B9A3A120
66</hash></process><process><diff>0</diff><pid>3076</pid><path>c:\program files
(x86)\cisco\cisco anyconnect secure mobility
client\vpnui.exe</path><hash>0131258625A16B78125EB2081E8D5678671B6DE52DDA9E0813D4674618177DC3</h
ash></process><process><diff>0</diff><pid>3384</pid><path>c:\program files (x86)\cisco\cisco
anyconnect secure mobility
client\acise.exe</path><hash>8636F5761663A0EB9EDE263609B6AEF0EA52292E5B093AD4C453097583F365DD</h
ash></process><process><diff>0</diff><pid>15924</pid><path>c:\program files (x86)\cisco\cisco
anyconnect secure mobility
client\aciseposture.exe</path><hash>7FA4B3B6F688642E800AD53B865DBDCC163FBCA92D83482248DB068BA421
92EA</hash></process></application><application><diff>0</diff><id></id><name>Cisco AnyConnect
Profile Editor</name><vendor>Cisco Systems,
Inc.</vendor><version>4.1.08005</version><path>C:\Program Files (x86)\Cisco\Cisco AnyConnect
Profile
Editor</path><category>Unclassified</category></application><application><diff>0</diff><id></id
><name>Cisco AnyConnect Secure Mobility Client </name><vendor>Cisco Systems,
Inc.</vendor><version>4.4.00209</version><category>Unclassified</category></application><applica
tion><diff>0</diff><id></id><name>Cisco AnyConnect Secure Mobility Client</name><vendor>Cisco
Systems, Inc.</vendor><version>4.4.00209</version><path>C:\Program Files (x86)\Cisco\Cisco
AnyConnect Secure Mobility
Client</path><category>Unclassified</category><process><diff>0</diff><pid>704</pid><path>c:\pro
gram files (x86)\cisco\cisco anyconnect secure mobility
client\vpnagent.exe</path><hash>7D7502DE53F0282A7AFC98BE89F54D39FDEC3FAC2A1F32674C76967ADC695E09
</hash></process><process><diff>0</diff><pid>1296</pid><path>c:\program files (x86)\cisco\cisco
anyconnect secure mobility
client\aciseagent.exe</path><hash>7E156520C184334D473506FFE8A482997581ACF6ABD34231FDEDC2B9A3A120
66</hash></process><process><diff>0</diff><pid>3076</pid><path>c:\program files
(x86)\cisco\cisco anyconnect secure mobility
client\vpnui.exe</path><hash>0131258625A16B78125EB2081E8D5678671B6DE52DDA9E0813D4674618177DC3</h
ash></process><process><diff>0</diff><pid>3384</pid><path>c:\program files (x86)\cisco\cisco
anyconnect secure mobility
client\acise.exe</path><hash>8636F5761663A0EB9EDE263609B6AEF0EA52292E5B093AD4C453097583F365DD</h
ash></process><process><diff>0</diff><pid>15924</pid><path>c:\program files (x86)\cisco\cisco
anyconnect secure mobility
client\aciseposture.exe</path><hash>7FA4B3B6F688642E800AD53B865DBDCC163FBCA92D83482248DB068BA421
```

92EA</hash></process></application><application><diff>0</diff><id></id><name>Cisco NAC Agent
</name><vendor>Cisco Systems, Inc.</vendor><version>4.9.5.10</version><path>C:\Program Files
(x86)\Cisco\Cisco NAC
Agent\</path><category>Unclassified</category><process><diff>0</diff><pid>1444</pid><path>c:\pro
gram files (x86)\cisco\cisco nac
agent\nacagent.exe</path><hash>502EF2A864254A2DF555E029BE2C39E94B111E8B01534D7161826650DE4CEB4D<
</hash></process><process><diff>0</diff><pid>2320</pid><path>c:\program files (x86)\cisco\cisco
nac
agent\nacagentui.exe</path><hash>DC617419F082BEAF26521E48CB410282631F93F1359E604A4D3D181A04FEE1F
B</hash></process></application><application><diff>0</diff><id>293</id><name>DAEMON Tools
Lite</name><vendor>Disc Soft Ltd</vendor><version>4.49.1.0356</version><path>C:\Program Files
(x86)\DAEMON Tools
Lite\</path><category>Unclassified</category></application><application><diff>0</diff><id></id><
name>Digital Operatives PAINT
Beta</name><vendor></vendor><version>0.0</version><category>Unclassified</category></application
><application><diff>0</diff><id></id><name>FileZilla Server</name><vendor>FileZilla
Project</vendor><version>beta 0.9.44</version><path>C:\Program Files (x86)\FileZilla
Server\</path><category>Unclassified</category><process><diff>0</diff><pid>1408</pid><path>c:\pr
ogram files (x86)\filezilla server\filezilla
server.exe</path><hash>E8DB1409DB694A90C759F418346AE5D71014AE3513A8B865B50923AD0DFEE395</hash></
process><process><diff>0</diff><pid>2348</pid><path>c:\program files (x86)\filezilla
server\filezilla server
interface.exe</path><hash>F57B0A7F4A9EBAACC1A67323EBB93D96FA910524FAE842953551DBA103EF71C5</hash
></process></application><application><diff>0</diff><id>180</id><name>FileZilla</name><vendor>Fi
leZilla Project</vendor><version>3.8.1.0</version><path>C:\Program Files (x86)\FileZilla FTP
Client\</path><category>FileShare</category></application><application><diff>0</diff><id>39</id>
<name>Google Chrome</name><vendor>Google
Inc.</vendor><version>55.0.2883.87</version><path>C:\Program Files
(x86)\Google\Chrome\Application\</path><category>AntiPhishing, Browser</category></application><a
pplication><diff>0</diff><id></id><name>Google Update Helper</name><vendor>Google
Inc.</vendor><version>1.3.24.15</version><category>Unclassified</category></application><applica
tion><diff>0</diff><id>100</id><name>Internet Explorer</name><vendor>Microsoft
Corporation</vendor><version>11.0.9600.18524</version><path>C:\Program Files\Internet
Explorer\</path><category>AntiPhishing, Browser</category></application><application><diff>0</dif
f><id></id><name>Java 7 Update
79</name><vendor>Oracle</vendor><version>7.0.790</version><path>C:\Program Files
(x86)\Java\jre7\</path><category>Unclassified</category></application><application><diff>0</diff
><id></id><name>Java 8 Update 91</name><vendor>Oracle
Corporation</vendor><version>8.0.910.15</version><path>C:\Program Files
(x86)\Java\jre1.8.0_91\</path><category>Unclassified</category></application><application><diff>
0</diff><id></id><name>Java Auto Updater</name><vendor>Oracle
Corporation</vendor><version>2.8.91.15</version><category>Unclassified</category></application><
application><diff>0</diff><id>111</id><name>Java</name><vendor>Oracle
Corporation</vendor><version>7.0.790.15</version><path>C:\Program Files
(x86)\Java\jre7\bin\</path><category>Unclassified</category></application><application><diff>0</
diff><id>111</id><name>Java</name><vendor>Oracle
Corporation</vendor><version>8.0.910.15</version><path>C:\Program Files
(x86)\Java\jre1.8.0_91\bin\</path><category>Unclassified</category></application><application><d
iff>0</diff><id></id><name>Microsoft .NET Framework 4.6.1</name><vendor>Microsoft
Corporation</vendor><version>4.6.01055</version><path>C:\Windows\Microsoft.NET\Framework64\v4.0.
30319\SetupCache\v4.6.01055\</path><category>Unclassified</category></application><application><
diff>0</diff><id></id><name>Microsoft Network Monitor 3.4</name><vendor>Microsoft
Corporation</vendor><version>3.4.2350.0</version><category>Unclassified</category></application>
<application><diff>0</diff><id></id><name>Microsoft Network Monitor: NetworkMonitor Parsers
3.4</name><vendor>Microsoft
Corporation</vendor><version>3.4.2350.0</version><category>Unclassified</category></application>
<application><diff>0</diff><id></id><name>Microsoft Visual C++ 2008 Redistributable - x64
9.0.30729.4148</name><vendor>Microsoft
Corporation</vendor><version>9.0.30729.4148</version><category>Unclassified</category></applicat
ion><application><diff>0</diff><id></id><name>Microsoft Visual C++ 2008 Redistributable - x86
9.0.30729.4148</name><vendor>Microsoft
Corporation</vendor><version>9.0.30729.4148</version><category>Unclassified</category></applicat
ion><application><diff>0</diff><id>44</id><name>Mozilla Firefox</name><vendor>Mozilla
Corporation</vendor><version>47.0.2</version><path>C:\Program Files (x86)\Mozilla

Firefox\</path><category>AntiPhishing, Browser</category><process><diff>0</diff><pid>8292</pid><path>c:\program files (x86)\mozilla
firefox\firefox.exe</path><hash>47F80E4FC4C43FAF468D94F5D51AAC78A125CC720FCBEA0B88B5F29D06719CE9
</hash></process></application><application><diff>0</diff><id></id><name>Mozilla Maintenance
Service</name><vendor>Mozilla</vendor><version>47.0.2.6148</version><category>Unclassified</cate
gory></application><application><diff>0</diff><id>298</id><name>Notepad++</name><vendor>Notepad+
+ Team</vendor><version>6.63</version><path>C:\Program Files
(x86)\Notepad++\</path><category>Unclassified</category></application><application><diff>0</diff
><id></id><name>Security Update for Microsoft .NET Framework 4.6.1
(KB3122661)</name><vendor>Microsoft
Corporation</vendor><version>1</version><category>Unclassified</category></application><applicat
ion><diff>0</diff><id></id><name>Security Update for Microsoft .NET Framework 4.6.1
(KB3127233)</name><vendor>Microsoft
Corporation</vendor><version>1</version><category>Unclassified</category></application><applicat
ion><diff>0</diff><id></id><name>Security Update for Microsoft .NET Framework 4.6.1
(KB3136000v2)</name><vendor>Microsoft
Corporation</vendor><version>2</version><category>Unclassified</category></application><applicat
ion><diff>0</diff><id></id><name>Security Update for Microsoft .NET Framework 4.6.1
(KB3142037)</name><vendor>Microsoft
Corporation</vendor><version>1</version><category>Unclassified</category></application><applicat
ion><diff>0</diff><id></id><name>Security Update for Microsoft .NET Framework 4.6.1
(KB3143693)</name><vendor>Microsoft
Corporation</vendor><version>1</version><category>Unclassified</category></application><applicat
ion><diff>0</diff><id></id><name>Security Update for Microsoft .NET Framework 4.6.1
(KB3164025)</name><vendor>Microsoft
Corporation</vendor><version>1</version><category>Unclassified</category></application><applicat
ion><diff>0</diff><id></id><name>TP-LINK TL-WDN3200 Driver</name><vendor>TP-
LINK</vendor><version>1.1.0</version><path>C:\Program Files (x86)\TP-LINK\TP-LINK Wireless
Configuration Utility and
Driver\</path><category>Unclassified</category></application><application><diff>0</diff><id></id
><name>Tftpd32 Standalone Edition (remove
only)</name><vendor></vendor><version>0.0</version><category>Unclassified</category></applicatio
n><application><diff>0</diff><id></id><name>VMware Tools</name><vendor>VMware,
Inc.</vendor><version>9.4.15.2827462</version><path>C:\Program Files\VMware\VMware
Tools\</path><category>Unclassified</category><process><diff>0</diff><pid>952</pid><path>c:\prog
ram files\vmware\vmware
tools\vmtoolsd.exe</path><hash>5C642EF7F4EF65A0445B2C2CD227F9431835712EE7F1BD4D01D1F7472199DE47<
</hash></process><process><diff>0</diff><pid>1516</pid><path>c:\program files\vmware\vmware
tools\vmtoolsd.exe</path><hash>5C642EF7F4EF65A0445B2C2CD227F9431835712EE7F1BD4D01D1F7472199DE47<
</hash></process></application><application><diff>0</diff><id></id><name>WinPcap
4.1.3</name><vendor>Riverbed Technology,
Inc.</vendor><version>4.1.0.2980</version><category>Unclassified</category></application><applic
ation><diff>0</diff><id>300</id><name>WinPcap</name><vendor>Riverbed Technology,
Inc.</vendor><version>4.1.0.2980</version><path>C:\Program Files
(x86)\WinPcap\</path><category>Unclassified</category></application><application><diff>0</diff><
id>923</id><name>Windows Backup and Restore</name><vendor>Microsoft
Corporation</vendor><version>6.1.7600.16385</version><path>C:\Windows\System32\</path><category>
BackupClient</category></application><application><diff>0</diff><id>362</id><name>Windows
Defender</name><vendor>Microsoft
Corporation</vendor><version>6.1.7600.16385</version><path>C:\Program Files\Windows
Defender\</path><category>AntiMalware</category></application><application><diff>0</diff><id>283
</id><name>Windows Firewall</name><vendor>Microsoft
Corporation</vendor><version>6.1.7600.16385</version><path>C:\Windows\System32\</path><category>
FireWall</category></application><application><diff>0</diff><id>1612</id><name>Windows Media
Player</name><vendor>Microsoft
Corporation</vendor><version>12.0.7601.23517</version><path>C:\Program Files\Windows Media
Player\</path><category>Unclassified</category><process><diff>0</diff><pid>1596</pid><path>c:\pr
ogram files\windows media
player\wmpnetwk.exe</path><hash>306467D280E99D0616E839278A4DB5BED684F002AE284C3678CABB5251459CB3
</hash></process></application><application><diff>0</diff><id>1587</id><name>Windows Security
Health Agent</name><vendor>Microsoft
Corporation</vendor><version>6.1.7600.16385</version><path>C:\Windows\System32\</path><category>
HealthAgent</category></application><application><diff>0</diff><id>1090</id><name>Windows Update
Agent</name><vendor>Microsoft

```

Corporation</vendor><version>7.6.7601.19161</version><path>C:\Windows\System32\</path><category>
PatchManagement</category></application><application><diff>0</diff><id>1106</id><name>Windows
VPN Client</name><vendor>Microsoft
Corporation</vendor><version>6.1.7600.16385</version><path>C:\Windows\System32\</path><category>
VPNClient</category></application><application><diff>0</diff><id>207</id><name>Wireshark</name><
vendor>The Wireshark developer community</vendor><version>1.10.7</version><path>C:\Program Files
(x86)\Wireshark\</path><category>Unclassified</category></application></check></package></report
> ]]
...

```

Alle Berichte sind XML-Zeichenfolgen. Beispiel für einen formatierten Bericht:

```

<report>
<version>1000</version>
<package>
<id>12</id>
<status>1</status>
<check>
<chk_id>Apps_Collection</chk_id>
<diff>0</diff>
<application>
<diff>0</diff>
<id>104</id>
<name>Adobe Flash Player</name>
<vendor>Adobe Systems Inc.</vendor>
<version>23.0.0.207</version>
<path>C:\Windows\SysWOW64\Macromed\Flash\</path>
<category>Unclassified</category>
</application>
...
<application>
<diff>0</diff>
<id></id>
<name>Cisco AnyConnect ISE Posture Module</name>
<vendor>Cisco Systems, Inc.</vendor>
<version>4.4.00209</version>
<path>C:\Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility Client\</path>
<category>Unclassified</category>
<process>
<diff>0</diff>
<pid>704</pid>
<path>c:\program files (x86)\cisco\cisco anyconnect secure mobility client\vpnagent.exe</path>
<hash>7D7502DE53F0282A7AFC98BE89F54D39FDEC3FAC2A1F32674C76967ADC695E09</hash>
</process>
<process>
<diff>0</diff>
<pid>1296</pid>
<path>c:\program files (x86)\cisco\cisco anyconnect secure mobility client\aciseagent.exe</path>
<hash>7E156520C184334D473506FFE8A482997581ACF6ABD34231FDEDC2B9A3A12066</hash>
</process>
<process>
<diff>0</diff>
<pid>3076</pid>
<path>c:\program files (x86)\cisco\cisco anyconnect secure mobility client\vpnui.exe</path>
<hash>0131258625A16B78125EB2081E8D5678671B6DE52DDA9E0813D4674618177DC3</hash>
</process>
<process>
<diff>0</diff>
<pid>3384</pid>
<path>c:\program files (x86)\cisco\cisco anyconnect secure mobility client\acise.exe</path>
<hash>8636F5761663A0EB9EDE263609B6AEF0EA52292E5B093AD4C453097583F365DD</hash>
</process>
<process>

```

```
<diff>0</diff>
<pid>15924</pid>
<path>c:\program files (x86)\cisco\cisco anyconnect secure mobility
client\aciseposture.exe</path>
<hash>7FA4B3B6F688642E800AD53B865DBDCC163FBCA92D83482248DB068BA42192EA</hash>
</process>
</application>
... </check> </package> </report>
```

AnyConnect sendet vollständige Berichte nur bei der ersten Verbindung. Darüber hinaus werden nur Änderungen gesendet. Beispielsweise wurde Notepad++ nach einiger Zeit gestartet:

```
2017-01-04 19:24:37,929 DEBUG [http-bio-10.48.26.60-8443-exec-7][]
cisco.cpm.posture.runtime.PostureHandlerImpl -::::- Received posture request [parameters:
reqtype=, userip=10.62.148.162, clientmac=C0-4A-00-15-75-C8, os=, osVerison=1.2.1.6.1.4,
architecture=, provider=, state=, userAgent=Mozilla/4.0 (compatible; WINDOWS; 1.2.1.6.1.4;
AnyConnect Posture Agent v.4.4.00209), session_id=
2017-01-04 19:24:37,929 DEBUG [http-bio-10.48.26.60-8443-exec-7][]
cisco.cpm.posture.runtime.PostureHandlerImpl -::::- Found a session info for endpoint C0-4A-00-
15-75-C8 cisco
2017-01-04 19:24:37,929 DEBUG [http-bio-10.48.26.60-8443-exec-7][]
cisco.cpm.posture.runtime.PostureHandlerImpl -::::- Got userid cisco from cache for endpoint C0-
4A-00-15-75-C8/
2017-01-04 19:24:37,929 DEBUG [http-bio-10.48.26.60-8443-exec-7][]
cisco.cpm.posture.runtime.PostureHandlerImpl -::::- Report IV in Base64:
JjneGgZcJbmqMKQcy8kJg==
2017-01-04 19:24:37,929 DEBUG [http-bio-10.48.26.60-8443-exec-7][]
cisco.cpm.posture.runtime.PostureHandlerImpl -::::- Using AES shared secret to decrypt report.
2017-01-04 19:24:37,929 DEBUG [http-bio-10.48.26.60-8443-exec-7][]
cisco.cpm.posture.util.CipherUtil -::::- Decrypting message using AES.
2017-01-04 19:24:37,930 DEBUG [http-bio-10.48.26.60-8443-exec-7][]
cisco.cpm.posture.runtime.PostureHandlerImpl -::::- Decrypted report [[
<report><version>1000</version><package><id>12</id><status>1</status><check><chk_id>Apps_Collect
ion</chk_id><diff>1</diff><application><diff>2</diff><id>298</id>
```

```
<vendor>Notepad++ Team</vendor><version>6.63</version><path>C:\Program Files
(x86)\Notepad++\</path><category>Unclassified</category><process><diff>0</diff>
```

```
<path>c:\program files
(x86)\notepad++\notepad++.exe</path><hash>43E9F528CD2405E6DD117857D440A634769C6E11C4D986605354C2
605B6E7D84</hash></process></application></check></package></report> ]]
```

Formatiert:

```
<report>
<version>1000</version>
<package>
<id>12</id>
<status>1</status>
<check>
<chk_id>Apps_Collection</chk_id>
<diff>1</diff>
<application>
<diff>2</diff>
<id>298</id>
```

```
<vendor>Notepad++ Team</vendor>
<version>6.63</version>
<path>C:\Program Files (x86)\Notepad++\</path>
<category>Unclassified</category>
<process>
<diff>0</diff>
```

```
<path>c:\program files (x86)\notepad++\notepad++.exe</path>
<hash>43E9F528CD2405E6DD117857D440A634769C6E11C4D986605354C2605B6E7D84</hash>
</process>
</application>
</check>
</package>
</report>
```

Von AnyConnect

Die Datei **AnyConnect_ISEPosture.txt** enthält alle zugehörigen Protokolle und Debugger. Diese Datei finden Sie im DART-Paket, das auf einem Endgerät gesammelt wurde. Im folgenden Beispiel wird ein periodischer Bericht mit AES256 verschlüsselt:

```
Date       : 01/04/2017
Time       : 19:34:38
Type       : Unknown
Source     : acise
```

```
Description : Function: Authenticator::bldMonitorReport
Thread Id: 0xD3C
File: Authenticator.cpp
Line: 724
Level: info
```

Monitor Report:

```
&user_key=dummykey&cm=10&ops=1&mac_list=C0%3a4A%3a00%3a15%3a75%3aC8&ip_list=10%2e62%2e148%2e162&
hostname=TSOPREK%2dWIN7%2d1&udid=766bb955e51e4ab063fd478c63acee81260ca592&dm_report_client_IV=Jj
neGgZcJbmjqMKQcy8kJg%3d%3d&dm_report=2yWwY7QzHWCY%2fDVEESSAabEZtYLTxNE7Qgy00a85Dgo2Ts4ok8sIrBM37
S2%2fe2Hs0URCP4KkfY4Ap8%2bh%2fqS%2biw50CZejKG%2bVbF7RTRqZyrg2veWAwVEDsSb%2bqWRRdzvZfSjS3G4ApQi07
qnfExwN1IvCqrVOp1j17TAcVXEht8NkDg00T9jM%2fTNH%2fMK1lc0o6Ha5juJo4YtWDWY%2bnOancw%3d%3d.
```

```
Date       : 01/04/2017
Time       : 19:34:38
Type       : Unknown
Source     : acise
```

```
Description : Function: Authenticator::buildAndSendHttpMsg
Thread Id: 0xD3C
File: Authenticator.cpp
Line: 196
```


Level: debug

```
MSG_SN_HTTP_REQUEST, {{url="https://ise22-pri.example.com:8443/auth/perfigo_validate.jsp"},  
{server="ise22-pri.example.com"}, {method="post"}, {object_path=""}, {reuse_existing=1},  
{close_when_done=0},  
{pkt="&user_key=dummykey&cm=10&ops=1&mac_list=C0%3a4A%3a00%3a15%3a75%3aC8&ip_list=10%2e62%2e148%  
2e162&hostname=TSOPREK%2dWIN7%2d1&udid=766bb955e51e4ab063fd478c63acee81260ca592&dm_report_client  
_IV=JjneGgZcJbmjqMKQcy8kJg%3d%3d&dm_report=2yWwY7QzHWCY%2fDVEESSAabEZtYltxNE7Qgy0Oa85Dgo2Ts4ok8s  
IrBM37S2%2fe2HsOURCP4KkfY4Ap8%2bh%2fgS%2biw50CZeJkG%2bVbF7RTRqZyrg2veWAwvEDsSb%2bqWRRdzvZfSjS3G4  
ApQi07qnfExwN1IvCqrVOp1j17TAcVXEht8NkDg00T9jM%2fTNH%2fMK1lc0o6Ha5juJo4YtWDWY%2bnOancw%3d%3d"},  
{path=""}, {type=1}}.
```

Date : 01/04/2017
Time : 19:34:39
Type : Unknown
Source : acise

Description : Function: HttpHandler::createOutgoingHTTPSMessage
Thread Id: 0xD3C
File: HttpHandler.cpp
Line: 295
Level: debug

```
MSG_NS_HTTP_RESPONSE, {{success=1}, {pkt="<!--error=0--><!--X-Perfigo-DM-Error=0--><!--X-  
Perfigo-Monitoring-Interval=5-->"}, {type=1}}.
```

Häufige Probleme

AnyConnect kann ISE nicht erreichen

In diesem Fall enthält AnyConnect_ISEPosture.txt Fehler:

Date : 01/04/2017
Time : 20:04:40
Type : Unknown
Source : acise

Description : Function: Authenticator::buildAndSendHttpMsg
Thread Id: 0xD3C
File: Authenticator.cpp
Line: 196
Level: debug

```
MSG_SN_HTTP_REQUEST, {{url="https://ise22-pri.example.com:8443/auth/perfigo_validate.jsp"},  
{server="ise22-pri.example.com"}, {method="post"}, {object_path=""}, {reuse_existing=1},  
{close_when_done=0},  
{pkt="&user_key=dummykey&cm=10&ops=1&mac_list=C0%3a4A%3a00%3a15%3a75%3aC8&ip_list=10%2e62%2e148%  
2e162&hostname=TSOPREK%2dWIN7%2d1&udid=766bb955e51e4ab063fd478c63acee81260ca592&dm_report_client  
_IV=JjneGgZcJbmjqMKQcy8kJg%3d%3d&dm_report=2yWwY7QzHWCY%2fDVEESSAabEZtYltxNE7Qgy0Oa85Dgo2Ts4ok8s  
IrBM37S2%2fe2HsOURCP4KkfY4Ap8%2bh%2fgS%2biw50CZeJkG%2bVbF7RTRqZyrg2veWAwvEDsSb%2bqWRRdzvZfSjS3G4  
ApQi07qnfExwN1Pdu7AztTn%2f3VYph9WNF1jG1jXSuTFm38e%2bVbDXQnx7avYHs9meVItYqA6MecAJK3WdkBNSrK1bYjmI  
vzkAPqR2LuoflnA9IcNOTZQ9iN%2fknOjllQsiV5eV6jLMSUeOakKsTwylgbPsFz99eKdtaCMv1F%2fSAmvLApjpke0IMKor  
XXkvpJURtAtOMK75ltXdykC85ihgHcI10JW7mlpvIppk5MbcZjihQbXldr5%2fQVdpB8eRqMHF1iCK1gx961wwdzBSfr%2bg  
rcF4072fYYNOa9cYnTFShgU%2bxrnBDcJ1GUoYE9K5nTfGQ01p4NrcbLjpm79e14v14YgfQhmSfktwxFA8pY7A6jml3BIp30  
9gmQVnoTgaaccqk76uT%2bPkjV0yrOgdG0CYwUwUMVqpctGKorxx1C3IwXhBWUmvRY9p2LRdePRqncN8hpiesyk%2bzTnyX  
00aNdHD6%2bGEMGo9QjQvwrL9dcvrUxxHtlQcJPeKXajXPfn98FpC8z%2b966tcz4DfMN6giSlEfK6y5%2bMpk0oAL%2fV4X  
Mg296PDocGaetK1OUR7Qkl%2b7S2fv%2fcfZdiQaTndZ6zHwUimq5JBRELmuKI9hWRN2cPERcDn64ISZZSiz9yPoJPlPPpFs
```

fggk2PdS00EEtMiM%2bBjNKcFx2Tcsq76eYfDtvDq9tGzjST8opInlIiXdAzdbeWsjCAerCvS73xg2vd2DHfpFlrd5lVa3q
wo3Vov3nFiAz4l3IrI1fOHjAE7rCZTy2dWU455icOjm0%2bCVAS3SzWcea4fZu3fAhmIhAVQKE1cFZ4CyyBv89340Vw62Bxu
5ij0wbH0STAsTsbxJXyuGBw8cqTPfuUtqPLx6nWtCRZ6p13MuQTq%2bKZLZ7hwY2Urf1o1Gi9OPGyo5zuJZAUQInU%2bkJKU
6ycXHZo17Uti3DITCy0%2fG%2bQ2gixzBIpmJctekKJO243rZiU1wbOUPWLzGum8ydRu3im2LiDisXquAu7ipY5P0D475AZN
3Cd6nlIPP5Mora493QhX4I139q%2birT1%2f5F7tI%2fKLv20FWFC%2fjKbfu%2bFe4QIbdtiSCvLkyZ%2bWdWBMWSXHGE11
CoErbj4LJP3h4oqLto17riGCMb%2bRHZXNJA2bwjcfgy4w2FE4hrL0cC6D3YgZxHHpUeT4gMXoXj0EJwODxQwElc9yfoe%2
bDgJ4Fy6%2fXc0ymDFYU7oOouAc0nwPKZwhZn4Q3mMZIG5aeOfcx9IM6M47IcMMbo0r78aUk8M94h5f4sK6JxHz75B6JyTx3
H%2bXFDJ3j5UtUYj1oir4CLQJgR8ABhMDGxqhAN4c4wA4y790bh2F5PxxVXMGYb4ghFNt3jIHGXRMenPTYkelND0falMmhJ
UXE%2fVashJ8aZwcGCU%2fNhSkCATRXb5UDameaSkwe3m4bcRtFbBNZ115CNQVH8ZPzSK1GCNpD6dOYkSxa%2ffErYqImEzm
9itwSzUujQXI%2f8%2f2fKewc9jeBujwHqnjuIYg5sJbjk%2bqc%2fwy5hKHTbxFacnFJ1gvJhHt3mht8oRC9EbbsULoAK1
fvLe4%2fE%2bqFjOe02bw4sQuu1ssMKxLsNQMCITIZFzh10K6BZdfo1RonKG0MEG1K%2ftSDNC4eyQw9ewYhgzopzDVHw1yprp
VY9UgcTvFVSh0Vy%2bWde4b0dtmPdhhQhvvsQOSgnIX6a8GN4AwXEOE7CoP6%2fFziTAJTuxUKMjC1m8iAsrAurJugnEgaK
KugSNk19y7bgSiYB6zkthDclEyBFWc1rAecfH6oMJs59aJodXnPSAA9FuyqLCWB%2f3WFZ03efhTviz2101G8%2fswMxR0w%
2fR56oNH2wzUwkmh9oczFaYLPzPg6k47ohlzmDJraqyvWgzZfPIipa7EKK8Yvsu04BCFGMrDZtYZnCO6B9CFoKDCNJE9Wxl
%2bhTdzFCA4GpeLE4nT7y1j113iTV%2faWyImNLARMU2ZiwuKy%2bd2OH55LqnLBCxrUUIMH7Ku4Mhd%2fYvw1NVpcZZ0L%2
bWOkMoephk2XXE4OQAY7Rk%2f%2fRncbbH1FOVQmEVOoxNneBEllEajK%2fxX6C0BZBaebAVYluwdGkkktvgQ5gUvzMiyqbs
vzyUMzq%2fhqKY7vMWUeyCsBnybuGPSILJikMgdgiz%2baUZsOyZsUE%2b7PPyiqphqXNRfQ6tj8wTzq7a2Z5XgCYI10Pi
qjlmq6hY1TiRYuPanyBqh61LfkxblkpQJX2339pqB4RBOzF4%2f3CsvfjU302NSU9fypX5dBYubAZt80DOBe84FSnQIX3pfx
2%2fw9LqclYwbc2QSOfoHoe6TgkCiOall%2fqUHWqeOogbgLO5s5ffBoNmUCxhJW%2fH1EqKcsFzA%2ba%2f2Q0%2bs2m99R
qlxdd55bg67LXVPGfKh2dbVHjghXj090nLEtVwCfs8oMUIg%2bmnip%2fdA7wDz4Nsma2W0ugEhOjppfFbL2TxHLhE0r%2bwy
3t%2bosvtaXNJZg84LJKpt3J%2bmc0pnIBH5S5H7zrNDKUnIYXY8BD5n1clZi4wwkRIp62avJw7lN22zNHsjp7NUjTYw9X%2
f1Iti1TKxjPZuitU%2bITeCRRHzeoaeGbzE1E%2bGSSqemw7F1wx4w9JXHDAjH%2bY4iX7z2Y4OrY1JQQleeS9KWzw5HdiCp
uHmhMtLMSpz%2fGagw7KeaLEe9FwxrOYILS%2fXuBSTz1XOpbQHilH0ZdQbv2I%2bA%2f3j3GvalSul%2f0YVWlPPPIC2Ogk
SSbd4HyXXh9TEB8dhDmfucy5VEZ5MsuOTgytkALNSK0t9cyvsAcWTQf0uVAMnyBeaMPJAvdE9fXUiH628eMD9PHvt3cL0GYd
RR9WBUCszIFTJNIA5AXj7abdbc6VZ8DqX4YfJ1xgTgg2qKSJqXvtbi5BJU49BGaxu01Ta6eBo2ABLtgBxKzb8DYNyqyqRB%2
bYkgr5YdU6z6va15jQJYGUJYVwZ8xDsKvYHz1fUFAHldzxxkq44myNAjD1H0DoYhQaXU120UXkg09w5kBgTfmKj9DOJhs5Q88
ilebAbHHxm3GTZSJP51jQjsPSU13doX3Mz8E7W5pYptxtW1XPwcSHhkxuhWjBVKKQRTgM5uSXCPQ0PDAqcc6NybV2t1BK3G
hQSPzqsQ5k3wklDK7CYuUWMPKTMNLZDVF8i25DoGpA0K5m5s3VMAukLA9Gob5ysU%2fsu2TVBrJZD0sa3L%2bNoF2b01f8BC3
2e.

Date : 01/04/2017
Time : 20:04:41
Type : Unknown
Source : acise

Description : Function: hs_transport_winhttp_post
Thread Id: 0xD3C
File: hs_transport_winhttp.c
Line: 5776
Level: debug

unable to send request: 12029.

Date : 01/04/2017
Time : 20:04:41
Type : Unknown
Source : acise

Description : Function: HttpHandler::createOutgoingHTTPSMessage
Thread Id: 0xD3C
File: HttpHandler.cpp
Line: 295
Level: debug

MSG_NS_HTTP_RESPONSE, {{success=0}, {pkt=""}, {type=1}}.

Date : 01/04/2017
Time : 20:04:41

Type : Error
Source : acise

Description : Function: Authenticator::parsePostureData
Thread Id: 0xD3C
File: Authenticator.cpp
Line: 257
Level: error

Failed to communicate with CAS..

Date : 01/04/2017
Time : 20:04:41
Type : Error
Source : acise

Description : Function: SMNavPosture::SMP_handleMonitorResp
Thread Id: 0xD3C
File: SMNavPosture.cpp
Line: 495
Level: error

Failed to parse monitor response.

ISE löst beim Erstellen von Anwendungs-Compliance aus der EP-Ansicht den Fehler "Null" aus

Der häufigste Grund dafür, dass bei der Erstellung der Anwendungs-Compliance aus der EP-Ansicht die Meldung "Null" angezeigt wird, ist das Fehlen der erforderlichen OPSWAT-Diagramme. Dieses Problem kann durch Statusaktualisierungen auf die neueste Version behoben werden.