

HPE Aruba Networking

Inhalt

Einführung.....	3
Sicheres Onboarding – IEEE 802.1AR/802.1X.....	4
Erstauthentifizierung.....	4
Bereitstellung.....	4
Produktionsnetzwerk.....	5
Konfiguration von HPE Aruba Networking.....	6
HPE Aruba Networking ClearPass Policy Manager.....	6
HPE Aruba Networking Zugangsschalter.....	15
Konfiguration Axis.....	16
Axis Netzwerkgerät.....	16
AXIS Device Manager.....	17
Sicherer Netzwerkbetrieb – IEEE 802.1AE MACsec.....	18
HPE Aruba Networking ClearPass Policy Manager.....	19
Rollen- und Rollenzuordnungsrichtlinie.....	19
Servicekonfiguration.....	20
Durchsetzungsprofil.....	21
HPE Aruba Networking Zugangsschalter.....	22
Zertifikatsverwaltung – Enrollment over Secure Transport (EST).....	23
Wichtigste Vorteile von EST.....	23
Konfiguration von HPE Aruba ClearPass Onboard.....	23
Konfiguration von HPE Aruba ClearPass Policy Manager.....	25
Konfiguration Axis.....	28
Legacy-Onboarding – MAC-Authentifizierung.....	33
HPE Aruba Networking ClearPass Policy Manager.....	33
Durchsetzungsrichtlinie.....	33
Quellenkonfiguration.....	34
Servicekonfiguration.....	35
HPE Aruba Networking Zugangsschalter.....	38

Einführung

Diese Integrationsanleitung beschreibt die empfohlene Konfiguration beim Onboarding und Betrieb von Axis Geräten in HPE Aruba Networking-Netzwerken. Bewährt haben sich Konfigurationen mit modernen Sicherheitsstandards und Protokollen wie IEEE 802.1X, IEEE 802.1AR, IEEE 802.1AE und HTTPS.

Die Einrichtung einer geeigneten Automatisierung für die Netzwerkintegration kann Ihnen Zeit und Geld sparen. Es ermöglicht die Beseitigung unnötiger Systemkomplexität bei der Verwendung von Anwendungen zur Verwaltung von Axis Geräten mit der Infrastruktur und den Anwendungen von HPE Aruba Networking. Die Kombination Ihrer Axis Geräte und Software mit einer HPE Aruba Networking-Netzwerkinfrastruktur bietet Ihnen die folgenden Vorteile:

- Durch den Wegfall von Netzwerken zur Gerätebereitstellung wird die Komplexität von Systemen minimiert.
- Die Automatisierung von Onboarding-Prozessen und Geräteverwaltung trägt zur Kostensenkung bei.
- Ihre Axis Geräte bieten Zero-Touch-Netzwerksicherheitskontrollen.
- Das kombinierte Know-how von HPE und Axis steigert die Gesamtnetzwerksicherheit.



Für einen reibungslosen softwaredefinierten Wechsel zwischen logischen Netzwerken während des gesamten Onboarding-Prozesses muss die Netzwerkinfrastruktur vor Beginn der Konfiguration zur sicheren Überprüfung der Integrität von Axis Geräten vorbereitet werden. Dazu müssen die folgenden Voraussetzungen vor der Konfiguration erfüllt sein:

- Erfahrung mit der Verwaltung der IT-Infrastruktur von Unternehmensnetzwerken mit HPE Aruba Networking, einschließlich HPE Aruba Networking-Zugangsschalter und HPE Aruba Networking ClearPass Policy Manager.
- Fachkenntnisse in modernen Netzwerkzugriffskontrolltechniken und Netzwerk-Sicherheitsrichtlinien.
- Grundlegende Vorkenntnisse über Axis Produkte sind wünschenswert, werden aber auch im Handbuch vermittelt.

Sicheres Onboarding – IEEE 802.1AR/802.1X



Rufen Sie zur Wiedergabe dieses Videos die Webversion dieses Dokuments auf.

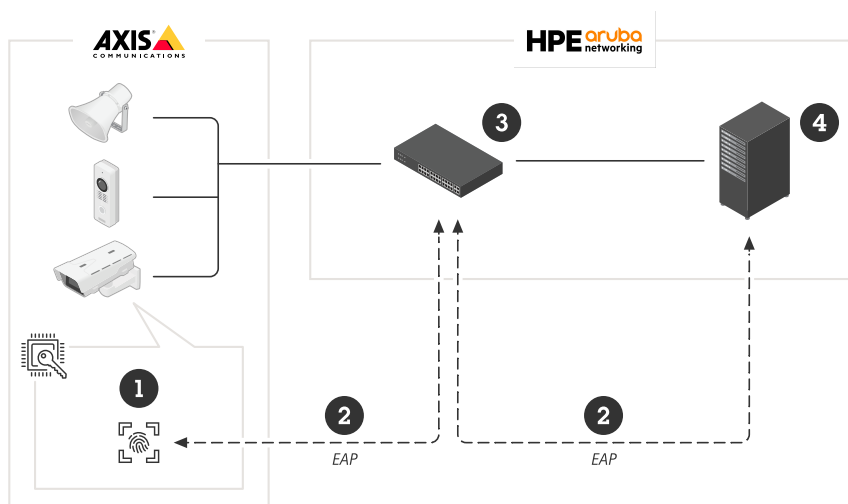
Sicheres Onboarding von Geräten in vertrauenswürdigen Netzwerken mit IEEE 802.1X/802.1AR

Erstauthentifizierung

Wenn das von Axis Edge Vault unterstützte Axis Gerät mit dem Netzwerk verbunden ist, verwendet es das IEEE 802.1AR Axis Geräte-ID-Zertifikat über die IEEE 802.1X-Netzwerkzugriffskontrolle, um sich zu authentifizieren.

Zur Gewährung des Netzwerkzugriffs überprüft der ClearPass Policy Manager die Axis Geräte-ID zusammen mit anderen gerätespezifischen Fingerabdrücken. Diese Informationen, wie beispielsweise die MAC-Adresse und die AXIS OS-Version des Geräts, werden für eine richtlinienbasierte Entscheidung herangezogen.

Das Axis Gerät authentifiziert sich im Netzwerk mithilfe des IEEE 802.1AR-konformen Axis Geräte-ID-Zertifikats.

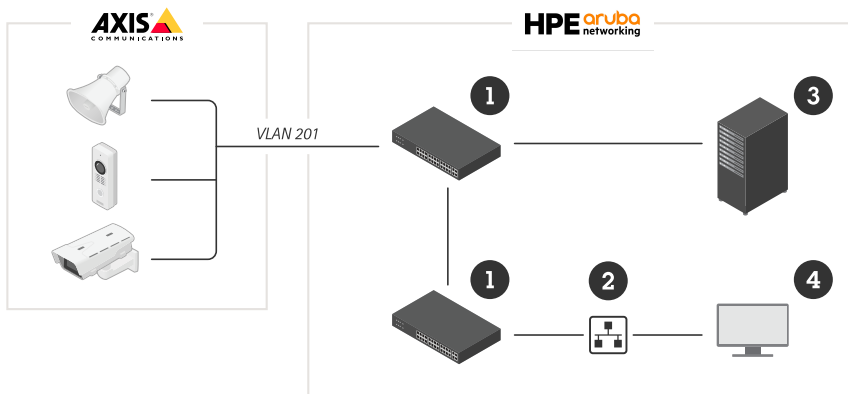


Das Axis Gerät authentifiziert sich im HPE Aruba Networking-Netzwerk mithilfe des IEEE 802.1AR-konformen Axis Geräte-ID-Zertifikats.

- 1 Axis Geräte-ID
- 2 IEEE 802,1x EAP-TLS-Netzwerkauthentifizierung
- 3 Zugangsschalter (Authentifikator)
- 4 ClearPass Policy Manager

Bereitstellung

Nach der Authentifizierung wird das Axis Gerät in das Bereitstellungsnetzwerk (VLAN201) verschoben. Dieses Netzwerk umfasst den AXIS Device Manager, der für die Gerätekonfiguration, die Verstärkung der Sicherheit und die Ausführung von AXIS OS-Updates zuständig ist. Um die Gerätebereitstellung abzuschließen, werden neue kundenspezifische Zertifikate in Produktionsqualität für IEEE 802.1X und HTTPS auf das Gerät hochgeladen.

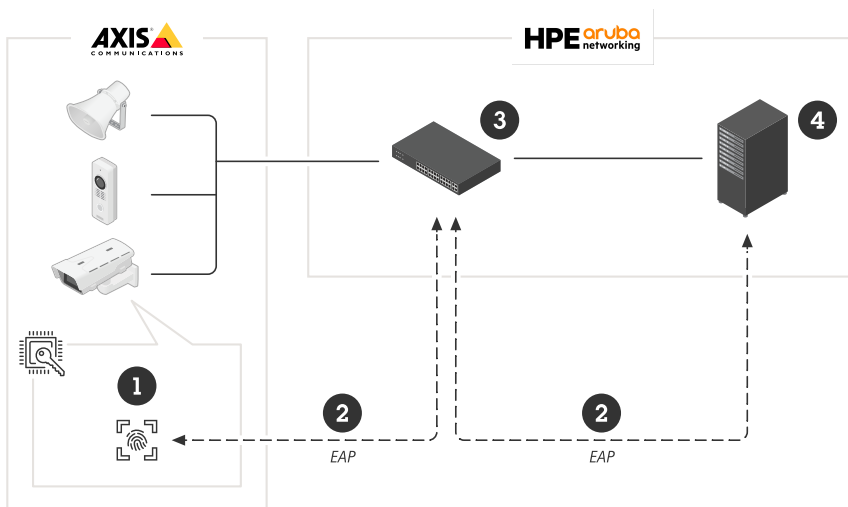


Nach erfolgreicher Authentifizierung wird das Axis Gerät zur Konfiguration in ein Bereitstellungsnetzwerk verschoben.

- 1 Zugangsschalter
- 2 Bereitstellung des Netzwerks
- 3 ClearPass Policy Manager
- 4 Anwendung zur Geräteverwaltung

Produktionsnetzwerk

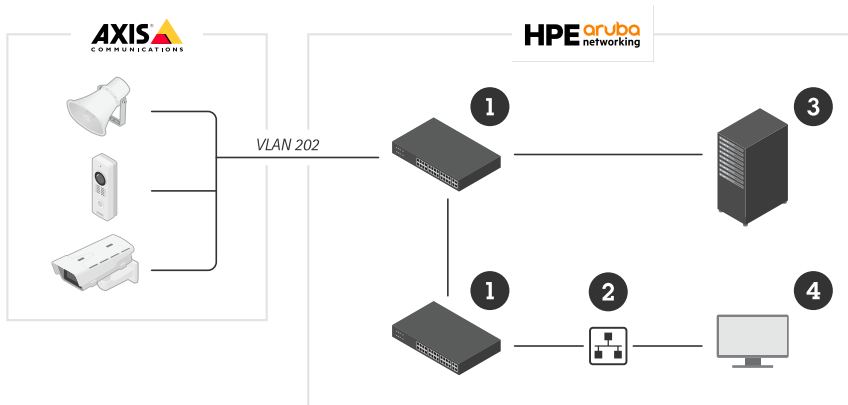
Die Bereitstellung des Axis Geräts mit neuen IEEE 802.1X-Zertifikaten löst einen neuen Authentifizierungsversuch aus. Der ClearPass Policy Manager überprüft die neuen Zertifikate und entscheidet, ob das Axis Gerät in das Produktionsnetzwerk verschoben wird oder nicht.



Nach der Konfiguration verlässt das Axis Gerät das Bereitstellungsnetzwerk und versucht, sich erneut im Netzwerk zu authentifizieren.

- 1 Axis Geräte-ID
- 2 IEEE 802,1x EAP-TLS-Netzwerkauthentifizierung
- 3 Zugangsschalter (Authentifikator)
- 4 ClearPass Policy Manager

Nach der erneuten Authentifizierung wird das Axis Gerät in das Produktionsnetzwerk (VLAN 202) verschoben, wo sich das Video Management System (VMS) mit dem Gerät verbindet und den Betrieb übernimmt.



Dem Axis Gerät wird Zugriff auf das Produktionsnetzwerk gewährt.

- 1 Zugangsschalter
- 2 Produktionsnetzwerk
- 3 ClearPass Policy Manager
- 4 Videoverwaltungssystem

Konfiguration von HPE Aruba Networking

HPE Aruba Networking ClearPass Policy Manager

Der ClearPass Policy Manager bietet die rollen- und gerätebasierte sichere Netzwerkzugriffssteuerung für IoT, BYOD, Unternehmensgeräte, Beschäftigte, Auftragnehmer und Gäste in der kabelgebundenen, kabellosen und VPN-Infrastruktur mehrerer Anbieter.

Konfiguration des vertrauenswürdigen Zertifikatspeichers

1. Laden Sie die Axis spezifische IEEE 802.1AR-Zertifikatskette von axis.com herunter.
2. Laden Sie die Axis spezifischen IEEE 802.1AR-Root-CA- und Intermediate-CA-Zertifikatketten in den vertrauenswürdigen Zertifikatspeicher hoch.
3. Aktivieren Sie ClearPass Policy Manager zur Authentifizierung von Axis Geräten über IEEE 802.1X EAP-TLS.
4. Wählen Sie im Verwendungsfeld EAP aus. Die Zertifikate werden für die IEEE 802.1X EAP-TLS-Authentifizierung verwendet.

The screenshot shows the ClearPass Policy Manager web interface. The 'Certificate Trust List' is displayed, showing a list of trusted Certificate Authorities (CA). A modal window is open for adding a new certificate, showing the file path 'Axis_device_ID_Int...e_CA_ECC_1.pem' and the usage 'EAP'. The modal window has buttons for 'Add Certificate' and 'Cancel'.

#	Subject	Usage	Validity	Enabled
1.	OU=VeriSign Trust Network,OU=(c) 1998 VeriSign, Inc. - For authorized use only,OU=Class 3 Public Primary Certification Authority - G2,O=VeriSign, Inc.,C=US	Others	Valid	Disabled
2.	OU=Go	AD/LDAP Servers, Endpoint Context Servers, SAML, SMTP, Others	Valid	Enabled
3.	OU=Class	Others	Valid	Disabled
4.	emailAd	EAP, Others	Valid	Enabled
5.	emailAd	EAP, Others	Valid	Enabled
6.	C=US,ST	Others	Valid	Disabled
7.	C=US,ST	Others	Valid	Disabled
8.	C=US,ST	Others	Valid	Disabled
9.	CN=Wired Phones,OU=PKI Authority,O=Akatec-Lucent,C=FR	Others	Valid	Disabled
10.	CN=VeriSign Class 3 Public Primary Certification Authority - G5,OU=(c) 2006 VeriSign, Inc. - For authorized use only,OU=VeriSign Trust Network,O=VeriSign, Inc.,C=US	Others	Valid	Disabled
11.	CN=VeriSign Class 3 Public Primary Certification Authority - G3,OU=(c) 1999 VeriSign, Inc. - For authorized use only,OU=VeriSign Trust Network,O=VeriSign, Inc.,C=US	Others	Valid	Disabled
12.	CN=VeriSign Class 1 Public Primary Certification Authority - G3,OU=(c) 1999 VeriSign, Inc. - For authorized use only,OU=VeriSign Trust Network,O=VeriSign, Inc.,C=US	AD/LDAP Servers, Endpoint Context Servers, SAML, SMTP, Others	Valid	Enabled
13.	CN=USERTrust RSA Certification Authority,O=The USERTRUST Network,L=Jersey City,ST=New Jersey,C=US	EAP, Others	Valid	Disabled
14.	CN=thawte Primary Root CA,OU=(c) 2006 thawte, Inc. - For authorized use only,OU=Certification Services Division,O=thawte, Inc.,C=US	Others	Valid	Disabled
15.	CN=TC TrustCenter Universal CA 1,OU=TC TrustCenter Universal CA,O=TC TrustCenter GmbH,C=DE	Others	Valid	Disabled

Hochladen der für Axis spezifischen IEEE 802.1AR-Zertifikate in den vertrauenswürdigen Zertifikatspeicher des ClearPass Policy Managers.

ClearPass Policy Manager - Administration » Certificates » Trust List

This page displays a list of trusted Certificate Authorities (CA). You can add, view, or delete a certificate.

Filter: Subject contains axis device Go Clear Filter Show 20 records

#	Subject	Usage	Validity	Enabled
1.	CN=Axis device ID Root CA RSA,O=Axis Communications AB	EAP	Valid	Enabled
2.	CN=Axis device ID Root CA ECC,O=Axis Communications AB	EAP	Valid	Enabled
3.	CN=Axis device ID Intermediate CA RSA 2,O=Axis Communications AB	EAP	Valid	Enabled
4.	CN=Axis device ID Intermediate CA RSA 1,O=Axis Communications AB	EAP	Valid	Enabled
5.	CN=Axis device ID Intermediate CA ECC 2,O=Axis Communications AB	EAP	Valid	Enabled
6.	CN=Axis device ID Intermediate CA ECC 1,O=Axis Communications AB	EAP	Valid	Enabled

Showing 1-6 of 6 Delete

© Copyright 2022 Hewlett Packard Enterprise Development LP Nov 25, 2022 08:48:50 CET ClearPass Policy Manager 6.9.12.136929 on CLABV (Trial Version) platform

Der vertrauenswürdige Zertifikatsspeicher im ClearPass Policy Manager mit für Axis spezifischer IEEE 802.1AR-Zertifikatskette.

Netzwerkgeräte-/Gruppenkonfiguration

1. Fügen Sie dem ClearPass Policy Manager vertrauenswürdige Netzwerkzugriffsgeräte wie HPE Aruba Netzwerk Access Switches hinzu. Der ClearPass Policy Manager muss wissen, welche Access Switches im Netzwerk für die IEEE 802.1X-Kommunikation verwendet werden. Zusätzlich muss das gemeinsame RADIUS-Geheimnis mit der spezifischen IEEE 802.1X-Konfiguration des Switches übereinstimmen.
2. Verwenden Sie die Netzwerkgerätegruppenkonfiguration, um mehrere vertrauenswürdige Netzwerkzugriffsgeräte zu gruppieren. Die Gruppierung von Geräten vereinfacht die Konfiguration von Richtlinien.

ClearPass Policy Manager - Configuration » Network » Devices

Network Devices

A Network Access Device (NAD) must belong to the global list of devices in the ClearPass database in order to connect to ClearPass.

Filter: Name contains Go Clear Filter Show 20 records

#	Name	IP or Subnet Address	Device Groups	Description
---	------	----------------------	---------------	-------------

Copy Export Delete

© Copyright 2022 Hewlett Packard Enterprise Development LP Dec 28, 2022 09:01:17 CET ClearPass Policy Manager 6.9.12.136929 on CLABV (Trial Version) platform

Die Schnittstelle für vertrauenswürdige Netzwerkgeräte im ClearPass Policy Manager.

ClearPass Policy Manager - Aruba

Configuration » Network » Devices

Network Devices

Add Device

Device | SNMP Read Settings | SNMP Write Settings | CLI Settings | OnConnect Enforcement | Attributes

Name: SW04

IP or Subnet Address: 172.25.200.13
(e.g., 192.168.1.10 or 192.168.1.1/24 or 2001:db8:a0b:12f0::1 or 2001:db8:a0b:12f0::1/64)

Description:

RADIUS Shared Secret: [masked] Verify: [masked]

TACACS+ Shared Secret: [masked] Verify: [masked]

Vendor Name: Aruba

Enable RADIUS Dynamic Authorization: ☐

Enable RadSec: ☐

Add Cancel

Copyright 2022 Hewlett Packard Enterprise Development LP Dec 28, 2022 09:02:18 CET ClearPass Policy Manager 6.9.12.136929 on CLABV (Trial Version) platform

Hinzufügen des HPE Aruba Networking-Zugangsschalters als vertrauenswürdiges Gerät im ClearPass Policy Manager. Bitte beachten Sie, dass das gemeinsame RADIUS-Geheimnis mit der spezifischen IEEE 802.1X-Konfiguration des Switches übereinstimmen muss.

ClearPass Policy Manager - Aruba

Configuration » Network » Devices

Network Devices

Device SW04 added

A Network Access Device (NAD) must belong to the global list of devices in the ClearPass database in order to connect to ClearPass.

Filter: Name contains [] Go Clear Filter

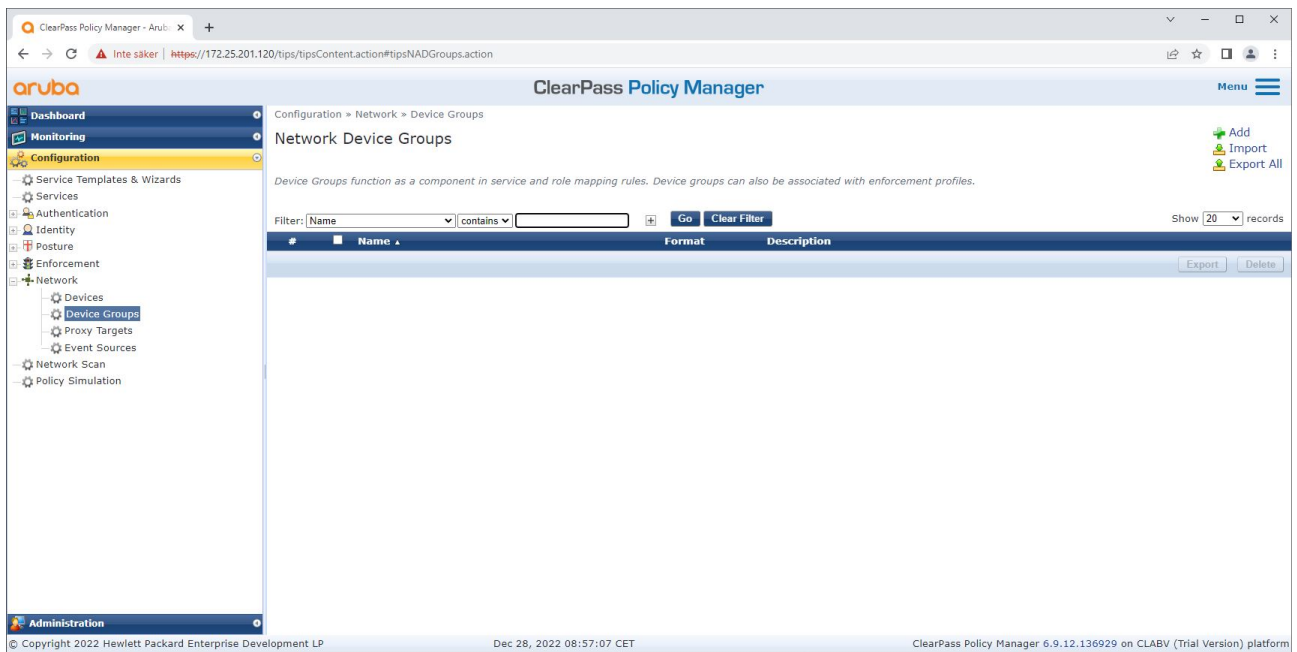
#	Name	IP or Subnet Address	Device Groups	Description
1.	SW04	172.25.200.13	-	

Showing 1-1 of 1

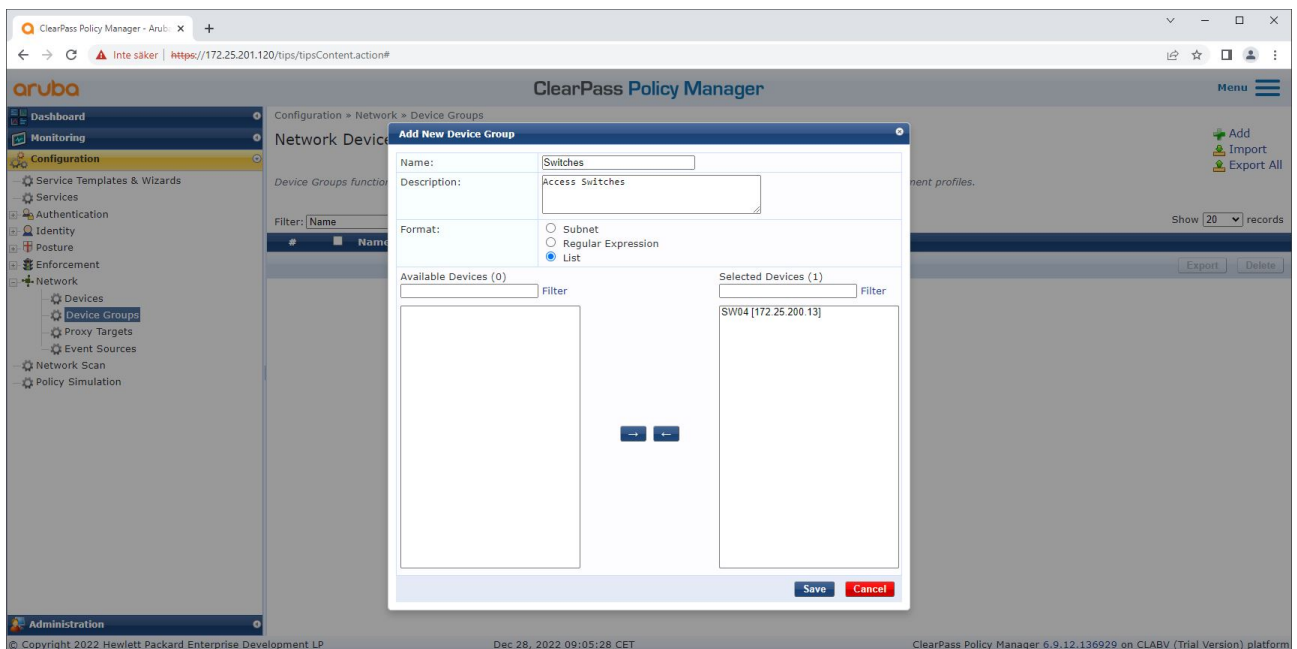
Copy Export Delete

Copyright 2022 Hewlett Packard Enterprise Development LP Dec 28, 2022 09:02:33 CET ClearPass Policy Manager 6.9.12.136929 on CLABV (Trial Version) platform

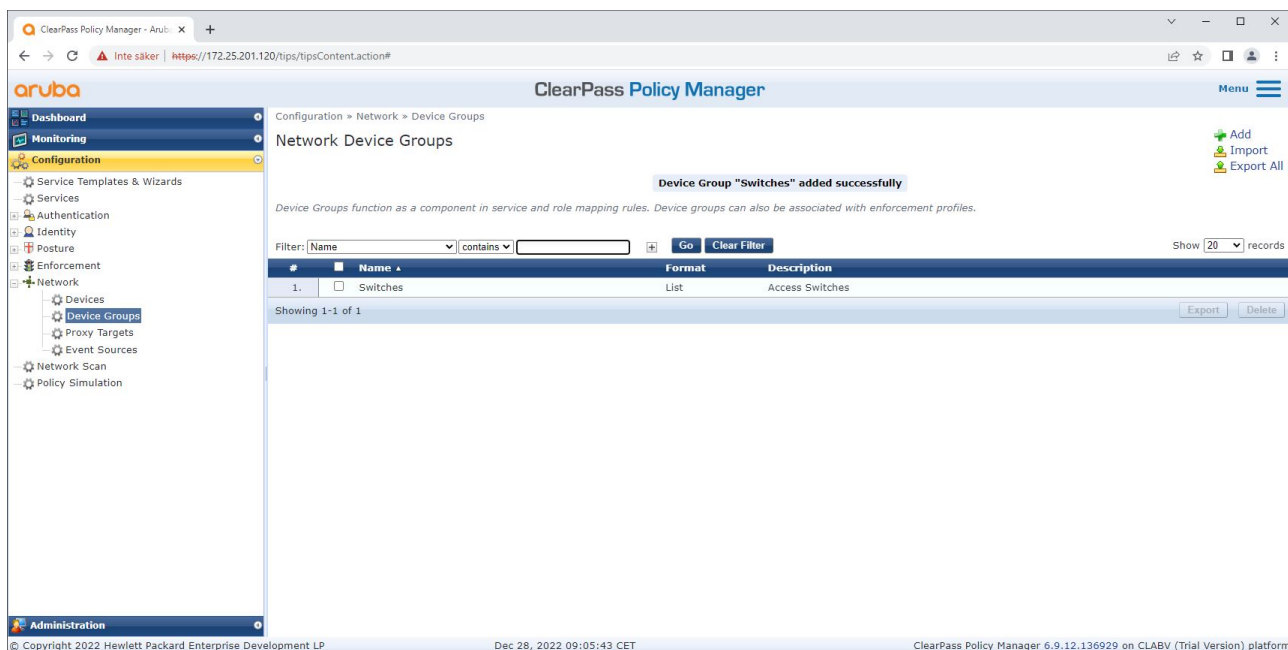
Der ClearPass Policy Manager mit einem konfigurierten vertrauenswürdigen Netzwerkgerät.



Die Schnittstelle für vertrauenswürdige Netzwerkgerätegruppen im ClearPass Policy Manager.



Hinzufügen eines vertrauenswürdigen Netzwerkzugriffsgeräts zu einer neuen Gerätegruppe im ClearPass Policy Manager.

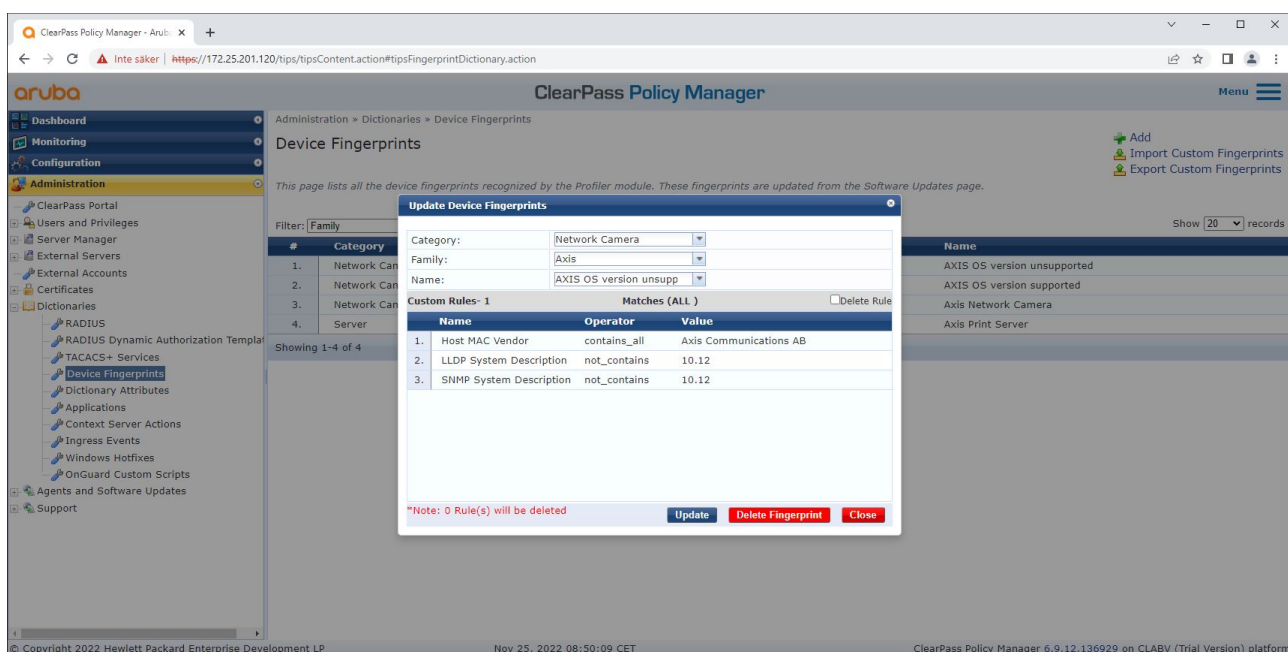


ClearPass Policy Manager mit konfigurierter Netzwerkgerätegruppe, die ein oder mehrere vertrauenswürdige Netzwerkgeräte umfasst.

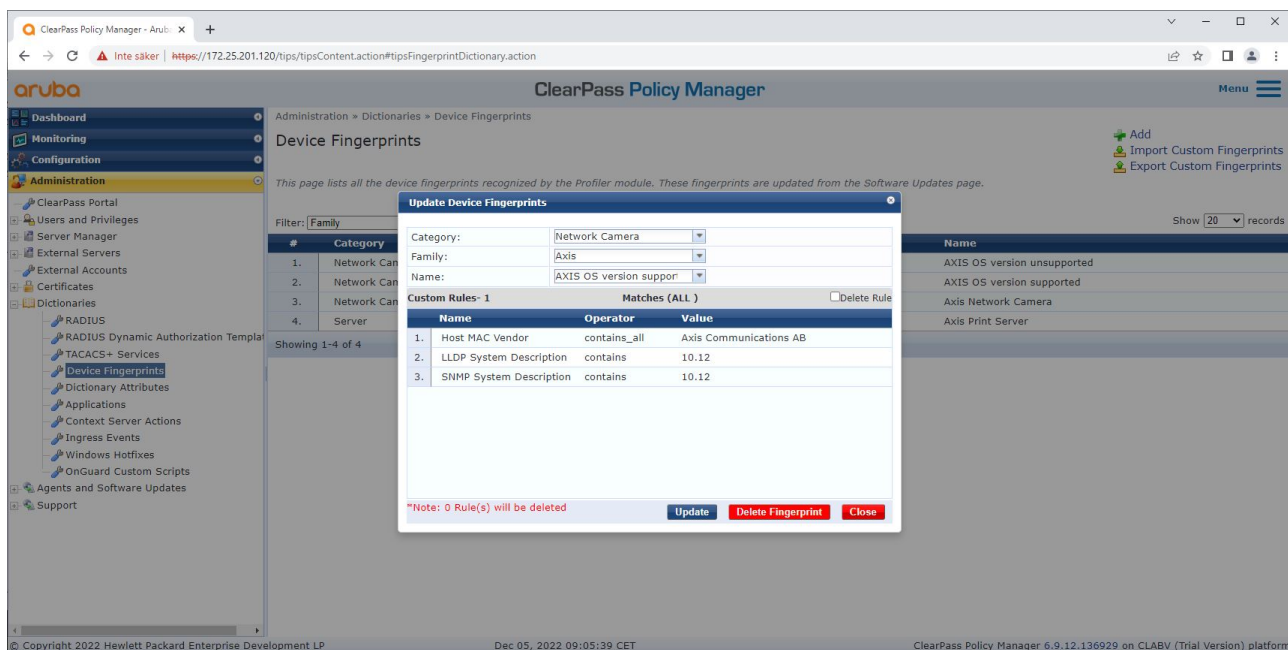
Konfiguration des Gerätefingerabdrucks

Das Axis Gerät kann über die Netzwerkerkennung gerätespezifische Informationen wie die MAC-Adresse und die Version der Gerätesoftware übertragen. Diese Informationen erlauben Ihnen die Erstellung, Aktualisierung und Verwaltung eines Gerätefingerabdrucks im ClearPass Policy Manager. Sie können den Zugriff auch auf Grundlage der AXIS OS-Version gewähren oder verweigern.

1. Gehen Sie zu Administration > Dictionaries > Device Fingerprints (Verwaltung > Wörterbücher > Gerätefingerabdrücke).
2. Wählen Sie einen vorhandenen Gerätefingerabdruck aus oder erstellen Sie einen neuen Gerätefingerabdruck.
3. Konfigurieren Sie den Gerätefingerabdruck.



Die Konfiguration des Gerätefingerabdrucks im ClearPass Policy Manager. Axis Geräte, die andere AXIS OS-Versionen als 10.12 verwenden, werden in diesem Beispiel nicht unterstützt.



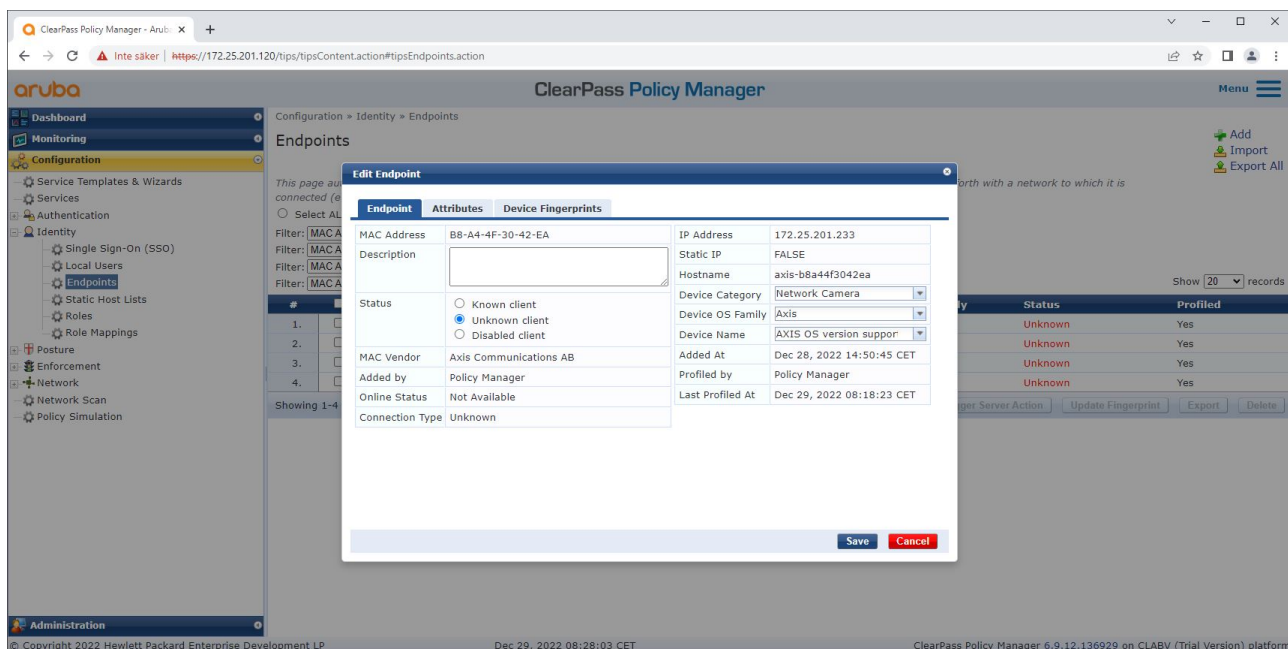
Die Konfiguration des Gerätefingerabdrucks im ClearPass Policy Manager. Axis Geräte, die andere AXIS OS-Versionen als 10.12 verwenden, werden in diesem Beispiel unterstützt.

Informationen zum Geräte-Fingerabdruck, der von ClearPass Policy Manager erfasst wurde, finden Sie im Abschnitt „Endpunkte“.

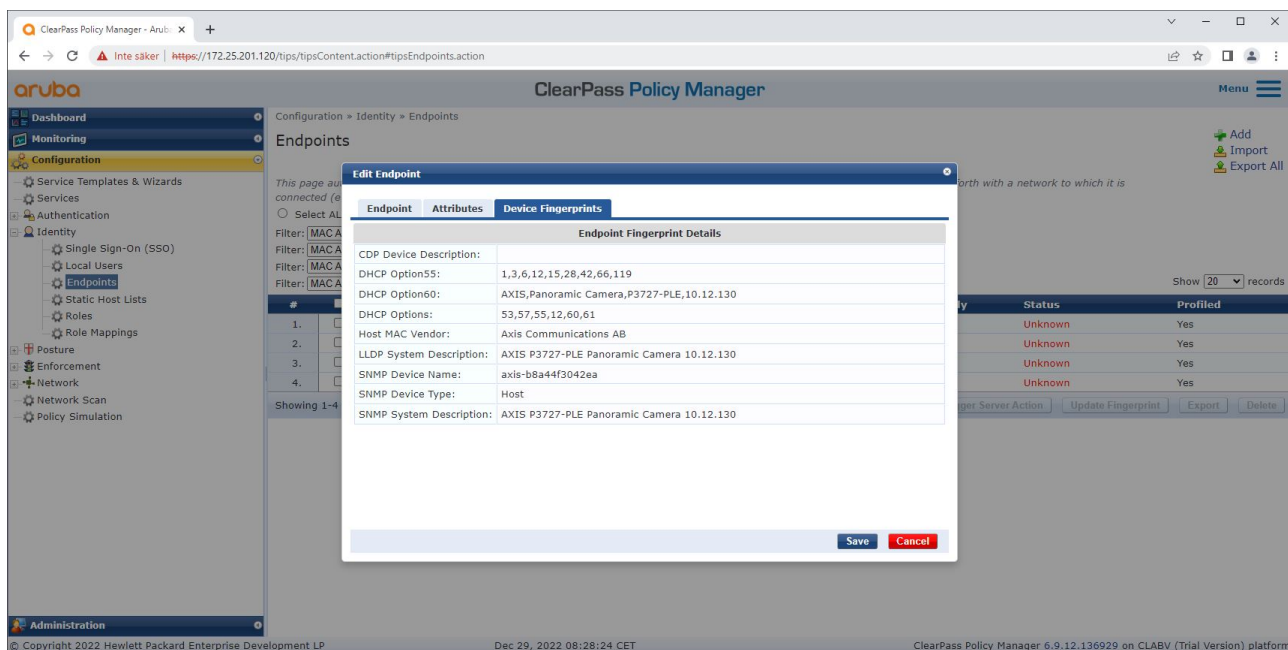
1. Gehen Sie zu **Configuration > Identity > Endpoints** (Konfiguration > Identität > Endpunkte).
2. Wählen Sie das Gerät, das Sie ansehen möchten.
3. Klicken Sie auf die Registerkarte **Device Fingerprints** (Gerätefingerabdrücke).

Hinweis

SNMP ist in Axis Geräten standardmäßig deaktiviert und wird vom HPE Aruba Netzwerk-Zugangsschalter erfasst.



Ein von ClearPass Policy Manager profiliertes Axis Gerät.

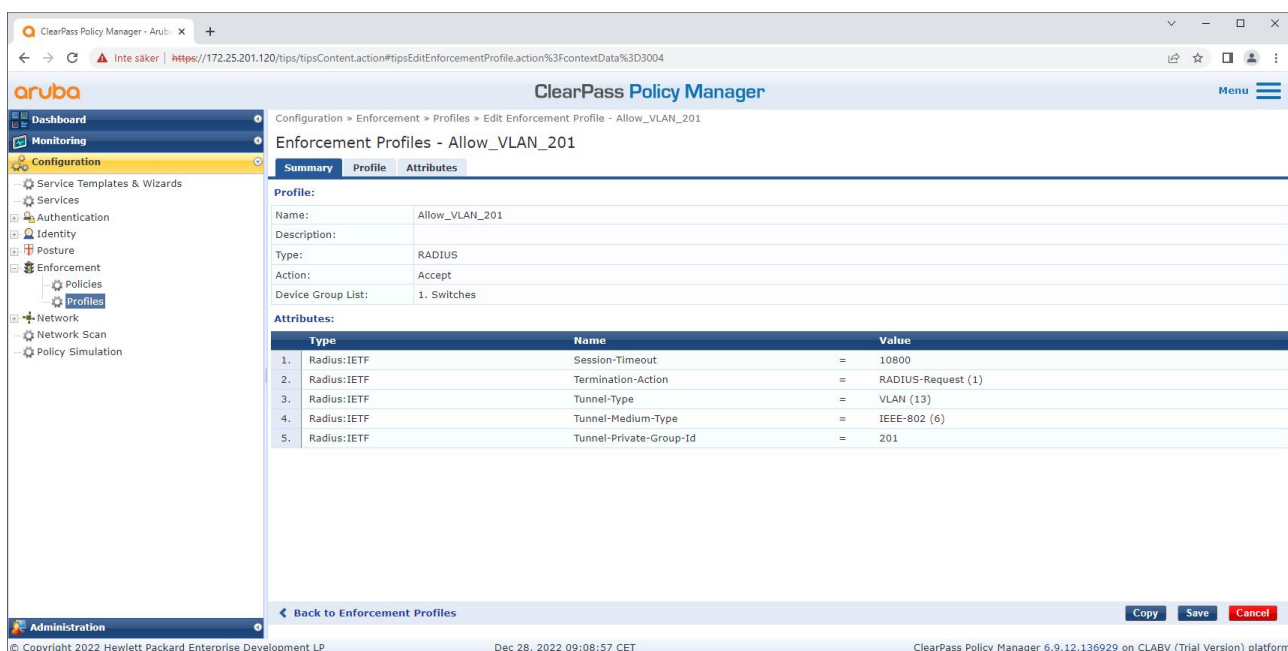


Die detaillierten Gerätefingerabdrücke eines profilierten Axis Geräts. Bitte beachten Sie, dass SNMP in Axis Geräten standardmäßig deaktiviert ist. LLDP-, CDP- und DHCP-spezifische Erkennungsinformationen werden vom Axis Gerät in der werksseitigen Standardeinstellung weitergegeben und vom HPE Aruba Networking-Zugangsschalter an den ClearPass Policy Manager weitergeleitet.

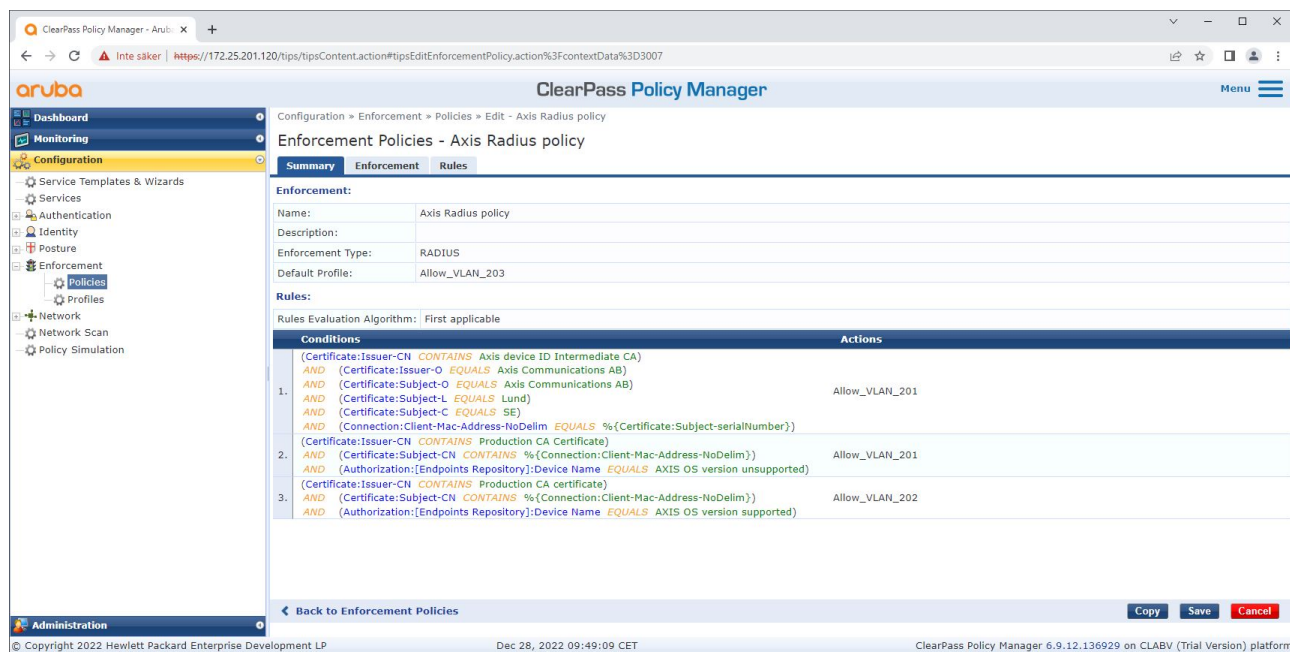
Konfiguration des Durchsetzungsprofils

Das Durchsetzungsprofil gestattet es dem ClearPass Policy Manager, einem Zugriffspunkt am Switch eine bestimmte VLAN-ID zuzuweisen. Hierbei handelt es sich um eine richtlinienbasierte Entscheidung, die für die Netzwerkgeräte in der Gerätegruppe „Switches“ (Schalter) gilt. Die erforderliche Anzahl von Durchsetzungsprofilen hängt von der Anzahl der verwendeten VLANs ab. Unsere Konfiguration umfasst drei VLANs (VLAN 201, 202, 203), was bedeutet, dass drei Durchsetzungsprofile zum Einsatz kommen.

Nachdem die Durchsetzungsprofile für das VLAN konfiguriert wurden, kann die eigentliche Durchsetzungsrichtlinie konfiguriert werden. Die Durchsetzungsrichtlinienkonfiguration im ClearPass Policy Manager definiert anhand von vier Beispielen für Richtlinienprofile, ob Axis Geräten Zugriff auf HPE Aruba Networking-Netzwerke gewährt wird.



Ein Beispiel für ein Durchsetzungsprofil, um den Zugriff auf VLAN 201 zu ermöglichen.



Die Konfiguration für die Durchsetzungsrichtlinie im ClearPass Policy Manager.

Die vier Durchsetzungsrichtlinien und ihre Maßnahmen sind:

Netzwerkzugriff verweigert

Der Zugriff auf das Netzwerk wird verweigert, wenn keine IEEE 802.1X-Authentifizierung zur Netzwerkzugriffskontrolle erfolgt.

Gastnetzwerk (VLAN 203)

Dem Axis Gerät wird Zugriff auf ein begrenztes, isoliertes Netzwerk gewährt, wenn die IEEE 802.1X-Authentifizierung der Netzwerkzugriffskontrolle fehlschlägt. Das macht die anschließende manuelle Überprüfung des Geräts erforderlich, um geeignete Aktionen zu ermitteln.

Bereitstellung des Netzwerks (VLAN 201)

Dem Axis Gerät wird Zugriff auf ein Bereitstellungsnetzwerk gewährt. So sollen Axis Geräteverwaltungsfunktionen durch *AXIS Device Manager* und *AXIS Device Manager Extend* bereitgestellt werden. Darüber hinaus ist es möglich, Axis Geräte mit AXIS OS-Updates, Produktionszertifikaten und anderen Konfigurationen zu konfigurieren. Die folgenden Bedingungen werden vom ClearPass Policy Manager überprüft:

- Die AXIS OS-Version des Geräts.
- Die MAC-Adresse des Geräts stimmt inklusive des Seriennummernattributs des Axis Geräte-ID-Zertifikats mit dem herstellerspezifischen MAC-Adressenschema überein.
- Das Axis Geräte-ID-Zertifikat ist überprüfbar und entspricht den für Axis spezifischen Attributen wie Aussteller, Organisation, Standort, Land.

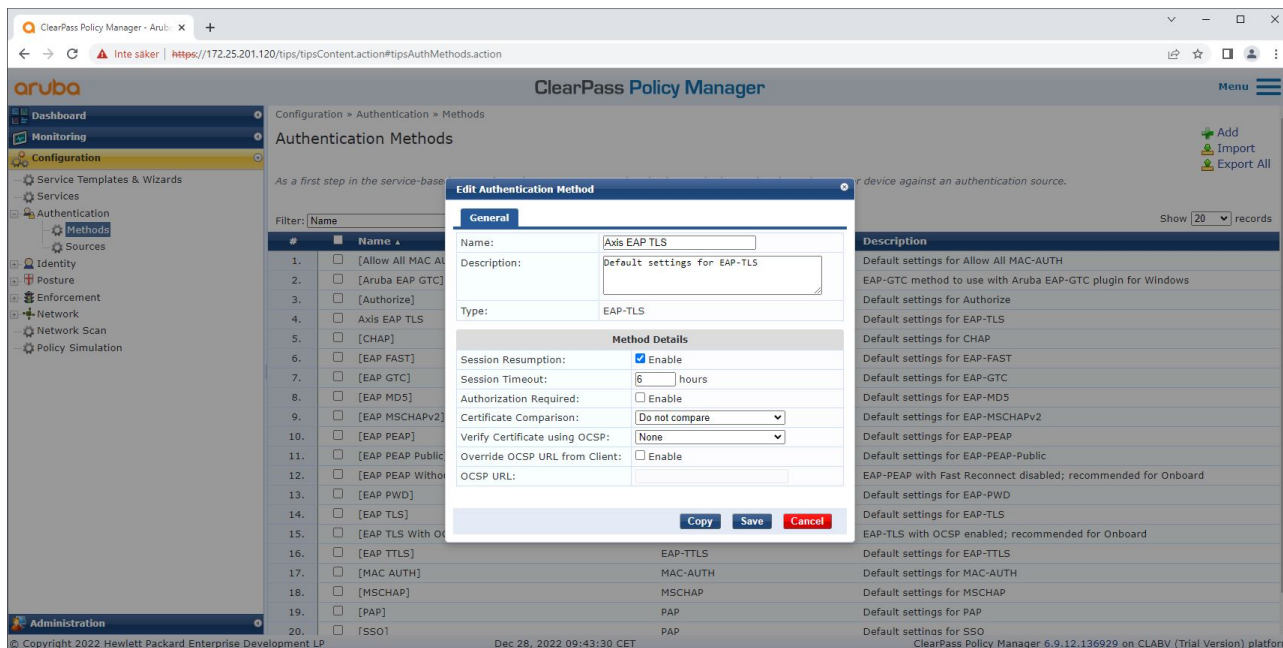
Produktionsnetzwerk (VLAN 202)

Dem Axis Gerät wird der Zugriff auf das Produktionsnetzwerk gewährt, in dem es betrieben werden soll. Der Zugriff wird gewährt, nachdem die Gerätebereitstellung im Bereitstellungsnetzwerk (VLAN 201) abgeschlossen wurde. Die folgenden Bedingungen werden vom ClearPass Policy Manager überprüft:

- Die AXIS OS-Version des Geräts.
- Die MAC-Adresse des Geräts stimmt inklusive des Seriennummernattributs des Axis Geräte-ID-Zertifikats mit dem herstellerspezifischen MAC-Adressenschema überein.
- Das Produktionszertifikat kann vom vertrauenswürdigen Zertifikatsspeicher überprüft werden.

Konfiguration der Authentifizierungsmethode

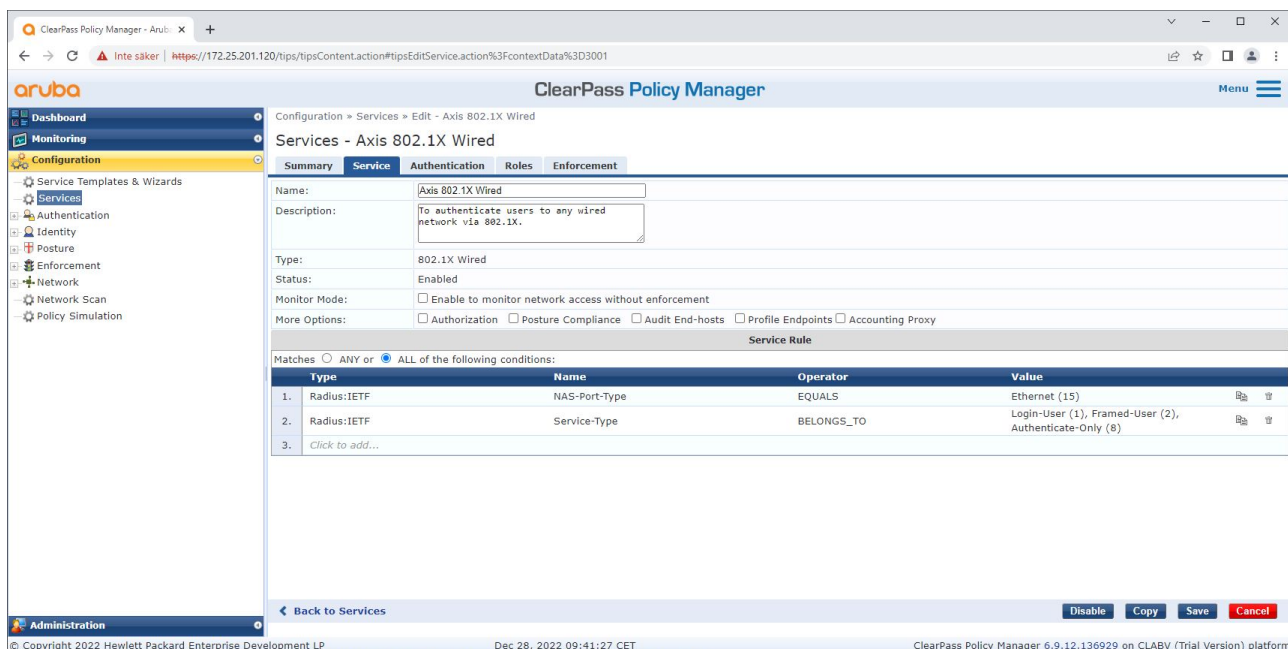
Die Authentifizierungsmethode gibt vor, wie ein Axis Gerät versucht, sich im Netzwerk zu authentifizieren. Die bevorzugte Methode ist IEEE 802.1X EAP-TLS, da bei Axis Geräten mit Axis Edge Vault standardmäßig IEEE 802.1X EAP-TLS aktiviert ist.



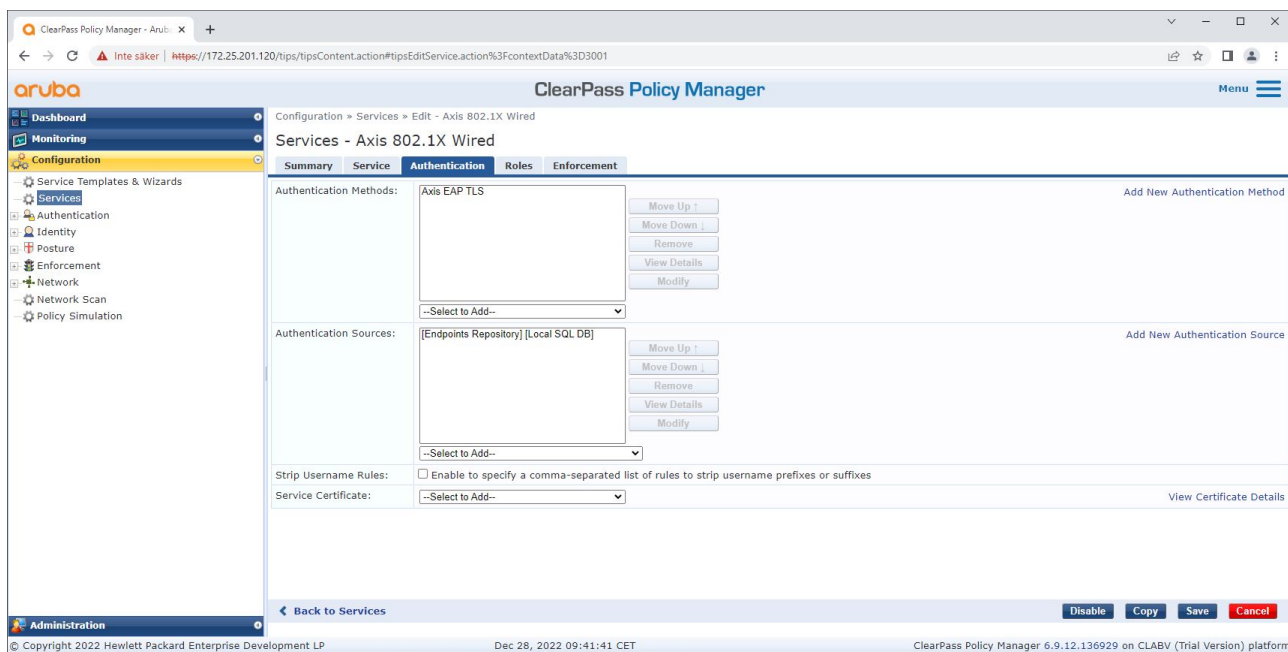
Benutzeroberfläche für Authentifizierungsmethoden im ClearPass Policy Manager, in der die EAP-TLS-Authentifizierungsmethode für Axis Geräte definiert wird.

Servicekonfiguration

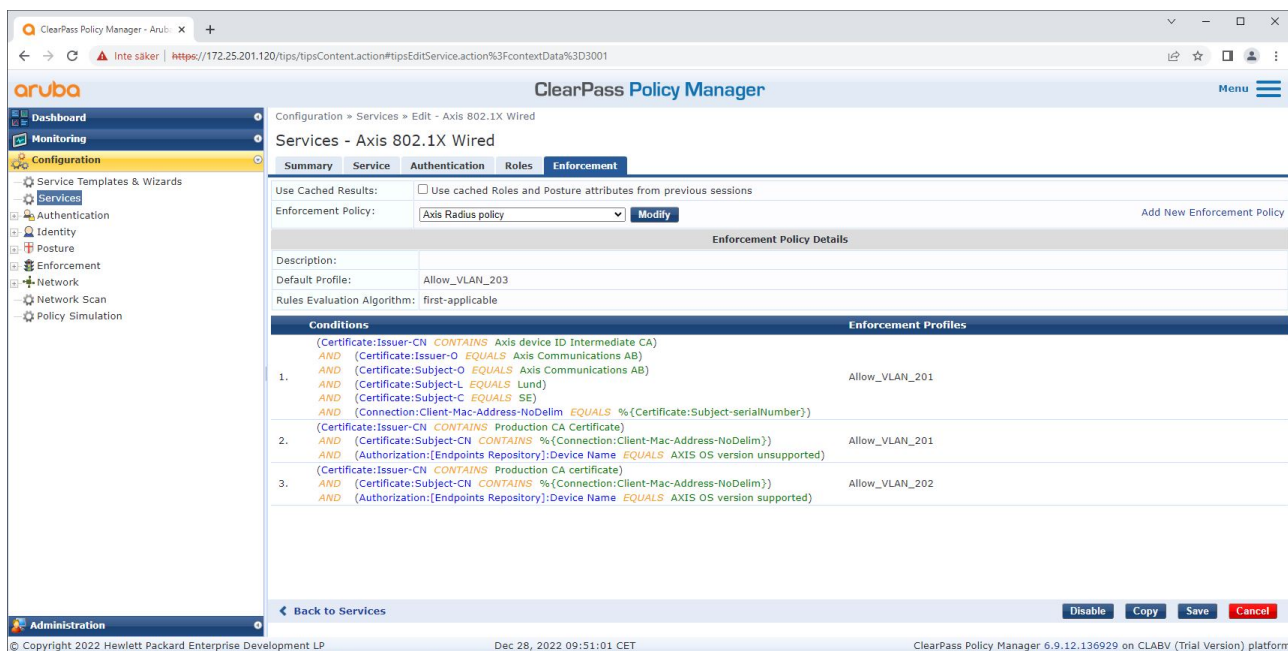
Auf der Seite Services werden die Konfigurationsschritte in einem Dienst zusammengefasst, der die Authentifizierung und Autorisierung von Axis Geräten in HPE Aruba Networking-Netzwerken übernimmt.



Ein dedizierter Axis Dienst mit IEEE 802.1X als Verbindungsmethode wird erstellt.



Die zuvor erstellte EAP-TLS-Authentifizierung wird für den Dienst konfiguriert.



Die zuvor erstellte Durchsetzungsrichtlinie wird für den Dienst konfiguriert.

HPE Aruba Networking Zugangsschalter

Axis Geräte werden entweder direkt mit PoE-fähigen Zugangsschaltern oder über kompatible Axis PoE-Midspans verbunden. Um Axis Geräte sicher in HPE Aruba Networking-Netzwerke einzubinden, muss der Zugriffsschalter für die IEEE 802.1X-Kommunikation konfiguriert werden. Das Axis Gerät leitet die IEEE 802.1x EAP-TLS-Kommunikation an den ClearPass Policy Manager weiter, der als RADIUS-Server fungiert.

Hinweis

Ein Intervall für die regelmäßige Neuauthentifizierung von 300 Sekunden ist für das Axis Gerät konfiguriert, um die allgemeine Portzugriffssicherheit zu erhöhen.

Dieses Beispiel zeigt die globale Konfiguration und die Portkonfiguration für HPE Aruba Networking-Zugangsschalter.

```
radius-server host MyRADIUSIPAddress key "MyRADIUSKey"
```

```

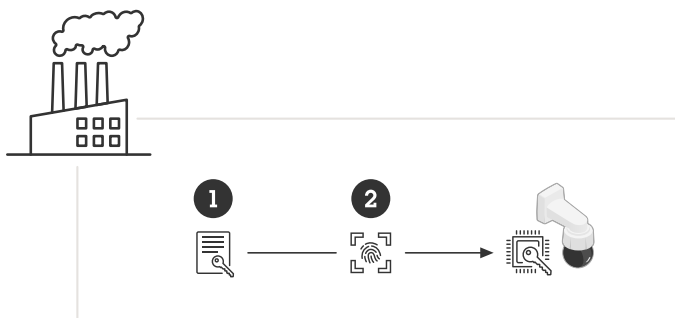
aaa authentication port-access eap-radiusaaa port-access authenticator 18-19aaa port-access
authenticator 18 reauth-period 300aaa port-access authenticator 19 reauth-period 300aaa port-
access authenticator active

```

Konfiguration Axis

Axis Netzwerkgerät

Axis Geräte mit *Axis Edge Vault*-Unterstützung werden werkseitig mit einer sicheren Geräteerkennung ausgestattet, der Axis Geräte-ID. Die Axis Geräte-ID basiert auf dem internationalen Standard IEEE 802.1AR, der eine Methode für die automatisierte, sichere Erkennung von Geräten und das Onboarding über IEEE 802.1X definiert.



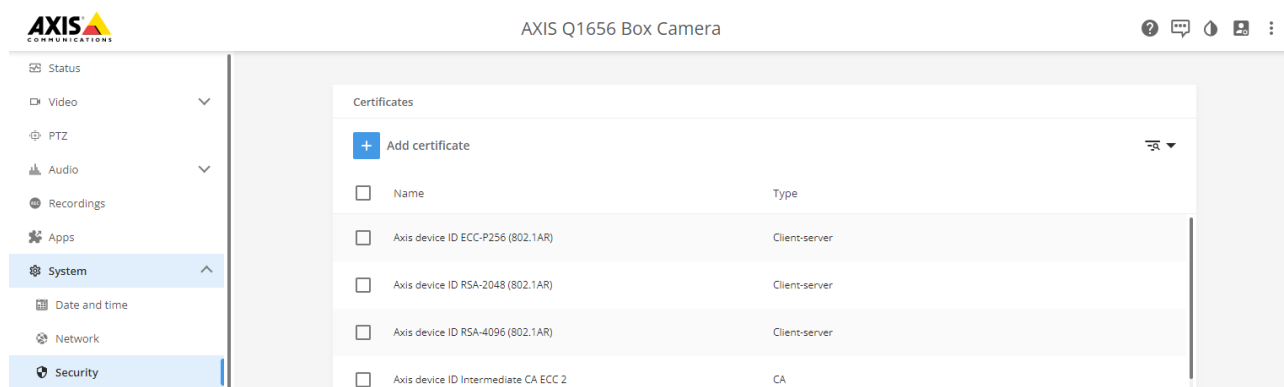
Axis Geräte werden mit dem IEEE 802.1AR-konformen Axis Geräte-ID-Zertifikat für vertrauenswürdige Geräteidentitätsdienste hergestellt

- 1 Axis Geräte-ID Public Key Infrastructure (PKI)
- 2 Axis Geräte-ID

Der hardwaregeschützte sichere Schlüsselspeicher, der von einem sicheren Element des Axis Geräts bereitgestellt wird, ist werkseitig mit einem gerätespezifischen Zertifikat und entsprechenden Schlüsseln (Axis Geräte-ID) ausgestattet, die die Authentizität des Axis Geräts global nachweisen können. Mit dem *Axis Product Selector* können Sie ermitteln, welche Axis Geräte Axis Edge Vault und Axis Geräte-ID unterstützen.

Hinweis

Die Seriennummer eines Axis Geräts ist seine MAC Adresse.



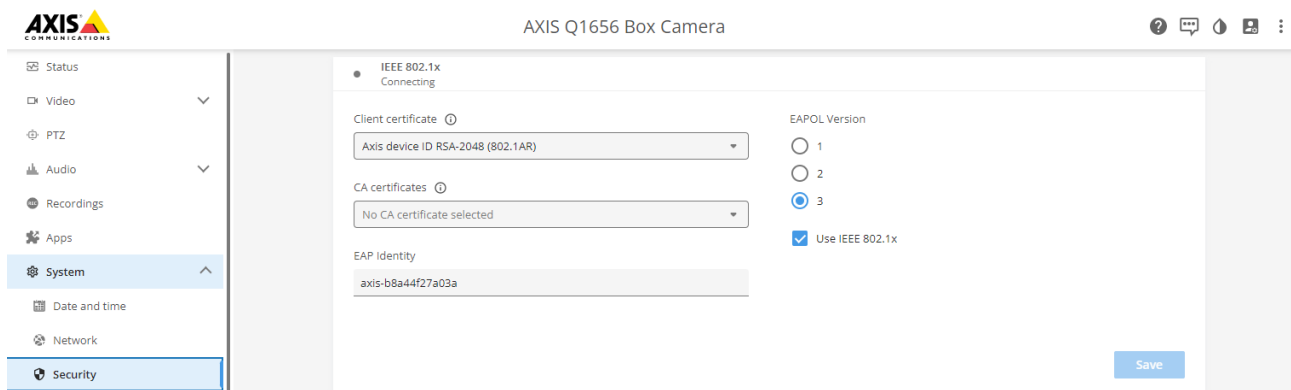
Der Zertifikatspeicher des Axis Geräts in der werkseitigen Standardeinstellung mit der Axis Geräte-ID.

Das IEEE 802.1AR-konforme Axis Geräte-ID-Zertifikat enthält Informationen zur Seriennummer und andere herstellersistenspezifische Informationen. Diese Informationen nutzt der ClearPass Policy Manager bei der Analyse und Entscheidungsfindung zur Gewährung des Zugriffs auf das Netzwerk. Die folgenden Informationen können Sie einem Axis Geräte-ID-Zertifikat entnehmen:



Land	SE
Standort	Lund
Ausstellerorganisation	Axis Communications AB
Allgemeiner Name des Ausstellers	Axis Geräte-ID intermediär
Organisation	Axis Communications AB
Einfacher Name	axis-b8a44f279511-eccp256-1
Seriennummer	b8a44f279511

Der einfache Name setzt sich aus einer Kombination des Firmennamens Axis, der Seriennummer des Geräts und schließlich des Kryptoalgorithmus (ECC P256, RSA 2048, RSA 4096) zusammen. Ab AXIS OS 10.1 (September 2020) ist IEEE 802.1X standardmäßig mit vorkonfigurierter Axis Geräte-ID aktiviert. Dadurch kann sich das Gerät in IEEE 802.1X-fähigen Netzwerken authentifizieren.



Das Axis Gerät in der werkseitigen Standardeinstellung mit aktiviertem IEEE 802.1X und vorab ausgewähltem Axis Geräte-ID-Zertifikat.

AXIS Device Manager

AXIS Device Manager und AXIS Device Manager Extend erlauben die kosteneffiziente Konfiguration und Verwaltung mehrerer Axis Geräte in einem Netzwerk. AXIS Device Manager ist eine Microsoft Windows®-basierte Anwendung, die lokal auf einem Rechner im Netzwerk installiert ist. Im Gegensatz dazu basiert AXIS Device Manager Extend auf einer Cloud-Infrastruktur, die die Verwaltung von Geräten an mehreren Standorten erlaubt. Beide bieten einfache Verwaltungs- und Konfigurationsfunktionen wie:

- Installation von AXIS OS-Aktualisierungen.
- Anwendung von Cybersicherheitskonfigurationen wie HTTPS- und IEEE 802.1X-Zertifikaten.
- Konfiguration gerätespezifischer Einstellungen wie Bildeinstellungen usw.

Sicherer Netzbetrieb – IEEE 802.1AE MACsec



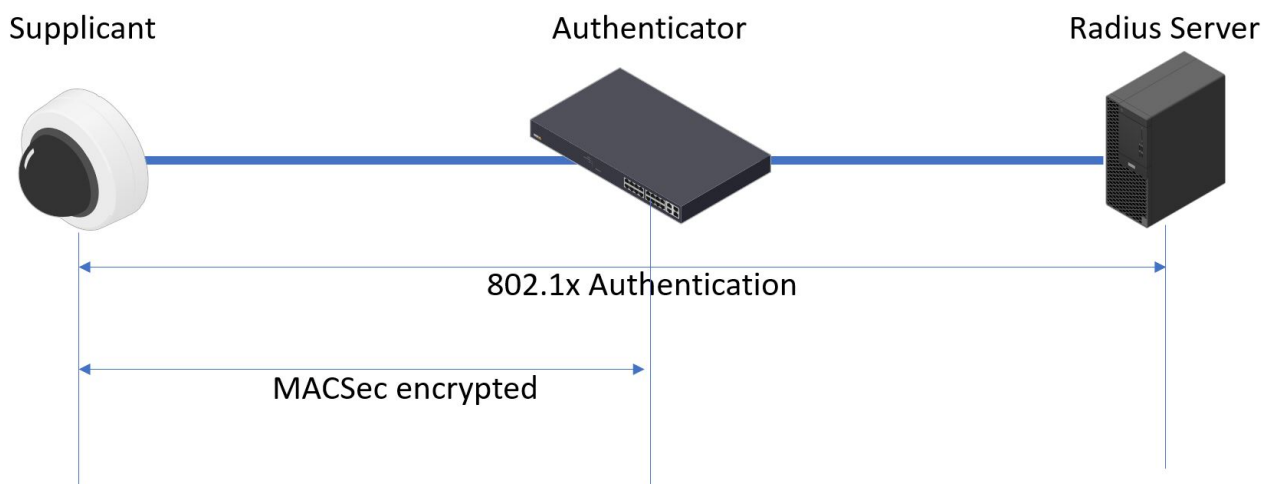
Rufen Sie zur Wiedergabe dieses Videos die Webversion dieses Dokuments auf.

Zero-Trust-Netzwerkverschlüsselung mit Sicherheitsstufe IEEE 802.1AE IEEEsec Layer-2

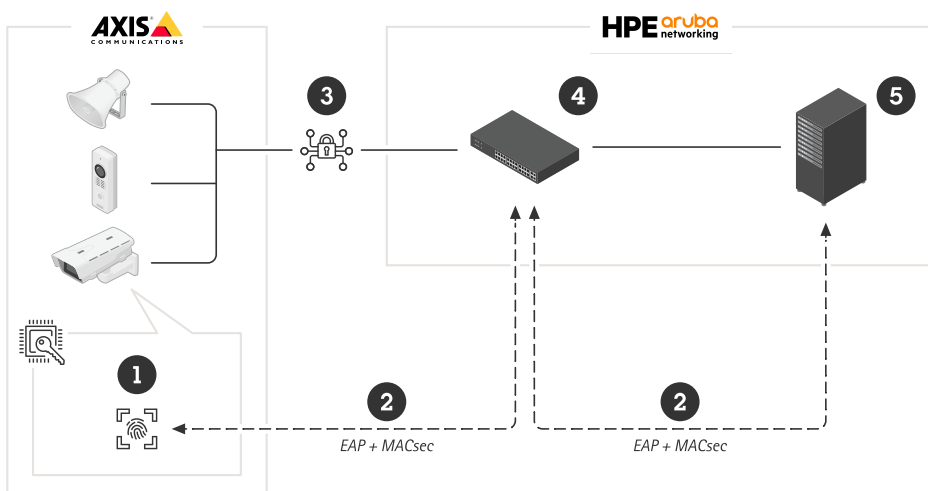
IEEE 802.1AE MACsec (Media Access Control Security) ist ein genau definiertes Netzwerkprotokoll, das Punkt-zu-Punkt-Ethernet-Verbindungen auf Netzwerkschicht 2 kryptografisch sichert. Es gewährleistet die Vertraulichkeit und Integrität der Datenübertragungen zwischen zwei Hosts.

Der IEEE 802.1AE MACsec-Standard beschreibt zwei Betriebsmodi:

- Manuell konfigurierbarer vorinstallierter Schlüssel/Static CAK-Modus
- Automatische Master-Sitzung/dynamischer CAK-Modus mit IEEE 802.1X EAP-TLS



Bei AXIS OS 10.1 (September 2020) und höher ist IEEE 802.1X standardmäßig für Geräte aktiviert, die mit der Axis Geräte-ID kompatibel sind. Bei AXIS OS 11.8 und höher wird MACsec mit einem automatischen dynamischen Modus unterstützt, wobei IEEE 802.1X-EAP-TLS standardmäßig aktiviert ist. Wenn Sie ein Axis Gerät mit werkseitiger Standardeinstellung verbinden, wird IEEE 802.1X für die Netzwerkauthentifizierung genutzt und bei Erfolg außerdem der dynamische CAK-Modus für die MACsec-Verbindung getestet.



Die sicher gespeicherte Axis Geräte-ID (1), eine IEEE 802.1AR-konforme sichere Geräteerkennung, dient zur Authentifizierung im Netzwerk (4, 5) durch die portbasierte IEEE 802.1X-EAP-TLS-Netzwerkzugriffskontrolle (2). Über die EAP-TLS-Sitzung werden MACsec-Schlüssel automatisch ausgetauscht, um eine sichere Verbindung einzurichten (3), die den gesamten Netzwerkverkehr vom Axis Gerät zum HPE Aruba Netzwerk-Switch schützt.

Für IEEE 802.1AE MACsec sind sowohl Konfigurationsvorbereitungen für den HPE Aruba Netzwerk-Zugangsschalter als auch für den ClearPass Policy Manager erforderlich. Um IEEE 802.1AE MACsec-verschlüsselte Kommunikation über EAP-TLS zu ermöglichen, ist keine Konfiguration auf dem Axis Gerät erforderlich.

Wenn der HPE Aruba Netzwerk-Zugangsschalter MACsec mit EAP-TLS nicht unterstützt, kann der Pre-Shared Key-Modus verwendet und manuell konfiguriert werden.

HPE Aruba Networking ClearPass Policy Manager

Rollen- und Rollenzuordnungsrichtlinie

The screenshot displays the ClearPass Policy Manager web interface. The left sidebar shows the navigation menu with categories like Dashboard, Monitoring, Configuration, Identity, Posture, Enforcement, Network, and Administration. The main content area is titled 'Roles' and shows a list of roles. An 'Edit Role' dialog box is open, showing the following details:

- Role ID: 3001
- Name: AxisDevice
- Description: (empty text area)

The background shows a table of roles with checkboxes for selection. The roles listed include [AirGroup v1], [AirGroup v2], [Aruba TACACS+ read-only Admin], [Aruba TACACS+ root Admin], [AxisDevice], [BYOD], [Contract], [Device], [Employee], [Guest], [MAC], [Onboard], [Onboard iOS], [Onboard iPadOS], [Onboard Linux], [Onboard macOS], [Onboard Windows], [Other], and [TACACS+ API Admin].

Hinzufügen eines Rollennamens für Axis Geräte. Der Name ist der Name der Port-Zugriffsrolle in der Zugangsschalter-Konfiguration.

Configuration » Identity » Role Mappings » Edit - Axis Role Mapping

Role Mappings - Axis Role Mapping

Summary Policy Mapping Rules

Policy:

Policy Name: Axis Role Mapping

Description:

Default Role: [Guest]

Mapping Rules:

Rules Evaluation Algorithm: Evaluate all

Conditions	Role Name
1. (Authentication:Full-Username BEGINS_WITH axis-00408c)	AxisDevice
2. (Authentication:Full-Username BEGINS_WITH axis-acc8e)	AxisDevice
3. (Authentication:Full-Username BEGINS_WITH axis-b8a44f)	AxisDevice

Back to Role Mappings Copy Save Cancel

Copyright 2023 Hewlett Packard Enterprise Development LP Oct 26, 2023 05:08:20 UTC ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform

Hinzufügen einer Axis Rollenzuordnungsrichtlinie für die zuvor erstellte Axis Geräte Rolle. Die definierten Bedingungen sind erforderlich, damit ein Gerät der Axis Geräte Rolle zugeordnet werden kann. Wenn die Bedingungen nicht erfüllt sind, wird dem Geräte eine Gastrolle [Guest] zugewiesen.

Standardmäßig nutzen Axis Geräte das EAP-Kennungsformat „axis-Seriennummer“. Die Seriennummer eines Axis Geräts wird als dessen MAC-Adresse verwendet. Zum Beispiel „axis-b8a44f45b4e6“.

Servicekonfiguration

Configuration » Services » Edit - Axis 802.1X Wired

Services - Axis 802.1X Wired

Summary Service Authentication Roles Enforcement

Role Mapping Policy: Axis Role Mapping Modify Add New Role Mapping Policy

Role Mapping Policy Details

Description:

Default Role: [Guest]

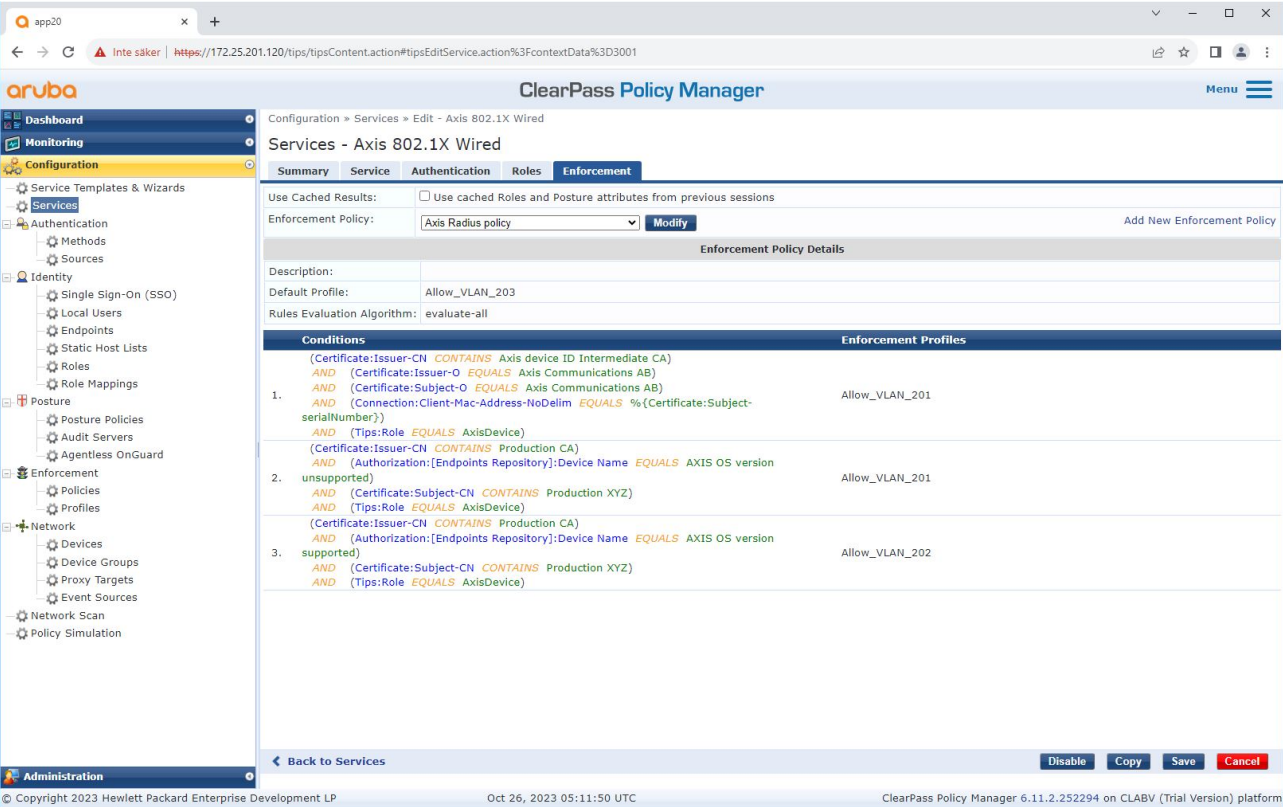
Rules Evaluation Algorithm: evaluate-all

Conditions	Role
1. (Authentication:Full-Username BEGINS_WITH axis-00408c)	AxisDevice
2. (Authentication:Full-Username BEGINS_WITH axis-acc8e)	AxisDevice
3. (Authentication:Full-Username BEGINS_WITH axis-b8a44f)	AxisDevice

Back to Services Disable Copy Save Cancel

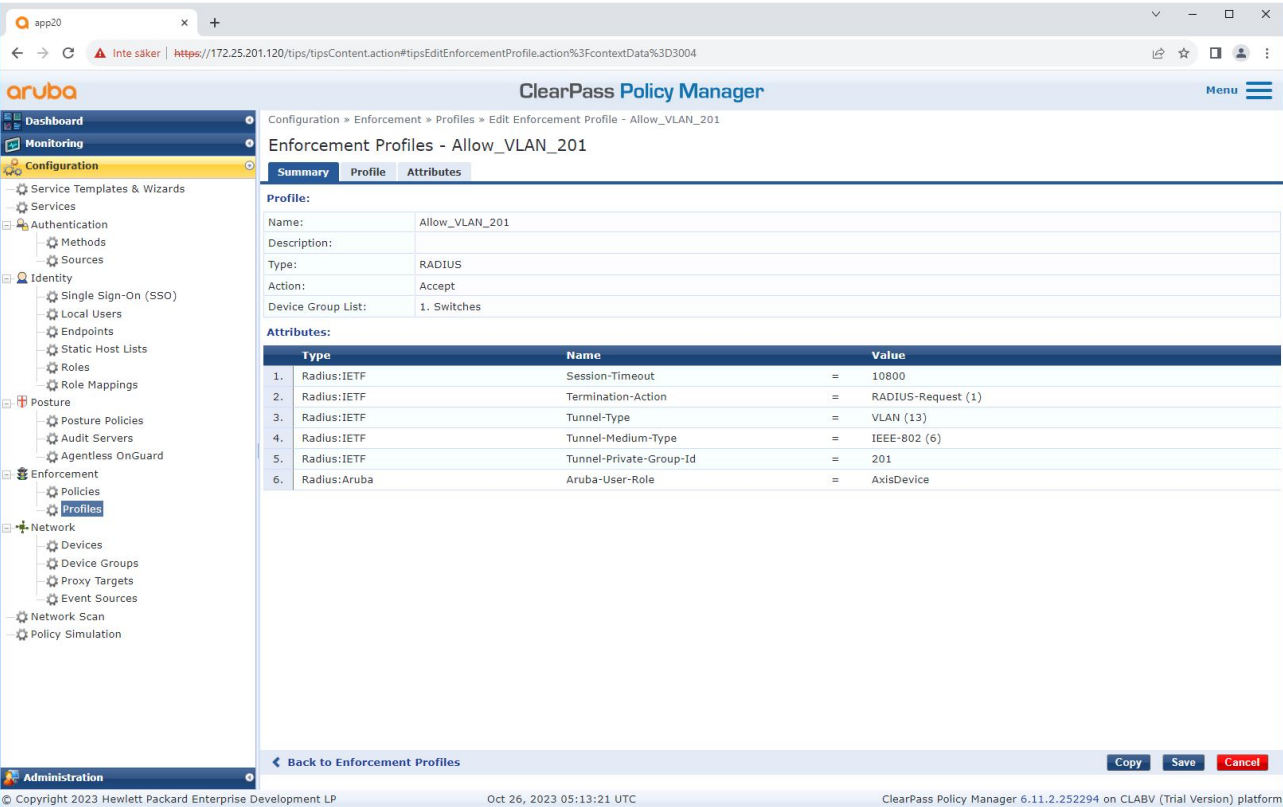
Copyright 2023 Hewlett Packard Enterprise Development LP Oct 26, 2023 05:09:16 UTC ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform

Hinzufügen der zuvor erstellten Axis Rollenzuordnungsrichtlinie zum Dienst, der IEEE 802.1X als Verbindungsmethode für das Onboarding von Axis Geräten definiert.



Hinzufügen des Axis Rollennamens als Bedingung zu den vorhandenen Richtliniendefinitionen.

Durchsetzungsprofil



Hinzufügen des Axis Rollennamens als Attribut zu den im IEEE 802.1X-Onboarding-Dienst zugewiesenen Durchsetzungsprofilen.

HPE Aruba Networking Zugangsschalter

Zusätzlich zur sicheren Onboarding-Konfiguration, die in *HPE Aruba Networking Zugangsschalter, on page 15* beschrieben wird, finden Sie weitere Informationen in der folgenden Beispiel-Portkonfiguration des HPE Aruba Networking-Zugangsschalters zur Konfiguration von IEEE 802.1AE MACsec.

```
macsec policy macsec-eapcipher-suite gcm-aes-128
port-access role AxisDeviceassociate macsec-policy macsec-eapauth-mode client-mode
aaa authentication port-access dot1x authenticatormacsecmkacac-length 16enable
```

Zertifikatsverwaltung – Enrollment over Secure Transport (EST)

Digitale Zertifikate sind für den Schutz von Geräten und Netzwerken von entscheidender Bedeutung, ihre Verwaltung kann jedoch komplex und zeitaufwändig sein. Zertifikate laufen ab und müssen regelmäßig erneuert werden. Ohne Automatisierung muss dieser Prozess manuell ausgeführt werden und wiederholt sich ständig, was speziell bei großen Systemen oder Systemen mit verschiedenen Gerätetypen gilt.

AXIS OS 12.9 unterstützt jetzt Enrollment over Secure Transport (EST), ein Protokoll zur sicheren automatisierten Ausstellung von Zertifikaten für Geräte. EST ist in RFC 7030 definiert und stellt eine standardisierte Lösung dar, die den gesamten Lebenszyklus von Zertifikaten vereinfacht und automatisiert, einschließlich:

- Registrierung – sichere Ausstellung neuer Zertifikate für Geräte
- Erneuerung – automatischer Ersatz ablaufender Zertifikate
- Neuregistrierung – Aktualisierung von Zertifikaten gemäß IT-Richtlinien

EST unterstützt IT-definierte Richtlinien für Zertifikatsattribute wie Gültigkeitsdauer, Schlüsseltyp (RSA/ECC) oder Schlüsselgröße und verwendet ausschließlich HTTPS.

Wichtigste Vorteile von EST

- Die automatisierte Registrierung, Erneuerung und Neuregistrierung von Zertifikaten auf der Grundlage von IT-Richtlinien, wodurch die zeitaufwändige manuelle Konfiguration vollständig entfällt.
- Hochmoderne, sichere Kommunikation ausschließlich über HTTPS TLS 1.2/1.3.
- Zentralisierte Sichtbarkeit/Überwachung für IT-Teams.
Standardisierung (RFC 7030) und Integration in die IT-Infrastruktur.
- Skalierbare Lösung für IoT, Unternehmensnetzwerke und Gerätemanagement.

Die allgemeine EST-Dokumentation finden Sie in unserer AXIS OS-Wissensdatenbank *AXIS OS Knowledge Base*.

Konfiguration von HPE Aruba ClearPass Onboard

Aruba ClearPass Onboard lässt sich mit EST kombinieren, um Gerätezertifikate für den Netzwerkzugriff sicher zu verteilen und zu verwalten. Mithilfe von EST authentifizieren sich Endpunkte bei ClearPass und registrieren sich über einen sicheren TLS-Kanal für ein eindeutiges Zertifikat, das anschließend für die Authentifizierung auf Grundlage des 802.1X-Zertifikats und andere Dienste verwendet wird. Das bietet ein standardisiertes, automatisiertes und kennwortloses Verfahren zur Durchsetzung von Richtlinien für den sicheren Zugriff auf Grundlage der Geräteidentität.

Konfiguration der Zertifizierungsstelle

ClearPass Onboard

Home » Onboard » Certificate Authorities

Certificate Authorities

There are errors with the server certificate configuration that will prevent devices from provisioning or authenticating:
 app20.r2d2.lab: The ClearPass HTTPS server root certificate is not trusted by Apple. This will cause enrollment over HTTPS to fail on iOS and iPadOS devices.
 app20.r2d2.lab: Self signed ClearPass RADIUS server certificate will cause some models of Android devices to fail to authenticate.

How do I fix this problem?

Use this list to manage certificate authorities.

Name	Mode	Status	Expiry	OCSP URL
Local Certificate Authority This is the default certificate authority.	root	Valid	2032-09-29T12:40:04+02:00	http://app20.r2d2.lab/onboard/mdps_ocsp.php/1
R2D2 ClearPass CA	root	Valid	2035-07-17T10:24:56+02:00	http://app20.r2d2.lab/onboard/mdps_ocsp.php/2
R2D2 EST CA 1	root	Valid	2035-07-17T10:56:41+02:00	http://app20.r2d2.lab/onboard/mdps_ocsp.php/3
R2D2 EST CA 2	root	Valid	2035-07-17T10:57:47+02:00	http://app20.r2d2.lab/onboard/mdps_ocsp.php/4

Refresh 1 Showing 1 - 4 of 4 20 rows per page

Back to Onboard
Back to main

© Copyright 2026 Hewlett Packard Enterprise Development LP ClearPass Onboard 6.11.2.252294 on CLABV platform

Erstellen Sie eine neue Zertifizierungsstelle in ClearPass Onboard.

ClearPass Onboard

Home » Onboard » Certificate Authorities

Certificate Authorities

There are errors with the server certificate configuration that will prevent devices from provisioning or authenticating:
 app20.r2d2.lab: The ClearPass HTTPS server root certificate is not trusted by Apple. This will cause enrollment over HTTPS to fail on iOS and iPadOS devices.
 app20.r2d2.lab: Self signed ClearPass RADIUS server certificate will cause some models of Android devices to fail to authenticate.

How do I fix this problem?

Use this list to manage certificate authorities.

Name	Mode	Status	Expiry	OCSP URL
Local Certificate Authority This is the default certificate authority.	root	Valid	2032-09-29T12:46:04+02:00	http://app20.r2d2.lab/onboard/mdps_ocsp.php/1
R2D2 ClearPass CA	root	Valid	2035-07-17T10:24:56+02:00	http://app20.r2d2.lab/onboard/mdps_ocsp.php/2
R2D2 EST CA 1	root	Valid	2035-07-17T10:56:41+02:00	http://app20.r2d2.lab/onboard/mdps_ocsp.php/3
R2D2 EST CA 2	root	Valid	2035-07-17T10:57:47+02:00	http://app20.r2d2.lab/onboard/mdps_ocsp.php/4

Refresh 1 Showing 1 - 4 of 4 20 rows per page

Back to Onboard
Back to main

© Copyright 2026 Hewlett Packard Enterprise Development LP ClearPass Onboard 6.11.2.252294 on CLABV platform

In der erstellten Zertifizierungsstelle werden der Schlüsseltyp, die Schlüsselgröße, die Gültigkeitsdauer und weitere Parameter definiert.

Guest

Devices

Onboard

Certificate Authorities

Management and Control

View by Device

View by Username

View by Certificate

Usage

Configuration

Network Settings

IOS Settings

Windows Applications

Deployment and Provisioning

Configuration Profiles

Provisioning Settings

Self-Service Portal

Configuration

Administration

ClearPass Onboard

Menu

Certificate Authority Settings

* Name: R2D2 EST CA 2

Description:

Mode: Root CA

Certificate Issuing

* Authority Info Access: Do not include OCSP Responder URL

* Validity Period: 365 days

* Clock Skew Allowance: 15

Subject Alternative Name:

* Digest Algorithm: SHA-256

Retention Policy

Store Certificates:

Maximum Period: 52 weeks

SCEP Server

SCEP Server:

Copyright 2026 Hewlett Packard Enterprise Development LP

ClearPass Onboard 6.11.2.252294 on CLABV platform

Aktivieren Sie die EST-Server-Funktion für die erstellte Zertifizierungsstelle. Konfigurieren Sie die EST-Authentifizierungsmethode für die Verwendung eines Client-Zertifikats.

Konfiguration von HPE Aruba ClearPass Policy Manager

Konfiguration des vertrauenswürdigen Zertifikatspeichers

Dashboard

Monitoring

Configuration

Administration

ClearPass Portal

Users and Privileges

Admin Users

Admin Privileges

Server Manager

Server Configuration

Log Configuration

Local Shared Folders

Licensing

Device Insight

External Servers

SNMP Trap Receivers

Syslog Targets

Syslog Export Filters

Messaging Setup

Endpoint Context Servers

File Backup Servers

External Accounts

Certificates

Certificate Store

Trust List

Revocation Lists

Dictionaries

RADIUS

RADIUS Dynamic Authorizati

TACACS+ Services

Device Fingerprints

Dictionary Attributes

ClearPass Policy Manager

Menu

Administration » Certificates » Trust List

Certificate Trust List

This page displays a list of trusted Certificate Authorities (CA). You can add, view, or delete a certificate.

Filter: Subject contains Axis Go Clear Filter

Show 20 records

#	Subject	Usage	Validity	Enabled
1.	☐ CN=Axis device ID Intermediate CA ECC 1,O=Axis Communications AB	EAP, EST	Valid	Enabled
2.	☐ CN=Axis device ID Intermediate CA ECC 2,O=Axis Communications AB	EAP, EST	Valid	Enabled
3.	☐ CN=Axis device ID Intermediate CA RSA 1,O=Axis Communications AB	EAP, EST	Valid	Enabled
4.	☐ CN=Axis device ID Intermediate CA RSA 2,O=Axis Communications AB	EAP, EST	Valid	Enabled
5.	☐ CN=Axis device ID Root CA ECC,O=Axis Communications AB	EAP, EST	Valid	Enabled
6.	☐ CN=Axis device ID Root CA RSA,O=Axis Communications AB	EAP, EST	Valid	Enabled
7.	☐	EAP, EST	Valid	Enabled
8.	☐ emailAddress=,CN=R2D2 ClearPass CA,O=R2D2,L=Lund,ST=Skane,C=SE	EAP, EST, Others	Valid	Enabled
9.	☐ emailAddress=,CN=R2D2 ClearPass Signing CA,O=R2D2,L=Lund,ST=Skane,C=SE	EAP, EST, Others	Valid	Enabled
10.	☐ emailAddress=,CN=R2D2 EST CA 1,O=R2D2,L=Lund,ST=Skane,C=SE	EAP, EST, Others	Valid	Enabled
11.	☐ emailAddress=,CN=R2D2 EST CA 2,O=R2D2,L=Lund,ST=Skane,C=SE	EAP, EST, Others	Valid	Enabled
12.	☐ emailAddress=,CN=R2D2 EST Signing CA 1,O=R2D2,L=Lund,ST=Skane,C=SE	EAP, EST, Others	Valid	Enabled
13.	☐ emailAddress=,CN=R2D2 EST Signing CA 2,O=R2D2,L=Lund,ST=Skane,C=SE	EAP, EST, Others	Valid	Enabled

Showing 1-13 of 13

Delete

Copyright 2023 Hewlett Packard Enterprise Development LP

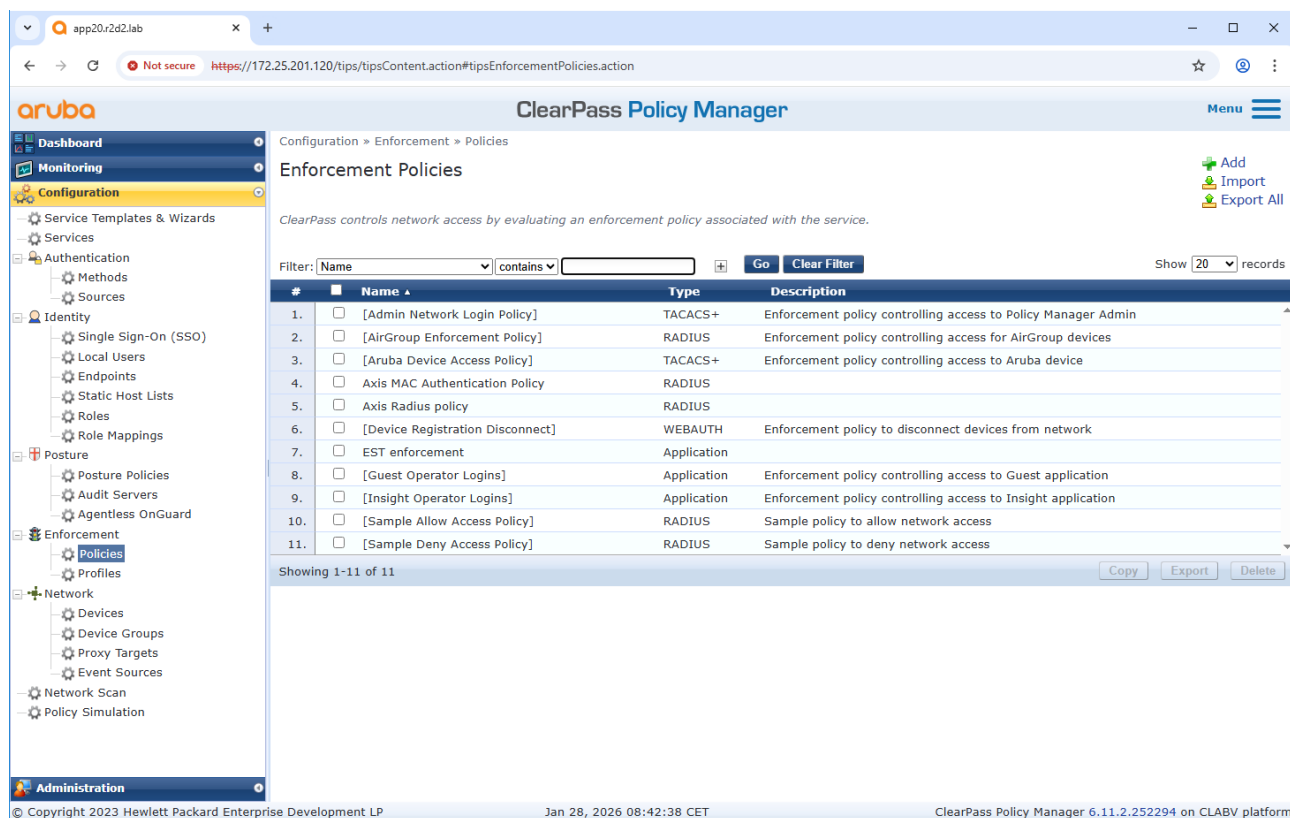
Jan 28, 2026 08:50:04 CET

ClearPass Policy Manager 6.11.2.252294 on CLABV platform

Falls nicht schon geschehen, laden Sie die *für Axis spezifischen IEEE 802.1AR-Zertifikate* in den Speicher für vertrauenswürdige Zertifikate des ClearPass Policy Managers. Achten Sie darauf, die EST-Nutzung hinzuzufügen. Überprüfen Sie dies auch für die zuvor erstellte Zertifizierungsstelle von ClearPass Onboard.

Konfiguration der Durchsetzungsrichtlinie

Mit dem Durchsetzungsprofil kann der ClearPass Policy Manager bestimmte Durchsetzungsmaßnahmen mit der EST-Anwendung verknüpfen. So können Sie beispielsweise festlegen, dass neue Zertifikate nur von bestimmten Endpunkten oder nur an bestimmten Wochentagen registriert werden dürfen.



Configuration » Enforcement » Policies

Enforcement Policies

ClearPass controls network access by evaluating an enforcement policy associated with the service.

Filter: Name contains [] Go Clear Filter Show 20 records

#	Name	Type	Description
1.	[Admin Network Login Policy]	TACACS+	Enforcement policy controlling access to Policy Manager Admin
2.	[AirGroup Enforcement Policy]	RADIUS	Enforcement policy controlling access for AirGroup devices
3.	[Aruba Device Access Policy]	TACACS+	Enforcement policy controlling access to Aruba device
4.	Axis MAC Authentication Policy	RADIUS	
5.	Axis Radius policy	RADIUS	
6.	[Device Registration Disconnect]	WEBAUTH	Enforcement policy to disconnect devices from network
7.	EST enforcement	Application	
8.	[Guest Operator Logins]	Application	Enforcement policy controlling access to Guest application
9.	[Insight Operator Logins]	Application	Enforcement policy controlling access to Insight application
10.	[Sample Allow Access Policy]	RADIUS	Sample policy to allow network access
11.	[Sample Deny Access Policy]	RADIUS	Sample policy to deny network access

Showing 1-11 of 11

Copy Export Delete

© Copyright 2023 Hewlett Packard Enterprise Development LP Jan 28, 2026 08:42:38 CET ClearPass Policy Manager 6.11.2.252294 on CLABV platform

Übersicht über die Durchsetzungsrichtlinien im ClearPass Policy Manager.

app20.r2d2.lab

Not secure https://172.25.201.120/tips/tipsContent.action#tipsEditEnforcementPolicy.action%3FcontextData%3D3016

aruba

ClearPass Policy Manager

Menu

Dashboard

Monitoring

Configuration

Administration

Service Templates & Wizards

Services

Authentication

Identity

Posture

Enforcement

Network

Configuration > Enforcement > Policies > Edit - EST enforcement

Enforcement Policies - EST enforcement

Summary Enforcement Rules

Enforcement:

Name: EST enforcement

Description:

Enforcement Type: Application

Default Profile: [Deny Application Access Profile]

Rules:

Rules Evaluation Algorithm: First applicable

Conditions

Actions

1. (Date:Day-of-Week BELONGS_TO Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday)

[Allow Application Access Profile]

Back to Enforcement Policies

Copy Save Cancel

Copyright 2023 Hewlett Packard Enterprise Development LP

Jan 28, 2026 08:43:37 CET

ClearPass Policy Manager 6.11.2.252294 on CLABV platform

In dieser Beispielrichtlinie hat die EST-Anwendung eine Berechtigung für alle Tage der Woche.

Servicekonfiguration

app20.r2d2.lab

Not secure https://172.25.201.120/tips/tipsContent.action#tipsServices.action

aruba

ClearPass Policy Manager

Menu

Dashboard

Monitoring

Configuration

Administration

Service Templates & Wizards

Services

Authentication

Identity

Posture

Enforcement

Network

Configuration > Services

Services

Add

Import

Export All

This page shows the current list and order of services that ClearPass follows during authentication and authorization.

Filter: Name contains Go Clear Filter Hit Count for Current hour Show 20 records

#	Order	Name	Type	Template	Hit Count	Status
1.	1	Axis 802.1X Wired	RADIUS	802.1X Wired	0	✓
2.	2	Axis 802.1X Wired - Mac Authentication	RADIUS	MAC Authentication	0	✓
3.	3	[Policy Manager Admin Network Login Service]	TACACS+	TACACS+ Enforcement	0	✗
4.	4	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	0	✗
5.	5	[Aruba Device Access Service]	TACACS+	TACACS+ Enforcement	0	✗
6.	6	[Guest Operator Logins]	Application	Aruba Application Authentication	0	✗
7.	7	[Insight Operator Logins]	Application	Aruba Application Authentication	0	✗
8.	8	[Device Registration Disconnect]	WEBAUTH	Web-based Authentication	0	✗
9.	9	EST	Application	Aruba Application Authentication	0	✓

Showing 1-9 of 9 Reorder Copy Export Delete

Copyright 2023 Hewlett Packard Enterprise Development LP

Jan 28, 2026 08:35:09 CET

ClearPass Policy Manager 6.11.2.252294 on CLABV platform

Ein spezieller EST-Dienst muss erstellt werden.

27

Configuration » Services » Edit - EST

Services - EST

Summary Service Authentication Roles Enforcement

Name: EST

Description: Authentication Service for Applications

Type: Aruba Application Authentication

Status: Enabled

Monitor Mode: ☐ Enable to monitor network access without enforcement

More Options: ☐ Authorization

Service Rule

Matches ☒ ANY or ☐ ALL of the following conditions:

Type	Name	Operator	Value
1. Application	Name	EQUALS	EST
2.	Click to add...		

Back to Services Disable Copy Save Cancel

Copyright 2023 Hewlett Packard Enterprise Development LP Jan 28, 2026 08:37:12 CET ClearPass Policy Manager 6.11.2.252294 on CLABV platform

Der Dienst muss für die EST-Anwendung konfiguriert werden.

Configuration » Services » Edit - EST

Services - EST

Summary Service Authentication Roles Enforcement

Use Cached Results: ☐ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: EST enforcement [Modify](#) [Add New Enforcement Policy](#)

Enforcement Policy Details

Description:

Default Profile: [Deny Application Access Profile]

Rules Evaluation Algorithm: first-applicable

Conditions	Enforcement Profiles
1. (Date:Day-of-Week BELONGS_TO Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday)	[Allow Application Access Profile]

Back to Services Disable Copy Save Cancel

Copyright 2023 Hewlett Packard Enterprise Development LP Jan 28, 2026 08:47:35 CET ClearPass Policy Manager 6.11.2.252294 on CLABV platform

Wählen Sie die zuvor erstellte EST-Durchsetzungsrichtlinie aus.

Konfiguration Axis

Die Konfiguration auf dem Axis Gerät erfolgt in zwei Schritten.

1. Stellen Sie eine vertrauenswürdige Verbindung mit dem ClearPass Onboard HTTPS-Endpunkt her.

2. Konfigurieren Sie den EST-Client auf dem Axis Gerät.

Konfiguration des vertrauenswürdigen Zertifikats

The screenshot shows the Aruba Onboard web interface. The left sidebar contains navigation options like Guest, Devices, Onboard, Management and Control, Configuration, and Administration. The main content area displays 'Certificate Authorities' with a list of certificates. A modal window titled 'Certificate Viewer: app20.r2d2.lab' is open, showing the following details:

Issued To	
Common Name (CN)	app20.r2d2.lab
Organization (O)	R2D2
Organizational Unit (OU)	<Not Part Of Certificate>

Issued By	
Common Name (CN)	R2D2 ClearPass Signing CA
Organization (O)	R2D2
Organizational Unit (OU)	<Not Part Of Certificate>

Validity Period	
Issued On	Wednesday, July 16, 2025 at 10:09:31 AM
Expires On	Thursday, July 16, 2026 at 10:39:31 AM

SHA-256 Fingerprints

Field	Value
Certificate	2fb7855b1779c99cc70004ae99ddc94b29ba8d4c4231edf7e39a41e9d08d18d
Public Key	26677c1deb12b5a5ac06ad2ef75881e8d75c8f6cab9830569360de6b5032ec17

Überprüfen Sie die Zertifikatskette vom ClearPass Onboard HTTPS-Endpunkt.

The screenshot shows the Axis P3265-LV Dome Camera web interface. The left sidebar contains navigation options like Status, Video, Analytics, Audio, Recordings, Apps, System, Time and location, Network, Security, Accounts, Events, MQTT, SIP, Storage, Stream profiles, ONVIF, Detectors, Power settings, and Power meter. The main content area displays the 'Security' page with the following sections:

Certificates (33)

+ Add certificate

Filter by name: Select type to filter:

5 rows 10 rows

Name	Type	Secure keystore
☐ GlobalSign Root CA - R6	CA	☐
☐ GlobalSign Root E46	CA	☐
☐ GlobalSign Root R46	CA	☐
☐ ISRG Root X1	CA	☐
☐ R2D2_ClearPass_CA	CA	☐

Secure keystore

☐ Trusted Execution Environment (SoC TEE)

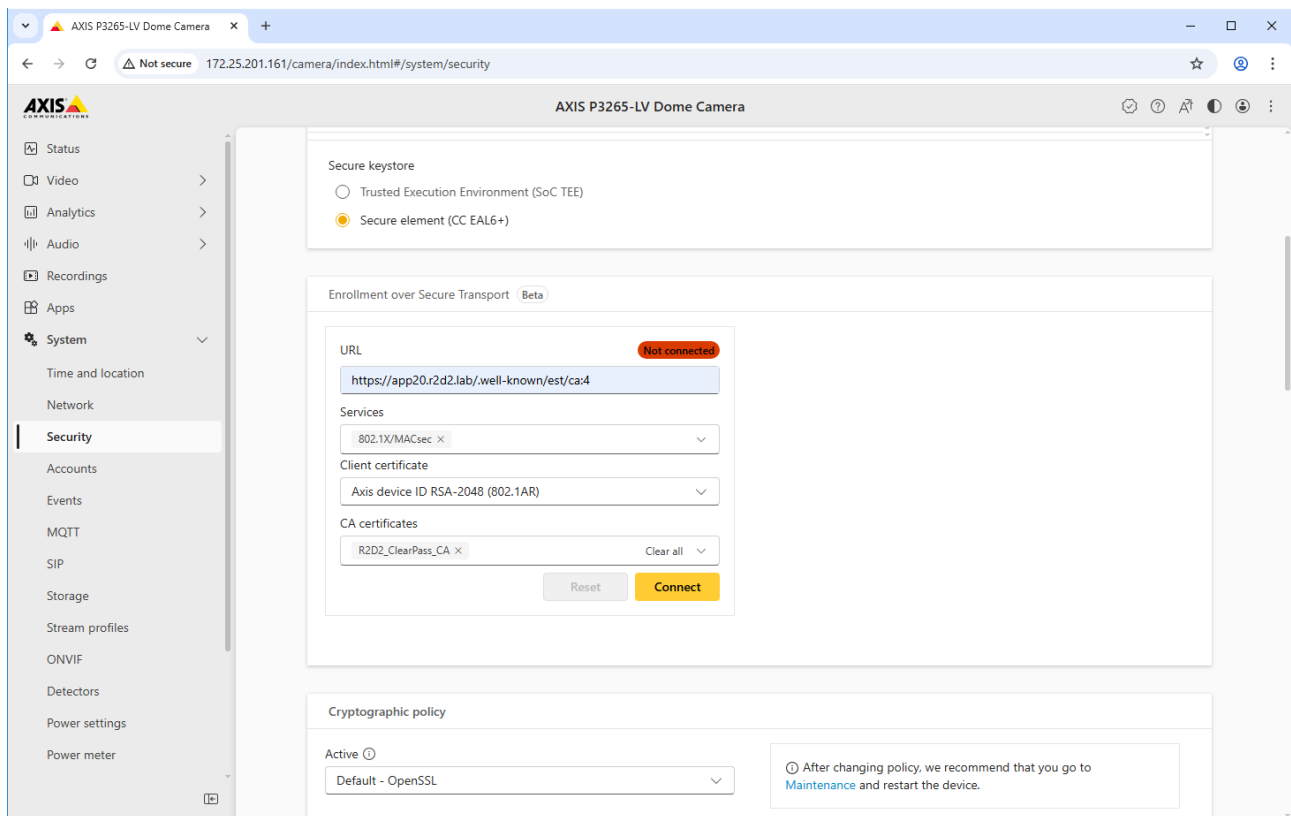
☒ Secure element (CC EAL6+)

Enrollment over Secure Transport Beta

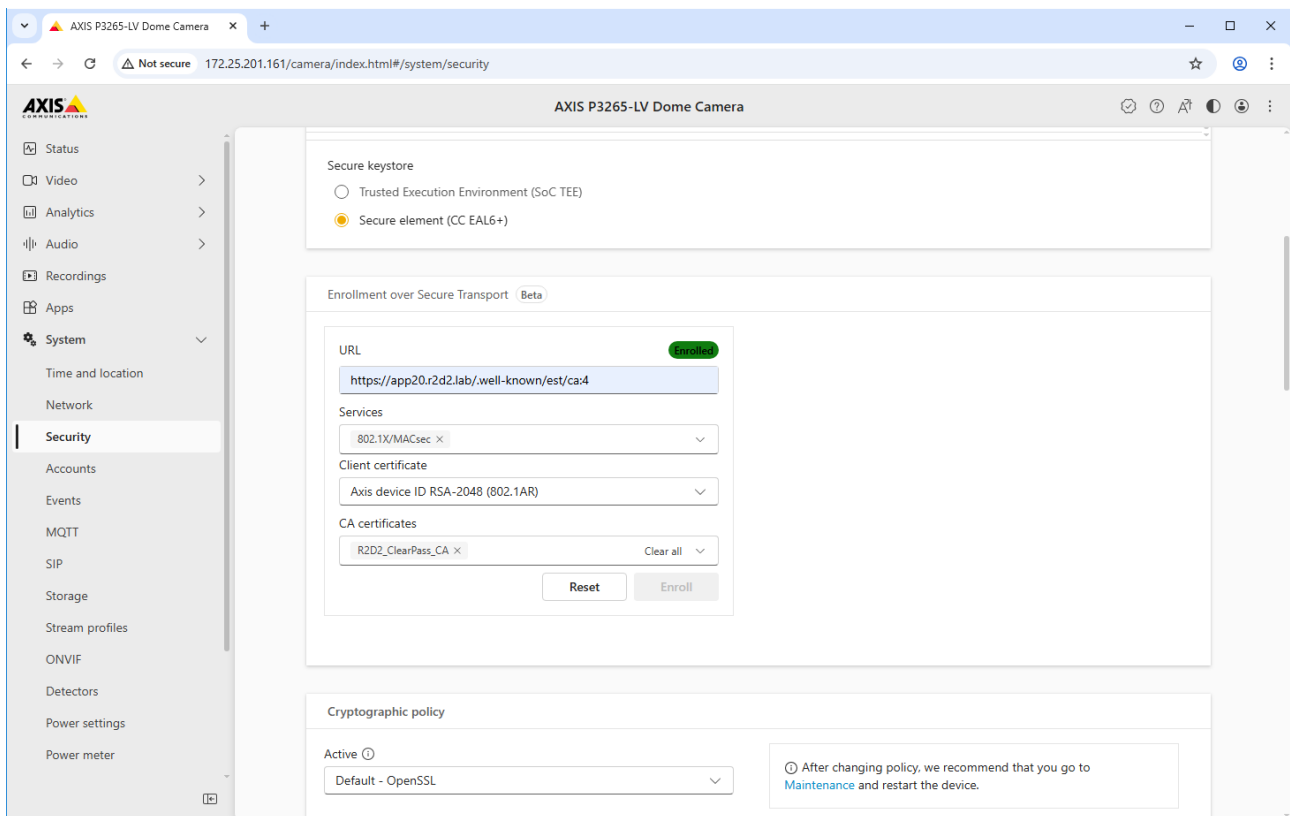
URL: Not connected

Laden Sie die Zertifizierungsstelle vom ClearPass Onboard HTTPS-Endpunkt auf das Axis Gerät hoch.

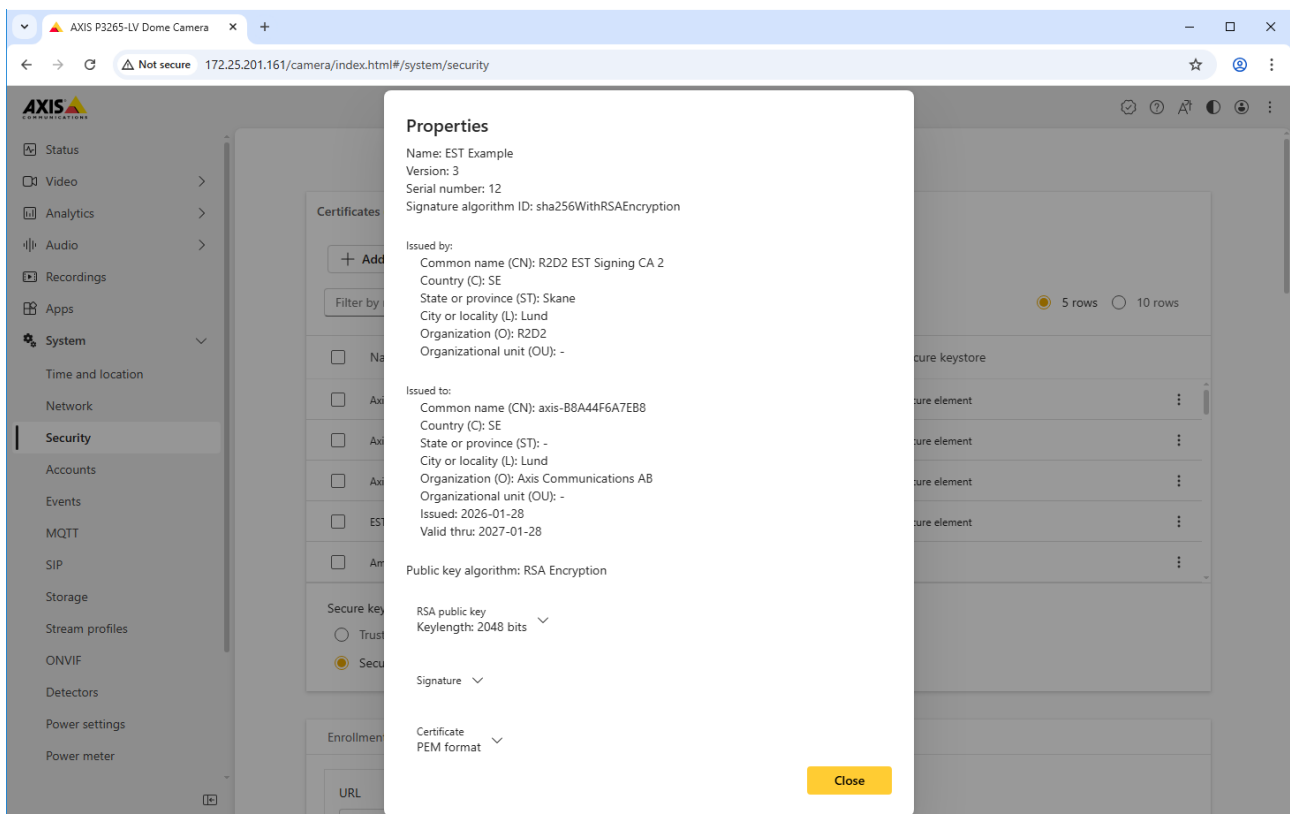
Konfiguration des EST-Clients



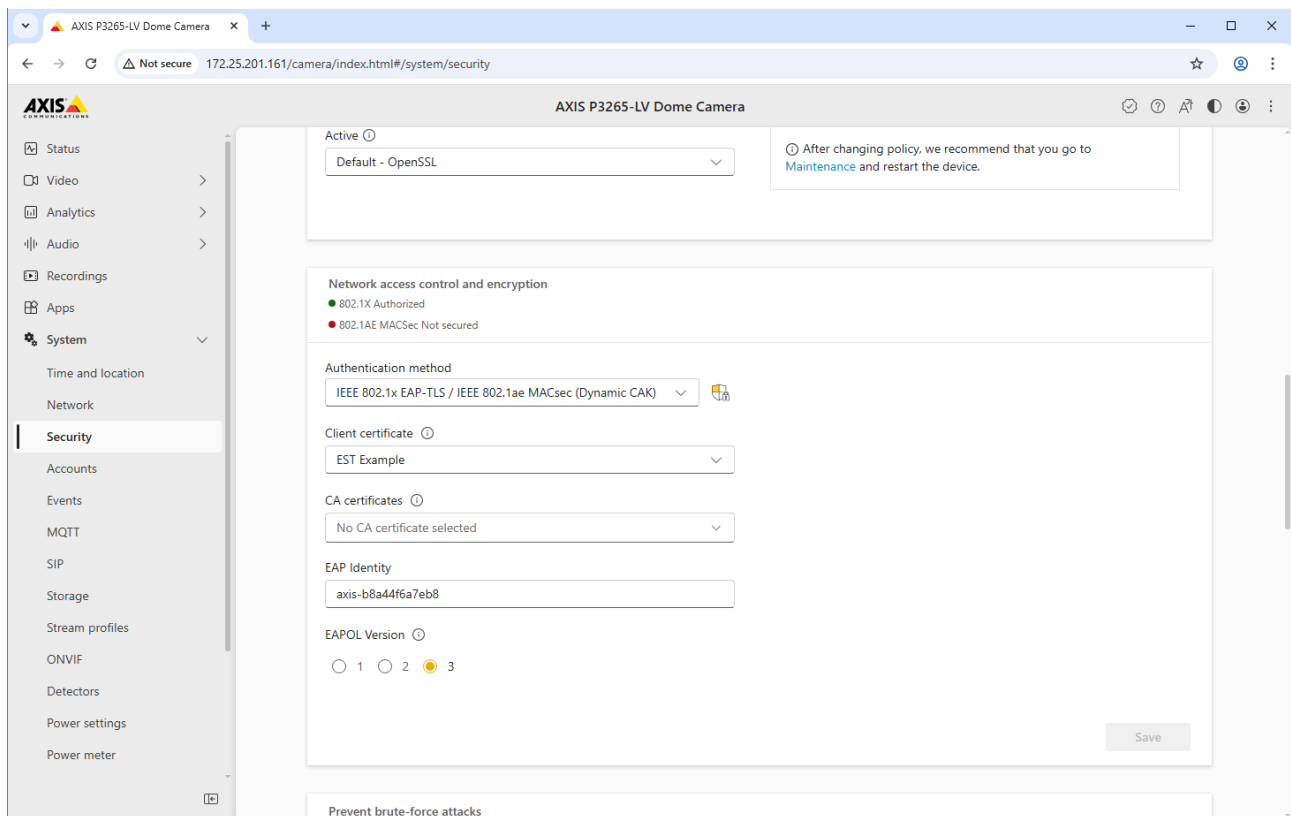
Parameter	Wert
URL	Die EST-URL finden Sie in der erstellten Zertifizierungsstelle für EST in ClearPass Onboard.
Services	Wählen Sie die Dienste aus, die automatisch mit dem registrierten Zertifikat konfiguriert werden sollen.
Client certificate (Clientzertifikat)	Wählen Sie ein Client-Zertifikat für die Authentifizierung beim ClearPass Onboard EST-Server aus. Geräte mit der Axis Geräte-ID werden bei der Registrierung automatisch als vertrauenswürdig eingestuft, da die Axis-spezifische IEEE 802.1AR-Zertifikatskette zum Speicher vertrauenswürdiger Zertifikate im ClearPass Policy Manager hinzugefügt wurde.
CA-Zertifikate	Wählen Sie das CA-Zertifikat des ClearPass Onboard HTTPS-Endpunkts aus, um einer vertrauenswürdige Verbindung zwischen dem Axis Gerät und diesem Endpunkt zu etablieren.



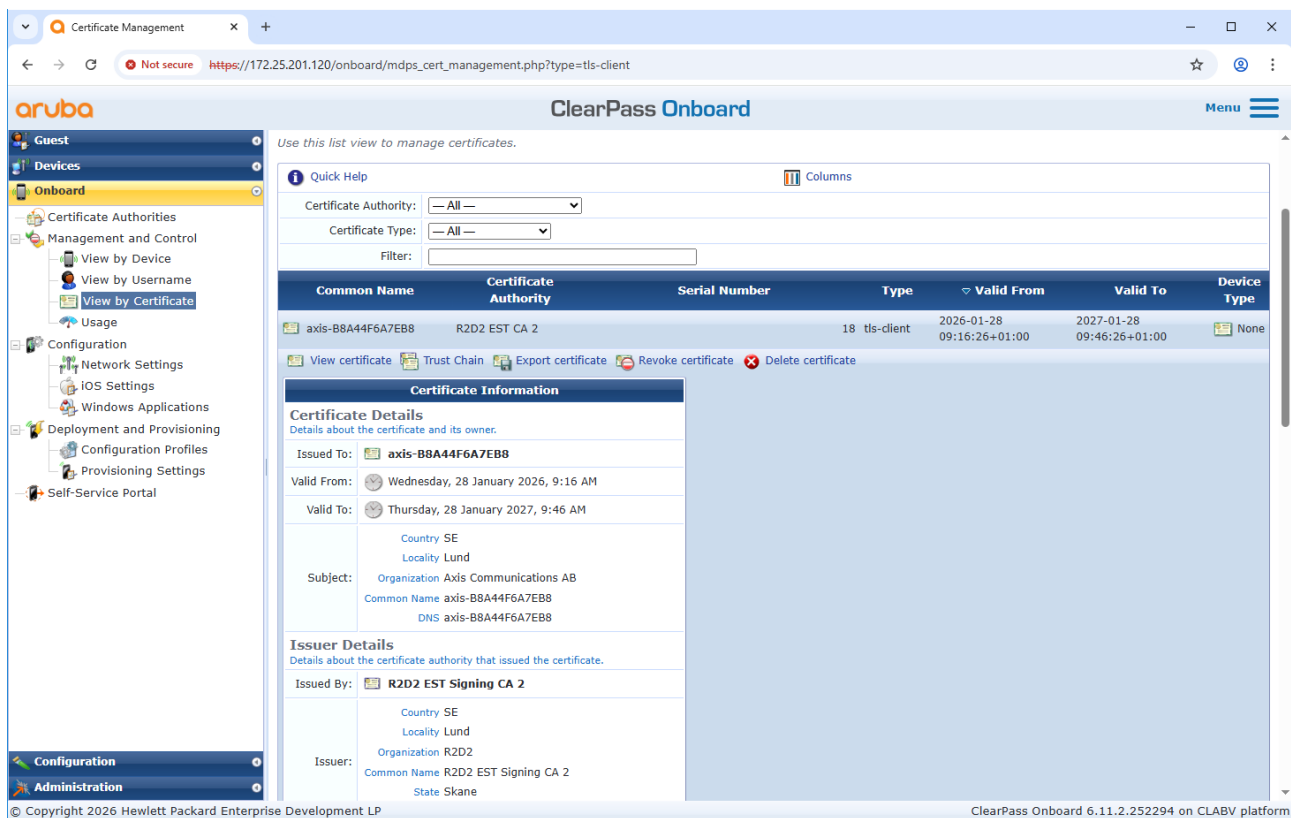
Die Registrierung wurde erfolgreich abgeschlossen.



Das per EST registrierte Zertifikat auf dem Axis Gerät.



Das registrierte Zertifikat wird automatisch dem zuvor ausgewählten Dienst zugewiesen.



Sie können das registrierte Zertifikat außerdem in ClearPass Onboard überprüfen.

Legacy-Onboarding – MAC-Authentifizierung

Sie können den MAC-Authentifizierungsbypass (MAB) nutzen, um Axis Geräte einzubinden, die das IEEE 802.1AR-Onboarding mit dem Axis Geräte-ID-Zertifikat und in der werkseitigen Standardeinstellung aktiviertem IEEE 802.1X nicht unterstützen. Wenn die 802.1X-Einbindung fehlschlägt, validiert ClearPass Policy Manager die MAC-Adresse des Axis Geräts und gewährt Zugriff auf das Netzwerk.

Für MAB sind sowohl Konfigurationsvorbereitungen für den Access Switch als auch für den ClearPass Policy Manager erforderlich. Das Axis Gerät muss nicht konfiguriert werden, um MAB für das Onboarding zu unterstützen.

HPE Aruba Networking ClearPass Policy Manager

Durchsetzungsrichtlinie

Die Durchsetzungsrichtlinienkonfiguration im ClearPass Policy Manager definiert anhand der folgenden zwei Beispiele für Richtlinienbedingungen, ob Axis Geräten Zugriff auf HPE Aruba-Netzwerke gewährt wird.

The screenshot displays the ClearPass Policy Manager web interface. The left sidebar contains navigation links: Dashboard, Monitoring, Configuration, and Administration. The 'Configuration' link is selected, leading to the 'Services - Axis 802.1X Wired - Mac Authentication' page. The 'Enforcement' tab is active, showing the 'Enforcement Policy' dropdown set to 'Axis MAC Authentication Policy'. Below this, the 'Enforcement Policy Details' section includes a description, default profile, and rules evaluation algorithm. A table lists conditions for enforcement profiles, such as 'Date:Day-of-Week' and 'Date:Time-of-Day'. The bottom of the interface shows a footer with copyright information and the version number.

Netzwerkzugriff verweigert

Wenn das Axis Gerät die konfigurierte Durchsetzungsrichtlinie nicht erfüllt, wird ihm der Zugriff auf das Netzwerk verweigert.

Gastnetzwerk (VLAN 203)

Dem Axis Gerät wird Zugriff auf ein begrenztes, isoliertes Netzwerk gewährt, wenn die folgenden Bedingungen erfüllt sind:

- Der Zugriff erfolgt an einem Wochentag von Montag bis Freitag.
- Der Zugriff erfolgt in einer Zeit zwischen 9:00 und 17:00 Uhr.
- Der mit der MAC-Adresse Hersteller ist Axis Communications.

Da es möglich ist, MAC-Adressen zu fälschen, wird der Zugriff auf das reguläre Bereitstellungsnetzwerk nicht gewährt. Wir empfehlen, dass Sie MAB nur für das erste Onboarding verwenden und das Gerät im Weiteren manuell überprüfen.

Quellenkonfiguration

Auf der Seite **Sources (Quellen)** wird eine neue Authentifizierungsquelle erstellt, um nur manuell importierte MAC Adressen zuzulassen.

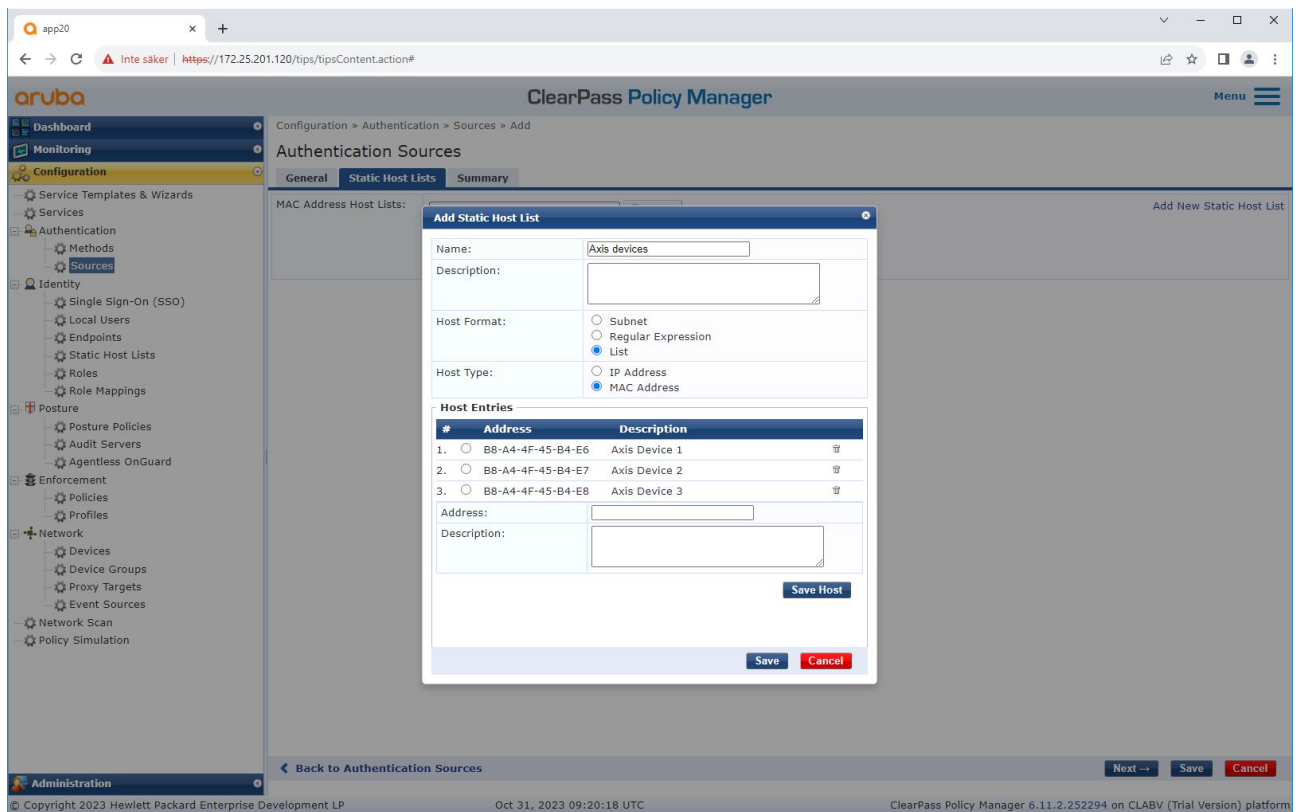
The screenshot displays the ClearPass Policy Manager web interface. The left sidebar shows the navigation menu with 'Configuration' selected. The main content area is titled 'Authentication Sources' and shows a list of existing sources. Below the list, the 'Add' button is visible. The bottom section shows the 'Add' form for a new source, with fields for Name, Description, Type, and Authorization Sources.

Authentication Sources List:

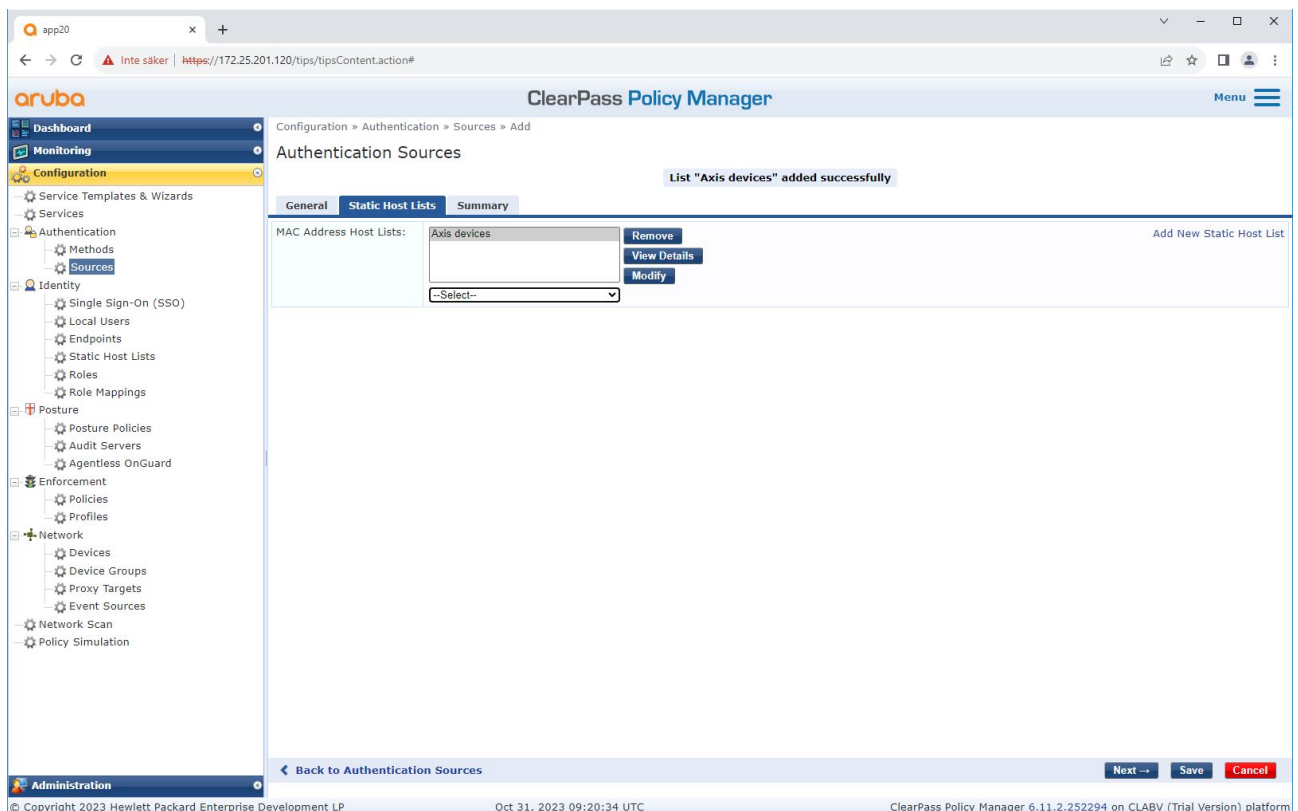
#	Name	Type	Description
1.	[Admin User Repository]	Local SQL DB	Authenticate users against Policy Manager admin user database
2.	[Denylist User Repository]	Local SQL DB	Denylist database with users who have exceeded bandwidth or session related limits
3.	[Endpoints Repository]	Local SQL DB	Authenticate endpoints against Policy Manager local database
4.	[Guest Device Repository]	Local SQL DB	Authenticate guest devices against Policy Manager local database
5.	[Guest User Repository]	Local SQL DB	Authenticate guest users against Policy Manager local database
6.	[Insight Repository]	Local SQL DB	Insight database with session information for users and devices
7.	[Local User Repository]	Local SQL DB	Authenticate users against Policy Manager local user database
8.	[Onboard Devices Repository]	Local SQL DB	Authenticate Onboard devices against Policy Manager local database
9.	[Social Login Repository]	Local SQL DB	Authenticate users against Policy Manager social login database
10.	[Time Source]	Local SQL DB	Authorization source for implementing various time functions
11.	[Zone Cache Repository]	HTTP	Access attributes cached by Context Server Actions in previous sessions

Add Authentication Source Form:

Name: Axis Devices
Description: MAC addresses of Axis devices in use.
Type: Static Host List
Use for Authorization: ☐ Enable to use this Authentication Source to also fetch role mapping attributes
Authorization Sources:



Eine statische Hostliste mit dem Axis MAC-Adressen wird erstellt.



Servicekonfiguration

Auf der Seite **Services** werden die Konfigurationsschritte in einem Dienst zusammengefasst, der die Authentifizierung und Autorisierung von Axis Geräten in HPE Aruba Networking-Netzwerken übernimmt.

app20 x +

Inte saker | <https://172.25.201.120/tips/tipsContent.action#tipsServices.action>

aruba ClearPass Policy Manager Menu

Configuration » Services

Services

This page shows the current list and order of services that ClearPass follows during authentication and authorization.

Filter: Name contains Go Clear Filter Hit Count for Current hour Show 20 records

#	Order	Name	Type	Template	Hit Count	Status	
1.	☐	1	Axis 802.1X Wired	RADIUS	802.1X Wired	0	✓
2.	☐	2	Axis 802.1X Wired - Mac Authentication	RADIUS	MAC Authentication	0	✓
3.	☐	3	Test_Service	RADIUS	802.1X Wired	0	✗
4.	☐	4	[Policy Manager Admin Network Login Service]	TACACS+	TACACS+ Enforcement	0	✗
5.	☐	5	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	0	✗
6.	☐	6	[Aruba Device Access Service]	TACACS+	TACACS+ Enforcement	0	✗
7.	☐	7	[Guest Operator Logins]	Application	Aruba Application Authentication	0	✗
8.	☐	8	[Insight Operator Logins]	Application	Aruba Application Authentication	0	✗
9.	☐	9	[Device Registration Disconnect]	WEBAUTH	Web-based Authentication	0	✗

Showing 1-9 of 9

Reorder Copy Export Delete

Copyright 2023 Hewlett Packard Enterprise Development LP Oct 26, 2023 05:34:53 UTC ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform

app20 x +

Inte saker | <https://172.25.201.120/tips/tipsContent.action#tipsEditService.action%3FcontextData%3D3006>

aruba ClearPass Policy Manager Menu

Configuration » Services » Edit - Axis 802.1X Wired - Mac Authentication

Services - Axis 802.1X Wired - Mac Authentication

Summary Service Authentication Roles Enforcement

Name: Axis 802.1X Wired - Mac Authentication

Description: To authenticate guest devices based on their MAC address.

Type: MAC Authentication

Status: Disabled

Monitor Mode: ☐ Enable to monitor network access without enforcement

More Options: ☐ Authorization ☐ Audit End-hosts ☐ Profile Endpoints ☐ Accounting Proxy

Service Rule

Matches ANY or ALL of the following conditions:

Type	Name	Operator	Value
1. Radius:IETF	NAS-Port-Type	BELONGS_TO	Ethernet (15)
2. Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Call-Check (10)
3. Connection	Client-Mac-Address	EQUALS	%{Radius:IETF:User-Name}
4.	Click to add...		

Back to Services

Enable Copy Save Cancel

Copyright 2023 Hewlett Packard Enterprise Development LP Oct 26, 2023 05:15:11 UTC ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform

Es wird ein dedizierter Axis Dienst erstellt, der MAB als Verbindungsmethode definiert.

The screenshot shows the 'ClearPass Policy Manager' web interface. The left sidebar contains navigation menus for Dashboard, Monitoring, Configuration, and Administration. The main content area is titled 'Services - Axis 802.1X Wired - Mac Authentication' and has tabs for Summary, Service, Authentication, Roles, and Enforcement. The 'Authentication' tab is active, showing 'Authentication Methods' with '[Allow All MAC AUTH]' and 'Authentication Sources' with 'Axis Devices [Static Host List]'. There are buttons for 'Move Up', 'Move Down', 'Remove', 'View Details', and 'Modify' for both methods and sources. A 'Strip Username Rules' section has a checkbox for 'Enable to specify a comma-separated list of rules to strip username prefixes or suffixes'. At the bottom, there are buttons for 'Back to Services', 'Disable', 'Copy', 'Save', and 'Cancel'. The footer shows copyright information and the platform version.

Die vorkonfigurierte MAC-Authentifizierungsmethode wird für den Dienst konfiguriert. Darüber hinaus wird die zuvor erstellte Authentifizierungsquelle mit einer Liste der Axis MAC-Adressen ausgewählt.

Axis Communications verwendet die folgenden MAC Adressen-OUIs:

- B8:A4:4F:XX:XX:XX
- AA:C8:3E:XX:XX:XX
- 00:40:8C:XX:XX:XX

The screenshot shows the 'ClearPass Policy Manager' web interface, specifically the 'Enforcement' tab for 'Services - Axis 802.1X Wired - Mac Authentication'. The 'Use Cached Results' checkbox is unchecked. The 'Enforcement Policy' is set to 'Axis MAC Authentication Policy'. The 'Enforcement Policy Details' section shows a description, default profile, and rules evaluation algorithm. A table lists conditions and enforcement profiles. The conditions include a date range and a connection type. The enforcement profile is 'Allow_VLAN_203'. At the bottom, there are buttons for 'Back to Services', 'Enable', 'Copy', 'Save', and 'Cancel'. The footer shows copyright information and the platform version.

Im letzten Schritt wird die zuvor erstellte Durchsetzungsrichtlinie für den Dienst konfiguriert.

HPE Aruba Networking Zugangsschalter

Zusätzlich zur sicheren Onboarding-Konfiguration, die in *HPE Aruba Networking Zugangsschalter, on page 15* beschrieben wird, finden Sie weitere Informationen in der folgenden Beispiel-Portkonfiguration des HPE Aruba Networking-Zugangsschalters zur Unterstützung von MAB.

```
aaa port-access authenticator 18 tx-period 5aaa port-access authenticator 19 tx-period 5aaa
port-access authenticator 18 max-requests 3aaa port-access authenticator 19 max-requests 3aaa
port-access authenticator 18 client-limit 1aaa port-access authenticator 19 client-limit 1aaa
port-access mac-based 18-19aaa port-access 18 auth-order authenticator mac-basedaaa port-
access 19 auth-order authenticator mac-basedaaa port-access 18 auth-priority authenticator
mac-basedaaa port-access 19 auth-priority authenticator mac-based
```


T10197992_de

2026-02 (M8.3)

© 2023 – 2026 Axis Communications AB