

Wi-Fi-Analysen für die Endgeräteklassifizierung auf der ISE 3.3

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Konfigurationen auf dem WLC](#)

[Schritt 1: Globale Aktivierung der Geräteklassifizierungsfunktion](#)

[Schritt 2: TLV-Caching und RADIUS-Profilerstellung aktivieren](#)

[Konfigurationen auf der ISE](#)

[Schritt 1: Aktivieren von Profiling Services in den PSNs der Bereitstellung](#)

[Schritt 2: Aktivieren Sie den RADIUS Profiling Probe auf ISE PSN.](#)

[Schritt 3: CoA-Typ und Endpunkt-Attributfilter festlegen](#)

[Schritt 4: Autorisierungsrichtlinien mit Datenattributen von Wi-Fi-Analysen konfigurieren](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Schritt 1: Buchungspakete erreichen ISE](#)

[Schritt 2: ISE analysiert das Abrechnungspaket mit den Endpunkt-Attributen](#)

[Schritt 3: Endpunkteigenschaften werden aktualisiert und Endpunkte klassifiziert](#)

[Schritt 4: CoA und Neuauthentifizierung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird die Funktionsweise von Wi-Fi Analytics für die Endpunktklassifizierung beschrieben. Außerdem wird beschrieben, wie Sie diese konfigurieren, überprüfen und Fehler beheben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Konfiguration der 9800 Wireless LAN Controller (WLC)
- Identity Services Engine (ISE)-Konfiguration
- RADIUS-Authentifizierung. AAA-Paketfluss und -terminologie (Authorization and Accounting)

In diesem Dokument wird davon ausgegangen, dass bereits ein funktionierendes WLAN vorhanden ist, das Clients authentifiziert, die die ISE als RADIUS-Server verwenden.

Damit diese Funktion funktioniert, müssen mindestens folgende Voraussetzungen erfüllt sein:

- 9800 WLC Cisco IOS® XE Dublin 17.10.1
- Identifizieren der Services Engine v3.3
- 802.11ac Wave2 oder 802.11ax (Wi-Fi 6/6E) Access Points

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- 9800 WLC Cisco IOSXE v17.12.x
- Identity Services Engine (ISE) v3.3
- Android 13-Gerät

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

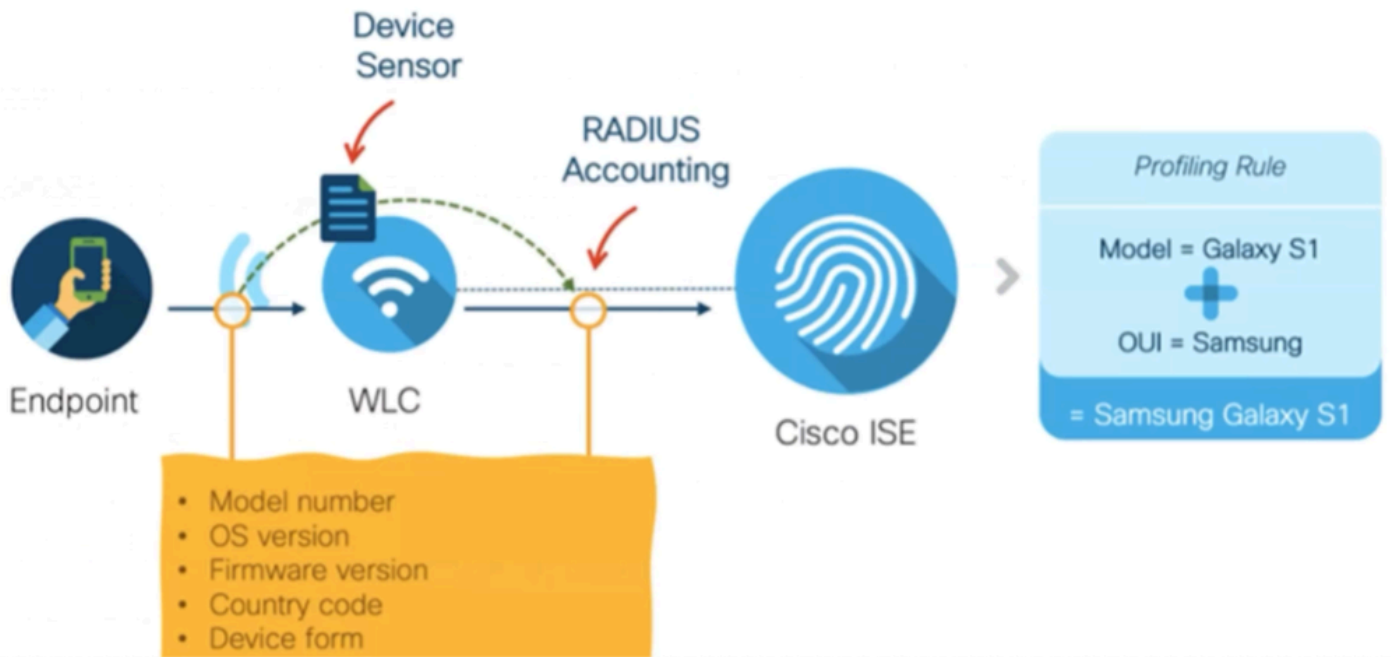
Hintergrundinformationen

Mithilfe von Wi-Fi-Geräteanalysen kann der Cisco 9800 WLC Attribute wie Modellnummer und Betriebssystemversion von einer Reihe von Endgeräten abrufen, die mit diesem Gerät verbunden sind, und diese für die ISE freigeben. Die ISE kann diese Informationen dann für die Endpunktklassifizierung, auch als Profilerstellung bekannt, verwenden.

Wi-Fi-Analysen werden derzeit von folgenden Anbietern unterstützt:

- Apfel
- Intel
- Samsung

Der WLC teilt die Attributinformationen mithilfe von RADIUS-Accounting-Paketen mit dem ISE-Server



WiFi Analytics-Datenfluss

Es ist wichtig zu beachten, dass RADIUS-Accounting-Pakete in einem RADIUS-AAA-Fluss erst gesendet werden, nachdem der RADIUS-Server ein RADIUS-Access-Accept-Paket als Antwort auf den Endpunkt-Authentifizierungsversuch gesendet hat. In dieser Reihenfolge gibt der WLC die Attributinformationen des Endpunkts erst frei, nachdem eine RADIUS-Sitzung für diesen Endpunkt zwischen dem RADIUS-Server (ISE) und dem Netzwerkzugriffgerät (WLC) eingerichtet wurde.

Die ISE kann die folgenden Attribute für die Endpunktklassifizierung und -autorisierung nutzen:

- GERÄTEINFORMATIONEN_FIRMWARE_VERSION
- GERÄTEINFORMATIONEN_HW_MODELL
- GERÄTEINFORMATIONEN_HERSTELLER_MODELL
- GERÄTEINFORMATIONEN_MODELLNAME
- GERÄTEINFORMATIONEN_MODELL_NUMMER
- GERÄTEINFORMATIONEN, BETRIEBSSYSTEMVERSION
- GERÄTEINFORMATIONEN ANBIERTERTYP



Hinweis: WLC kann je nach Verbindungstyp des Endpunkts weitere Attribute senden, aber nur die aufgeführten Attribute können für die Erstellung von Autorisierungsrichtlinien in der ISE verwendet werden.

Sobald die ISE das Abrechnungspaket erhält, kann sie die darin enthaltenen Analysedaten verarbeiten und nutzen und damit ein Endpunktprofil bzw. eine Endpunktgruppe neu zuweisen.

Die Attribute von WiFi Endpoint Analytics werden im Wörterbuch `WiFi_Device_Analytics` aufgeführt. Netzwerkadministratoren können diese Attribute in die Endpunkt-Autorisierungsrichtlinien und -bedingungen integrieren.

Select attribute for condition



| | Dictionary | Attribute | ID | Info |
|--|---------------------------|--------------------------|----|------|
| | Wifi_Device_Analytics ✓ X | Attribute | ID | |
| | Wifi_Device_Analytics | DEVICE_INFO_FIRMWARE_... | | |
| | Wifi_Device_Analytics | DEVICE_INFO_HW_MODEL | | |
| | Wifi_Device_Analytics | DEVICE_INFO_MANUFACT... | | |
| | Wifi_Device_Analytics | DEVICE_INFO_MODEL_NA... | | |
| | Wifi_Device_Analytics | DEVICE_INFO_MODEL_NUM | | |
| | Wifi_Device_Analytics | DEVICE_INFO_OS_VERSION | | |
| | Wifi_Device_Analytics | DEVICE_INFO_VENDOR_T... | | |

Wi-Fi Device Analytics-Wörterbuch

Wenn Änderungen an den aktuellen Attributwerten vorgenommen werden, die ISE für den Endpunkt speichert, initiiert ISE eine Autorisierungsänderung (Change of Authorization, CoA), sodass der Endpunkt unter Berücksichtigung der aktualisierten Attribute ausgewertet werden kann.

Konfigurieren

Konfigurationen auf dem WLC

Schritt 1: Globale Aktivierung der Geräteklassifizierungsfunktion

Navigieren Sie zu Konfiguration > Wireless > Wireless Global, und aktivieren Sie das Kontrollkästchen Geräteklassifizierung.

| | |
|----------------------------------|--------------------------------------|
| Default Mobility Domain * | <input type="text" value="default"/> |
| RF Group Name* | <input type="text" value="default"/> |
| Maximum Login Sessions Per User* | <input type="text" value="0"/> |
| Management Via Wireless | <input type="checkbox"/> |
| Device Classification | <input checked="" type="checkbox"/> |
| AP LAG Mode | <input type="checkbox"/> |
| Dot15 Radio | <input type="checkbox"/> |
| Wireless Password Policy | <input type="text" value="None"/> ⓘ |

Konfiguration der Geräteklassifizierung

Schritt 2: TLV-Caching und RADIUS-Profilerstellung aktivieren

Navigieren Sie zu Configuration > Tags and Profiles > Policy, und wählen Sie das Policy Profile (Richtlinienprofil) aus, das vom WLAN verwendet wird, mit dem die RADIUS-Clients verbunden sind.

| Admin Status | Associated Policy Tags | Policy Profile Name | Description |
|--------------------------|------------------------|------------------------|------------------------|
| <input type="checkbox"/> | ✔ | ise-policy | |
| <input type="checkbox"/> | ⊘ | default-policy-profile | default policy profile |

Wireless-Richtlinienauswahl

Klicken Sie auf Access Policies (Zugriffsrichtlinien), und überprüfen Sie die Optionen RADIUS Profiling, HTTP TLV Caching und DHCP TLV Caching. Aufgrund der im vorherigen Schritt

ergriffenen Maßnahmen wird der Status "Global State of Device Classification" jetzt als "Enabled" (Aktiviert) angezeigt.

Edit Policy Profile ✕

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General **Access Policies** QOS and AVC Mobility Advanced

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

WLAN Local Profiling

Global State of Device Classification **Enabled** ⓘ

Local Subscriber Policy Name ⓘ

VLAN

VLAN/VLAN Group ⓘ

Multicast VLAN

WLAN ACL

IPv4 ACL ⓘ

IPv6 ACL ⓘ

URL Filters ⓘ

Pre Auth ⓘ

Post Auth ⓘ

Konfiguration von RADIUS-Profilerstellung und -Caching

Melden Sie sich bei der WLC-CLI an, und aktivieren Sie dot11 TLV Accounting.

```
vimontes-wlc#configure terminal
vimontes-wlc(config)#wireless profile policy policy-profile-name
vimontes-wlc(config-wireless-policy)#dot11-tlv-accounting
```





Hinweis: Das Wireless-Richtlinienprofil muss deaktiviert werden, bevor dieser Befehl verwendet werden kann. Dieser Befehl ist nur in der Version Cisco IOS XE Dublin 17.10.1 und höher verfügbar.







Konfigurationen auf der ISE


Schritt 1: Aktivieren von Profiling Services in den PSNs der Bereitstellung

Navigieren Sie zu **Administration > Deployment**, und klicken Sie auf den Namen des PSN.

Deployment Nodes

Selected 0 Total 1  

 Edit  Register  Syncup  Deregister All  


| <input type="checkbox"/> | Hostname | Personas | Role(s) | Services | Node Status |
|--------------------------|----------|--|------------|------------------|---|
| <input type="checkbox"/> | iselab | Administration, Monitoring, Policy Service | STANDALONE | SESSION,PROFILER |  |


ISE PSN-Knotenauswahl


Blättern Sie nach unten zum Abschnitt **Richtliniendienst**, und markieren Sie das Kontrollkästchen **Profildienst aktivieren**. Klicken Sie auf die Schaltfläche **Speichern**.


Policy Service


Enable Session Services


Include Node in Node Group 


Enable Profiling Service 

Enable Threat Centric NAC Service 

> Enable SXP Service 

Enable Device Admin Service 

Enable Passive Identity Service 

> pxGrid 

[Reset](#)

Konfiguration der Profilerdienste

Schritt 2: Aktivieren Sie den RADIUS Profiling Probe auf ISE PSN.

Blättern Sie zum Seitenanfang, und klicken Sie auf die Registerkarte **Profiling Configuration**. Es werden alle Profilerstellungs sonden angezeigt, die auf der ISE verwendet werden können. Aktivieren Sie den **RADIUS-Datensensor**, und klicken Sie auf **Speichern**.

Edit Node

General Settings

Profiling Configuration

> NETFLOW

> DHCP

> DHCPSPAN

> HTTP

Hinweis: Das CoA-Paket enthält immer ein leeres Identitätsfeld, die Endpunkt-ID ist jedoch mit der ID des ersten Authentifizierungspakets identisch.

Klicken Sie im Datensatz für die Autorisierungsänderung in der Spalte **Details** auf das **Symbol**.

Sep 27, 2023 06:19:24.36...



0A:5A:F0:B3:B5:9C

Zugriff auf CoA-Paketdetails

Die detaillierten CoA-Informationen werden in einer neuen Browser-Registerkarte angezeigt. Blättern Sie nach unten zum Abschnitt **Andere Attribute**.

Die CoA-Quellkomponente wird als Profiler angezeigt. Der CoA-Grund wird als "Change in endpoint identity group/policy/logical profile" (Änderung der Endpunkt-Identitätsgruppe/des logischen Profils) angezeigt, die in Autorisierungsrichtlinien verwendet werden.

Other Attributes

| | |
|------------------------|---|
| ConfigVersionId | 1493 |
| Event-Timestamp | 1695838764 |
| Device CoA type | Cisco CoA |
| Device CoA port | 1700 |
| NetworkDeviceProfileId | b0699505-3150-4215-a80e-6753d45bf56c |
| IsThirdPartyDeviceFlow | false |
| AcsSessionID | 89f67978-be8f-4145-8801-45e2fffa1fe8 |
| TotalAuthenLatency | 3621649740 |
| ClientLatency | 3621649732 |
| CoASourceComponent | Profiler |
| CoAReason | Change in endpoint identity group/policy/logical profile which are used in authorization policies |
| Network Device Profile | Cisco |
| Location | Location#All Locations |
| Device Type | Device Type#All Device Types |
| IPSEC | IPSEC#Is IPSEC Device#No |
| Device IP Address | 172.16.5.169 |
| CPMSessionID | A90510AC00000058D7DD0AA7 |
| CiscoAVPair | subscriber:reauthenticate-type=last, subscriber:command=reauthenticate, audit-session-id=A90510AC00000058D7DD0AA7 |

CoA-auslösende Komponente und Grund

Navigieren Sie zur Registerkarte **Context Visibility > Endpoints > Authentication**. Verwenden Sie auf dieser Registerkarte die Filter, um den Testendpunkt zu finden.

Klicken Sie auf die **Endpunkt-MAC-Adresse**, um auf die **Endpunkteigenschaften** zuzugreifen.

| <input type="checkbox"/> | MAC Address | Status | IP Address | Username | Hostname | Location | Endpoint Profile | Authen... | Authentication ... | Authorization P... |
|-------------------------------------|-------------------|--------|------------|----------|--------------|-------------|------------------|------------|----------------------|------------------------|
| <input checked="" type="checkbox"/> | 0A:5A:F0:B3:B5:9C | Status | IP Address | Username | Hostname | Location | Endpoint Profile | Authentic: | Authentication Polic | Authorization Policy |
| <input type="checkbox"/> | 0A:5A:F0:B3:B5:9C | ... | | bob | Victor-s-S22 | Location... | Android | - | Default | Wifi Endpoint Analy... |

Endgerät zur Kontextsensitivität

Mit dieser Aktion werden alle Informationen angezeigt, die die ISE über diesen Endpunkt speichert. Klicken Sie auf **Attribute**, und wählen Sie dann **Andere Attribute** aus.

MAC ADDRESS: 0A:5A:F0:B3:B5:9C

Username: bob
Endpoint Profile: Android
Current IP Address: -
Location: Location → All Locations

MFC Endpoint Type: Phone
MFC Hardware Manufacturer: Samsung Electronics Co.,Ltd
MFC Hardware Model: Samsung Galaxy S22+
MFC Operating System: Android 13

Applications: **Attributes** | Authentication | Threats | Vulnerabilities

General Attributes | Custom Attributes | **Other Attributes**

Auswahl anderer Attribute für Endpunkt auf Kontexttransparenz

Blättern Sie nach unten, bis Sie die Attribute des **Wörterbuchs WiFi_Device_Analytics** gefunden haben. Wenn Sie diese Attribute in diesem Abschnitt finden, bedeutet dies, dass die ISE sie erfolgreich über die Accounting-Pakete empfangen hat und für die Endpunktklassifizierung verwendet werden kann.

| | |
|------------------------------|---------------------|
| DEVICE_INFO_COUNTRY_CODE | Unknown |
| DEVICE_INFO_DEVICE_FORM | PHONE |
| DEVICE_INFO_FIRMWARE_VERSION | WH6 |
| DEVICE_INFO_MODEL_NUM | Samsung Galaxy S22+ |
| DEVICE_INFO_OS_VERSION | Android 13 |
| DEVICE_INFO_SALES_CODE | MXO |
| DEVICE_INFO_VENDOR_TYPE | SAMSUNG |

Wi-Fi-Analyseattribute für Kontexttransparenz

Hier finden Sie Beispiele für Windows 10- und iPhone-Attribute:

| | |
|-------------------------------|--------------|
| DEVICE_INFO_DEVICE_FORM | 0 |
| DEVICE_INFO_FIRMWARE_VERSION | 22.180.02.01 |
| DEVICE_INFO_HW_MODEL | AX201/AX1650 |
| 160MHZ | |
| DEVICE_INFO_MANUFACTURER_NAME | LENOVO |
| DEVICE_INFO_MODEL_NAME | 20RAS0C000 |
| DEVICE_INFO_MODEL_NUM | LENOVO |
| 20RAS0C000 | |
| DEVICE_INFO_OS_VERSION | WINDOWS 10 |
| DEVICE_INFO_POWER_TYPE | AC POWERED |
| DEVICE_INFO_VENDOR_TYPE | 3 |

Beispiel für Windows 10-Endgeräteattribute

| | |
|-------------------------|----------|
| DEVICE_INFO_DEVICE_FORM | 0 |
| DEVICE_INFO_MODEL_NUM | IPHONE |
| 11 PRO | |
| DEVICE_INFO_OS_VERSION | IOS 16.4 |
| DEVICE_INFO_VENDOR_TYPE | 1 |

*für
iPhone-Endgeräteattribute*

Fehlerbehebung

Schritt 1: Buchungspakete erreichen ISE

Stellen Sie in der WLC-CLI sicher, dass **DOT11 TLV-Accounting**, **DHCP TLV-Caching** und **HTTP TLV-Caching** in den Richtlinienprofilkonfigurationen aktiviert sind.

```
<#root>
```

```
vimontes-wlc#show running-config | section wireless profile policy policy-profile-name
wireless profile policy policy-profile-name
aaa-override
accounting-list AAA-LIST
```

```
dhcp-tlv-caching
```

```
dot11-tlv-accounting
```

```
http-tlv-caching
```

```
radius-profiling
```

```
no shutdown
```

Sammeln von **Paketerfassungen** an WLC- oder ISE-Enden beim Verbinden eines Endpunkts Sie können jedes bekannte Paketanalyse-Tool wie Wireshark verwenden, um die gesammelten Dateien zu analysieren.

Filtern Sie nach RADIUS-Accounting-Paketen und nach Calling Station ID (Test-Endpunkt-MAC-Adresse). Dieser Filter kann z. B. verwendet werden:

```
radius.code == 4 && radius.Calling_Station_Id == "xx-xx-xx-xx-xx-xx"
```

Erweitern Sie nach dem Auffinden die Felder **Cisco-AVPair**, um die **WiFi-Analysedaten** im Abrechnungspaket zu finden.

```

No. | Time | Source | Destination | Protocol | Length | Info
---|---|---|---|---|---|---
104 2023-09-27 12:19:23.584661 172.16.5.169 172.16.5.112 RADIUS 976 Accounting-Request id=39

> AVP: t=Vendor-Specific(26) l=28 vnd=ciscoSystems(9)
> AVP: t=Vendor-Specific(26) l=36 vnd=ciscoSystems(9)
> AVP: t=Vendor-Specific(26) l=39 vnd=ciscoSystems(9)
> AVP: t=Vendor-Specific(26) l=36 vnd=ciscoSystems(9)
> AVP: t=Vendor-Specific(26) l=49 vnd=ciscoSystems(9)
  Type: 26
  Length: 49
  Vendor ID: ciscoSystems (9)
  > VSA: t=Cisco-AVPair(1) l=43 val=dot11-device-info=\000\000\000\023Samsung Galaxy S22+
> AVP: t=Vendor-Specific(26) l=33 vnd=ciscoSystems(9)
  Type: 26
  Length: 33
  Vendor ID: ciscoSystems (9)
  > VSA: t=Cisco-AVPair(1) l=27 val=dot11-device-info=\000\001\000\003WH6
> AVP: t=Vendor-Specific(26) l=33 vnd=ciscoSystems(9)
  Type: 26
  Length: 33
  Vendor ID: ciscoSystems (9)
  > VSA: t=Cisco-AVPair(1) l=27 val=dot11-device-info=\000\002\000\003MX0
> AVP: t=Vendor-Specific(26) l=31 vnd=ciscoSystems(9)
  Type: 26
  Length: 31
  Vendor ID: ciscoSystems (9)
  > VSA: t=Cisco-AVPair(1) l=25 val=dot11-device-info=\000\003\000\0011
> AVP: t=Vendor-Specific(26) l=40 vnd=ciscoSystems(9)
  Type: 26
  Length: 40
  Vendor ID: ciscoSystems (9)
  > VSA: t=Cisco-AVPair(1) l=34 val=dot11-device-info=\000\004\000\Android 13
> AVP: t=Vendor-Specific(26) l=37 vnd=ciscoSystems(9)
  Type: 26
  Length: 37
  Vendor ID: ciscoSystems (9)
  > VSA: t=Cisco-AVPair(1) l=31 val=dot11-device-info=\000\005\000\Unknown
> AVP: t=Vendor-Specific(26) l=31 vnd=ciscoSystems(9)
  Type: 26
  Length: 31
  Vendor ID: ciscoSystems (9)
  > VSA: t=Cisco-AVPair(1) l=25 val=dot11-device-info=\000\n\000\0012
> AVP: t=Framed-IP-Address(8) l=6 val=172.16.5.76

```

Endpunkt-TLV-Attribute in einem Buchungspaket

Schritt 2: ISE analysiert das Abrechnungspaket mit den Endpunkt-Attributen

Auf ISE-Ebene können diese Komponenten auf die DEBUG-Ebene gesetzt werden, um sicherzustellen, dass die vom WLC gesendeten RADIUS-Accounting-Pakete die ISE erreichen und ordnungsgemäß verarbeitet werden.

Sie können dann das **ISE-Supportpaket** sammeln, um die Protokolldateien zu sammeln. Weitere Informationen zum Sammeln von Support-Paketen finden Sie im Abschnitt **Zugehörige Informationen**.

| Component Name | Log Level | Description | Log file Name |
|----------------|-----------|-----------------------------|-----------------|
| Component Name | DEBUG | Description | Log file Name |
| nsf | DEB... ▾ | NSF related messages | ise-psc.log |
| nsf-session | DEB... ▾ | Session cache messages | ise-psc.log |
| profiler | DEB... ▾ | profiler debug messages | profiler.log |
| runtime-AAA | DEB... ▾ | AAA runtime messages (prrt) | prrt-server.log |

Komponenten, die zur Fehlerbehebung debuggt werden müssen



Hinweis: Komponenten sind nur auf dem PSN, das die Endpunkte authentifiziert, für die DEBUG-Ebene aktiviert.

Auf iseLocalStore.log wird die Accounting-Start-Nachricht protokolliert, ohne dass eine Komponente auf DEBUG-Ebene aktiviert werden muss. Hier muss die ISE das eingehende Abrechnungspaket mit den WiFi-Analyseattributen sehen.

<#root>

2023-09-27 18:19:23.600 +00:00 0000035538 3000

NOTICE Radius-Accounting: RADIUS Accounting start request,

ConfigVersionId=1493,
Device IP Address=172.16.5.169,

cisco-av-pair=dhcp-option=host-name=Victor-s-S22, cisco-av-pair=dhcp-option=dhcp-class-identifier=andro
cisco-av-pair=dot11-device-info=DEVICE_INFO_MODEL_NUM=Samsung Galaxy S22+, cisco-av-pair=dot11-device-in

cisco-av-pair=dot11-device-info=DEVICE_INFO_DEVICE_FORM=1, cisco-av-pair=dot11-device-info=DEVICE_INFO_C

cisco-av-pair=dot11-device-info=DEVICE_INFO_VENDOR_TYPE=2, cisco-av-pair=audit-session-id=A90510AC000000
, cisco-av-pair=vlan-id=2606, cisco-av-pair=method=dot1x, cisco-av-pair=cisco-wlan-ssid=VICSSID,
cisco-av-pair=wlan-profile-name=ISE-AAA, Airespace-Wlan-Id=1, AcsSessionID=iselab/484624451/304,

Die Endpunktattributinformationen werden aktualisiert.

<#root>

2023-09-27 18:19:23,602

DEBUG [RADIUSParser-1-thread-2][[]]

cisco.profiler.probes.radius.RadiusParser -:A90510AC0000005BD7DDDA7::::-

Device Analytics data 1: DEVICE_INFO_FIRMWARE_VERSION=[WH6]

2023-09-27 18:19:23,602

DEBUG [RADIUSParser-1-thread-2][[]]

cisco.profiler.probes.radius.RadiusParser -:A90510AC0000005BD7DDDA7::::-

Device Analytics data 1: DEVICE_INFO_SALES_CODE=[MXO]

2023-09-27 18:19:23,602

DEBUG [RADIUSParser-1-thread-2][[]]

cisco.profiler.probes.radius.RadiusParser -:A90510AC0000005BD7DDDA7::::-

Device Analytics data 1: DEVICE_INFO_DEVICE_FORM=[1]

2023-09-27 18:19:23,602

DEBUG [RADIUSParser-1-thread-2][[]]

cisco.profiler.probes.radius.RadiusParser -:A90510AC0000005BD7DDDA7::::-

Device Analytics data 1: DEVICE_INFO_OS_VERSION=[Android 13]

2023-09-27 18:19:23,602

DEBUG [RADIUSParser-1-thread-2][[]]

cisco.profiler.probes.radius.RadiusParser -:A90510AC0000005BD7DDDA7::::-

Device Analytics data 1: DEVICE_INFO_COUNTRY_CODE=[Unknown]

2023-09-27 18:19:23,602

DEBUG [RADIUSParser-1-thread-2][[]]

cisco.profiler.probes.radius.RadiusParser -:A90510AC0000005BD7DDDA7::::-

Device Analytics data 1: DEVICE_INFO_VENDOR_TYPE=[2]

<#root>

2023-09-27 18:19:23,602

DEBUG [RADIUSParser-1-thread-2][[]]

cisco.profiler.probes.radius.RadiusParser -:A90510AC0000005BD7DDDA7:::- Endpoint: EndPoint[id=,name=

MAC: 0A:5A:F0:B3:B5:9C

Attribute:AAA-Server value:iselab Attribute:Acct-Authentic value:Remote Attribute:Acct-Delay-Time valu

Attribute:DEVICE_INFO_COUNTRY_CODE value:Unknown Attribute:DEVICE_INFO_DEVICE_FORM value:PHONE Attribute

Attribute:Device IP Address value:172.16.5.169 Attribute:Device Type value:Device Type#All Device Type

Die Attributaktualisierung löst ein neues Endpunktprofilierungsereignis aus. Profilrichtlinien werden erneut ausgewertet, und ein neues Profil wird zugewiesen.

<#root>

2023-09-27 18:19:24,098

DEBUG [pool-533-thread-35]

[[]] cisco.profiler.infrastructure.profiling.ProfilerManager -:A90510AC0000005BD7DDDA7:::62cc7a10-5d62-

Policy Android matched 0A:5A:F0:B3:B5:9C (certainty 30)

2023-09-27 18:19:24,098

DEBUG [pool-533-thread-35]

[[]] cisco.profiler.infrastructure.profiling.ProfilerManager -:A90510AC0000005BD7DDDA7:::62cc7a10-5d62-

DEBUG [pool-533-thread-35]

[[]] cisco.profiler.infrastructure.profiling.ProfilerManager -:A90510AC0000005BD7DDDA7:::62cc7a10-5d62-

Policy Android matched 0A:5A:F0:B3:B5:9C (certainty 30)

com.cisco.profiler.infrastructure.profiling.ProfilerManager\$MatchingPolicyInternal@14ec7800

Schritt 4: CoA und Neuauthentifizierung

Die ISE muss eine CoA für die Endpunktsitzung senden, da die Attribute der WiFi-Geräteanalyse geändert wurden.

<#root>

2023-09-27 18:19:24,103

DEBUG [pool-533-thread-35]

```
[[]] cisco.profiler.infrastructure.profilng.ProfilerManager -:A90510AC000005BD7DDDA7::62cc7a10-5d62-
Endpoint 0A:5A:F0:B3:B5:9C IdentityGroup / Logical Profile Changed/ WiFi device analytics attribute char
2023-09-27 18:19:24,103
```

```
DEBUG [pool-533-thread-35]
```

```
[[]] cisco.profiler.infrastructure.profilng.ProfilerManager -:A90510AC000005BD7DDDA7::62cc7a10-5d62-
ConditionalCoAEvent with Endpoint Details : EndPoint[id=62caa550-5d62-11ee-bf1f-b6bb1580ab0d,name=] MAC:
Attribute:AAA-Server value:iselab Attribute:Airespace-Wlan-Id value:1 Attribute:AllowedProtocolsMatched
Attribute:DEVICE_INFO_COUNTRY_CODE value:Unknown Attribute:DEVICE_INFO_DEVICE_FORM value:PHONE Attribute:
Attribute:DTLSSupport value:Unknown Attribute:DestinationIPAddress value:172.16.5.112 Attribute:Destin
```

Die Paketerfassung trägt dazu bei, dass die ISE die CoA an den WLC sendet. Außerdem wird angezeigt, dass ein neues Access-Request-Paket nach der Verarbeitung der CoA empfangen wird.

| | | | | | |
|-----|----------------------------|--------------|--------------|--------|-----------------------|
| 111 | 2023-09-27 12:19:24.357572 | 172.16.5.112 | 172.16.5.169 | RADIUS | 244 CoA-Request id=13 |
| 112 | 2023-09-27 12:19:24.361138 | 172.16.5.169 | 172.16.5.112 | RADIUS | 111 CoA-ACK id=13 |

```
> Frame 111: 244 bytes on wire (1952 bits), 244 bytes captured (1952 bits)
> Ethernet II, Src: VMware_b3:f0:73 (00:50:56:b3:f0:73), Dst: Cisco_5c:16:ff (00:1e:f6:5c:16:ff)
> Internet Protocol Version 4, Src: 172.16.5.112, Dst: 172.16.5.169
> User Datagram Protocol, Src Port: 41440, Dst Port: 1700
v RADIUS Protocol
  Code: CoA-Request (43)
  Packet identifier: 0xd (13)
  Length: 202
  Authenticator: d622a25b73d3b2b475cf5d4ad2b00b5c
  [The response to this request is in frame 112]
v Attribute Value Pairs
  > AVP: t=NAS-IP-Address(4) l=6 val=172.16.5.169
  > AVP: t=Calling-Station-Id(31) l=19 val=0A:5A:F0:B3:B5:9C
    Type: 31
    Length: 19
    Calling-Station-Id: 0A:5A:F0:B3:B5:9C
  > AVP: t=Event-Timestamp(55) l=6 val=Sep 27, 2023 12:19:24.000000000 CST
  > AVP: t=Message-Authenticator(80) l=18 val=3edaf9ffdb25ceee5451e90a1cef21af
v AVP: t=Vendor-Specific(26) l=43 vnd=ciscoSystems(9)
  Type: 26
  Length: 43
  Vendor ID: ciscoSystems (9)
  > VSA: t=Cisco-AVPair(1) l=37 val=subscriber:reauthenticate-type=last
v AVP: t=Vendor-Specific(26) l=41 vnd=ciscoSystems(9)
  Type: 26
  Length: 41
  Vendor ID: ciscoSystems (9)
  > VSA: t=Cisco-AVPair(1) l=35 val=subscriber:command=reauthenticate
v AVP: t=Vendor-Specific(26) l=49 vnd=ciscoSystems(9)
  Type: 26
  Length: 49
  Vendor ID: ciscoSystems (9)
  > VSA: t=Cisco-AVPair(1) l=43 val=audit-session-id=A90510AC000005BD7DDDA7
```

Radius-CoA-Paket nach Endpunktprofilierung

| | | | | | | | |
|-----|------------|-----------------|--------------|--------------|--------|------|-------------------------|
| 111 | 2023-09-27 | 12:19:24.357572 | 172.16.5.112 | 172.16.5.169 | RADIUS | 244 | CoA-Request id=13 |
| 112 | 2023-09-27 | 12:19:24.361138 | 172.16.5.169 | 172.16.5.112 | RADIUS | 111 | CoA-ACK id=13 |
| 113 | 2023-09-27 | 12:19:24.373874 | 172.16.5.169 | 172.16.5.112 | RADIUS | 480 | Access-Request id=55 |
| 114 | 2023-09-27 | 12:19:24.386280 | 172.16.5.112 | 172.16.5.169 | RADIUS | 167 | Access-Challenge id=55 |
| 115 | 2023-09-27 | 12:19:24.397609 | 172.16.5.169 | 172.16.5.112 | RADIUS | 557 | Access-Request id=63 |
| 116 | 2023-09-27 | 12:19:24.400463 | 172.16.5.112 | 172.16.5.169 | RADIUS | 167 | Access-Challenge id=63 |
| 117 | 2023-09-27 | 12:19:24.413943 | 172.16.5.169 | 172.16.5.112 | RADIUS | 720 | Access-Request id=71 |
| 118 | 2023-09-27 | 12:19:24.456036 | 172.16.5.112 | 172.16.5.169 | RADIUS | 1179 | Access-Challenge id=71 |
| 119 | 2023-09-27 | 12:19:24.477140 | 172.16.5.169 | 172.16.5.112 | RADIUS | 557 | Access-Request id=79 |
| 120 | 2023-09-27 | 12:19:24.481172 | 172.16.5.112 | 172.16.5.169 | RADIUS | 1175 | Access-Challenge id=79 |
| 121 | 2023-09-27 | 12:19:24.496743 | 172.16.5.169 | 172.16.5.112 | RADIUS | 557 | Access-Request id=87 |
| 122 | 2023-09-27 | 12:19:24.499901 | 172.16.5.112 | 172.16.5.169 | RADIUS | 289 | Access-Challenge id=87 |
| 123 | 2023-09-27 | 12:19:24.546538 | 172.16.5.169 | 172.16.5.112 | RADIUS | 715 | Access-Request id=95 |
| 124 | 2023-09-27 | 12:19:24.553619 | 172.16.5.112 | 172.16.5.169 | RADIUS | 218 | Access-Challenge id=95 |
| 125 | 2023-09-27 | 12:19:24.568069 | 172.16.5.169 | 172.16.5.112 | RADIUS | 557 | Access-Request id=103 |
| 126 | 2023-09-27 | 12:19:24.571945 | 172.16.5.112 | 172.16.5.169 | RADIUS | 201 | Access-Challenge id=103 |
| 127 | 2023-09-27 | 12:19:24.584229 | 172.16.5.169 | 172.16.5.112 | RADIUS | 594 | Access-Request id=111 |
| 128 | 2023-09-27 | 12:19:24.588165 | 172.16.5.112 | 172.16.5.169 | RADIUS | 232 | Access-Challenge id=111 |
| 129 | 2023-09-27 | 12:19:24.599493 | 172.16.5.169 | 172.16.5.112 | RADIUS | 648 | Access-Request id=119 |
| 130 | 2023-09-27 | 12:19:24.624360 | 172.16.5.112 | 172.16.5.169 | RADIUS | 247 | Access-Challenge id=119 |
| 131 | 2023-09-27 | 12:19:24.638515 | 172.16.5.169 | 172.16.5.112 | RADIUS | 592 | Access-Request id=127 |
| 132 | 2023-09-27 | 12:19:24.642039 | 172.16.5.112 | 172.16.5.169 | RADIUS | 200 | Access-Challenge id=127 |
| 133 | 2023-09-27 | 12:19:24.654578 | 172.16.5.169 | 172.16.5.112 | RADIUS | 557 | Access-Request id=135 |
| 134 | 2023-09-27 | 12:19:24.677792 | 172.16.5.112 | 172.16.5.169 | RADIUS | 330 | Access-Accept id=135 |

Radius-CoA und neue Zugriffsanforderung nach Endpunktprofilierung

Zugehörige Informationen

- [Administratorleitfaden für die Cisco Identity Services Engine, Version 3.3](#)
- [Versionshinweise für Cisco Identity Services Engine, Version 3.3](#)
- [Collect Support-Paket auf der Identity Services Engine](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.