

Secure integration of Axis devices into Aruba networks

Secure integration of Axis devices into Aruba networks

Inhalt

Einführung	3
Sicheres Onboarding – IEEE 802.1AR/802.1X	4
Erstauthentifizierung	4
Bereitstellung	4
Produktionsnetzwerk	4
Konfiguration von HPE Aruba	5
Konfiguration Axis	17
Sicherer Netzwerkbetrieb – IEEE 802.1AE MACsec	20
Aruba ClearPass Policy Manager	20
Aruba-Zugangsschalter	25
Legacy-Onboarding – MAC-Authentifizierung	26
Aruba ClearPass Policy Manager	26
Aruba-Zugangsschalter	34

Secure integration of Axis devices into Aruba networks

Einführung

Einführung

Dieser Integrationsleitfaden soll die Best-Practice-Konfiguration für die Einbindung und den Betrieb von Axis Geräten in Aruba-Netzwerken skizzieren. 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 Zeit und Geld sparen. Es ermöglicht die Beseitigung unnötiger Systemkomplexität bei der Verwendung von Anwendungen zur Verwaltung von Axis Geräten in Kombination mit Aruba-Netzwerkgeräten und -Anwendungen. Im Folgenden sind nur einige Vorteile aufgeführt, die durch die Kombination von Axis Geräten und Software mit einer Aruba-Netzwerkinfrastruktur erzielt werden können:

- Minimieren Sie die Systemkomplexität, indem Sie Netzwerke zur Bereitstellung von Geräten entfernen.
- Sparen Sie Kosten, indem Sie Einbindungsprozesse und Geräteverwaltung automatisieren.
- Profitieren Sie von den Zero-Touch-Netzwerksicherheitskontrollen der Axis Geräte.
- Erhöhen Sie die allgemeine Netzwerk-Sicherheit durch den Einsatz des Fachwissens von Aruba und Axis.

Die Netzwerkinfrastruktur muss darauf vorbereitet sein, die Integrität der Axis Geräte sicher zu überprüfen, bevor mit der Konfiguration begonnen wird. Dies ermöglicht einen reibungslosen softwaredefinierten Übergang zwischen logischen Netzwerken während des gesamten Onboarding-Prozesses. Vor der Konfiguration sind Kenntnisse in den folgenden Bereichen erforderlich:

- Verwaltung der IT-Infrastruktur des Aruba-Unternehmensnetzwerks, einschließlich Aruba Access Switches und Aruba ClearPass Policy Manager.
- Fachkenntnisse in modernen Netzwerkzugriffskontrolltechniken und Netzwerk-Sicherheitsrichtlinien.
- Grundkenntnisse über Axis Produkte sind wünschenswert, werden aber im gesamten Handbuch vermittelt.

Secure integration of Axis devices into Aruba networks

Sicheres Onboarding – IEEE 802.1AR/802.1X

Sicheres Onboarding – IEEE 802.1AR/802.1X

Erstauthentifizierung

Schließen Sie das von Axis Edge Vault unterstützte Axis Gerät an, um das Gerät gegenüber dem Aruba-Netzwerk zu authentifizieren. Das Gerät verwendet das Axis Geräte-ID-Zertifikat IEEE 802.1AR über die Netzwerkzugriffskontrolle IEEE 802.1X, um sich zu authentifizieren.

Um Zugriff auf das Netzwerk zu gewähren, überprüft der Aruba ClearPass Policy Manager die Axis Geräte-ID zusammen mit anderen gerätespezifischen Fingerabdrücken. Die Informationen, wie MAC Adresse und laufende Firmware, werden verwendet, um eine richtlinienbasierte Entscheidung zu treffen.

Das Axis Gerät authentifiziert sich beim Aruba-Netzwerk mithilfe des IEEE 802.1AR-kompatiblen Axis Geräte-ID-Zertifikats.

Das Axis Gerät authentifiziert sich beim Aruba-Netzwerk mithilfe des IEEE 802.1AR-kompatiblen 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 verschiebt das Aruba-Netzwerk das Axis Gerät in das Bereitstellungsnetzwerk (VLAN201), in dem Axis Device Manager installiert ist. Über den Axis Device Manager können Gerätekonfiguration, Sicherheitshärtung und Firmware-Updates durchgeführt werden. 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 Aruba ClearPass Policy Manager überprüft die neuen Zertifikate und entscheidet, ob das Axis Gerät in das Produktionsnetzwerk verschoben wird oder nicht.

Nach der Gerätekonfiguration verlässt das Axis Gerät das Bereitstellungsnetzwerk und versucht, sich erneut beim Aruba-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. In diesem Netzwerk stellt das Video Management System (VMS) eine Verbindung zum Axis Gerät her und nimmt den Betrieb auf.

Secure integration of Axis devices into Aruba networks

Sicheres Onboarding – IEEE 802.1AR/802.1X

Dem Axis Gerät wird Zugriff auf das Produktionsnetzwerk gewährt.

- 1 Zugangsschalter
- 2 Produktionsnetzwerk
- 3 ClearPass Policy Manager
- 4 Video Management System

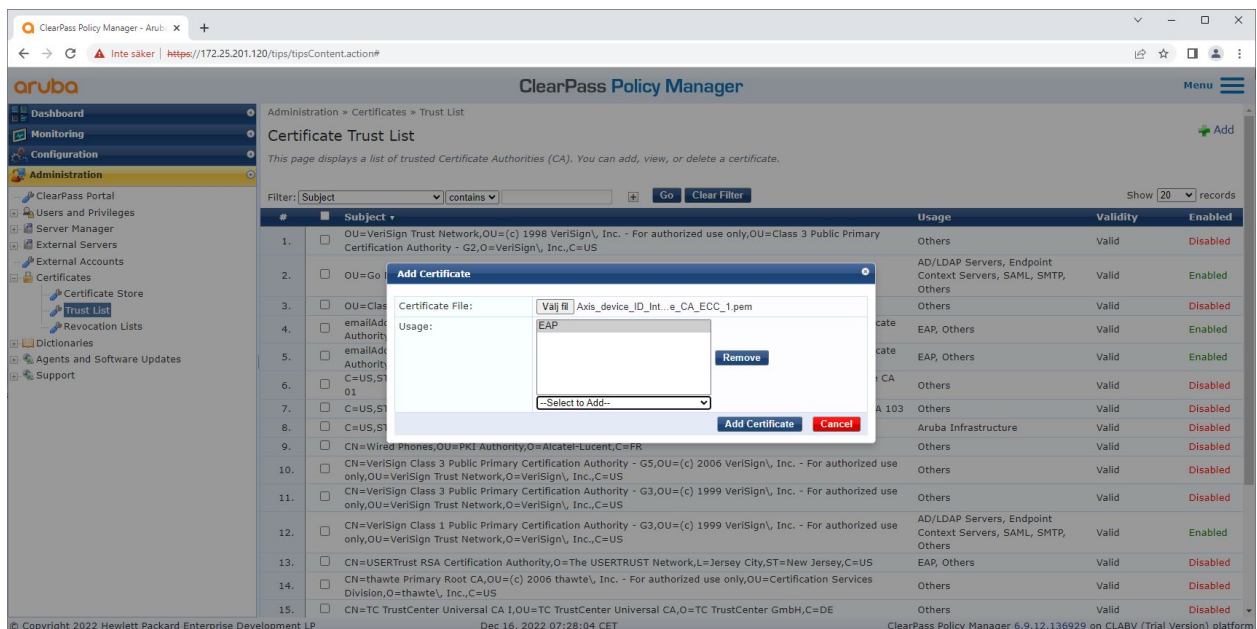
Konfiguration von HPE Aruba

Aruba ClearPass Policy Manager

Der ClearPass Policy Manager von Aruba bietet rollen- und gerätebasierte sichere Netzwerkzugriffskontrolle für IoT, BYOD, Unternehmensgeräte, Mitarbeiter, Auftragnehmer und Gäste in der kabelgebundenen, kabellosen und VPN-Infrastruktur mehrerer Anbieter.

Konfiguration des vertrauenswürdigen Zertifikatspeichers

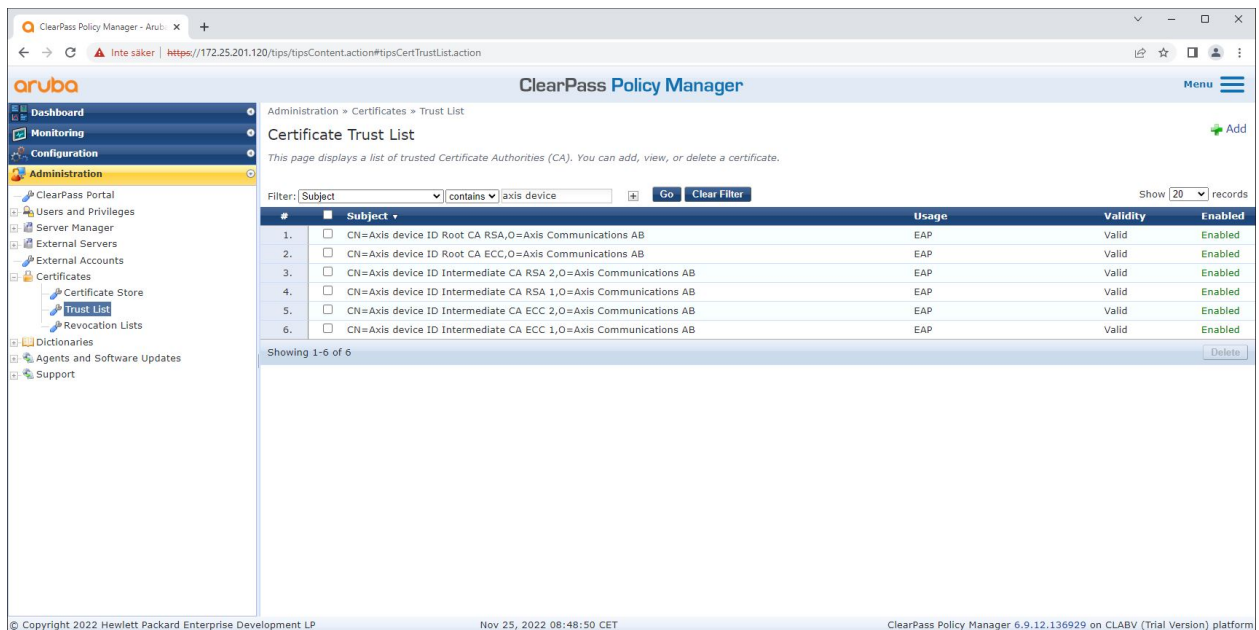
1. Laden Sie die Axis spezifische IEEE 802.1AR-Zertifikatskette von axis.com herunter.
2. Laden Sie die Axis spezifischen IEEE 802.1AR-Root-CA- und Intermediate-CA-Zertifikatsketten in den vertrauenswürdigen Zertifikatspeicher hoch.
3. Aktivieren Sie den Aruba ClearPass Policy Manager zur Authentifizierung 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.



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

Secure integration of Axis devices into Aruba networks

Sicheres Onboarding – IEEE 802.1AR/802.1X



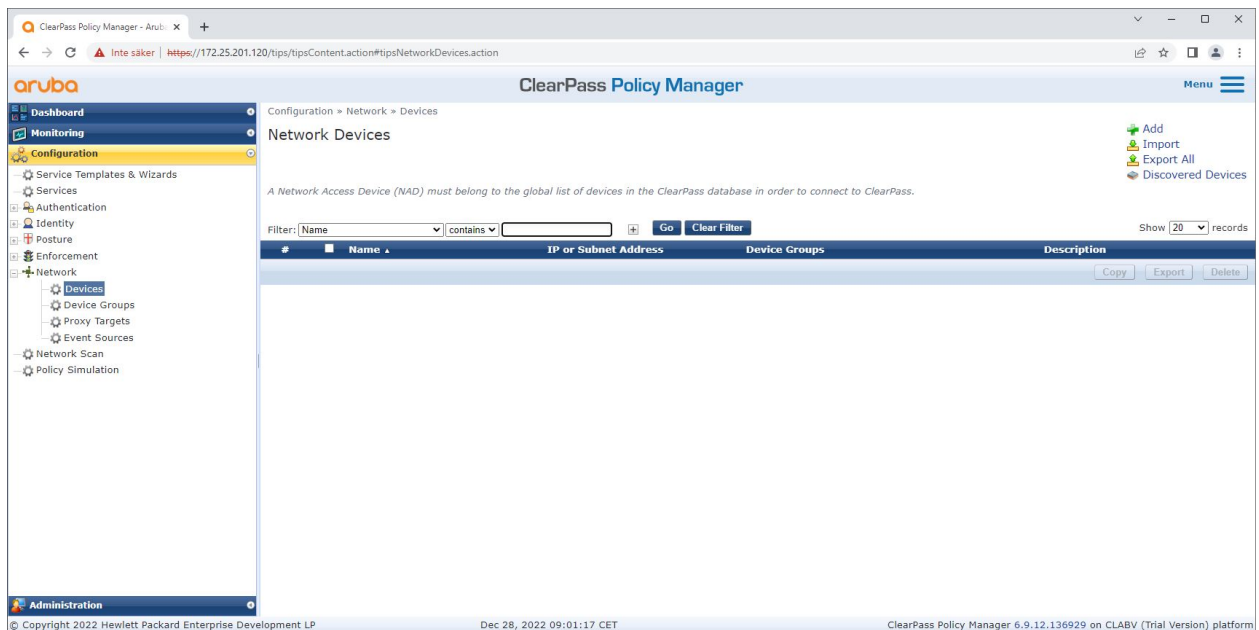
Der vertrauenswürdige Zertifikatsspeicher im Aruba ClearPass Policy Manager mit für Axis spezifischer IEEE 802.1AR-Zertifikatskette.

Netzwerkgeräte-/Gruppenkonfiguration

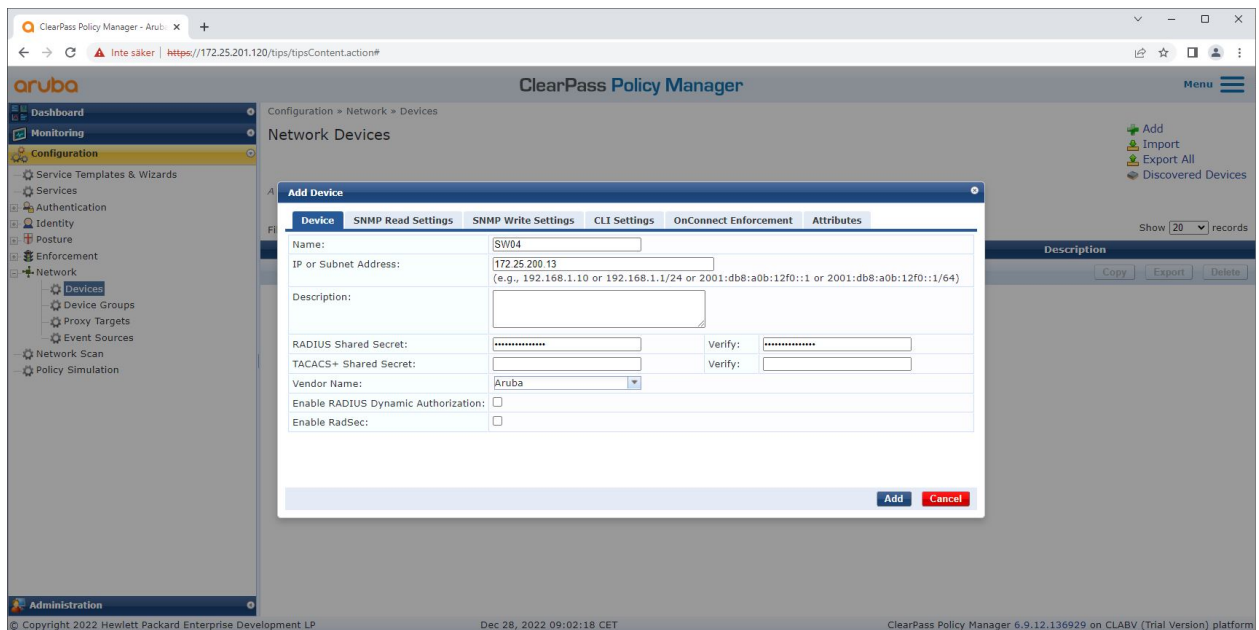
1. Fügen Sie dem ClearPass Policy Manager vertrauenswürdige Netzwerkzugriffsgeräte wie Aruba Access Switches hinzu. Der ClearPass Policy Manager muss wissen, welche Aruba Access Switches im Netzwerk für die IEEE 802.1X-Kommunikation verwendet werden.
2. Verwenden Sie die Netzwerkgerätegruppenkonfiguration, um mehrere vertrauenswürdige Netzwerkzugriffsgeräte zu gruppieren. Das Gruppieren vertrauenswürdiger Netzwerkzugriffsgeräte ermöglicht eine einfachere Richtlinienkonfiguration.
3. Das gemeinsame RADIUS-Geheimnis muss mit der spezifischen IEEE 802.1X-Konfiguration des Switches übereinstimmen.

Secure integration of Axis devices into Aruba networks

Sicheres Onboarding – IEEE 802.1AR/802.1X



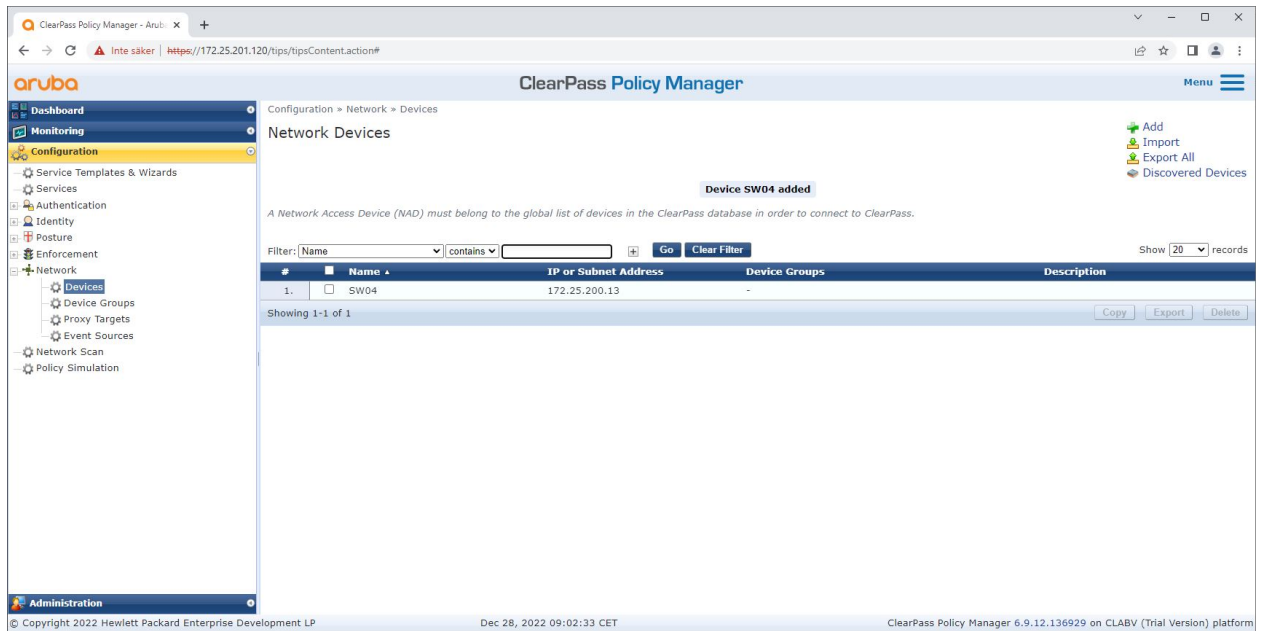
Die Schnittstelle für vertrauenswürdige Netzwerkgeräte im Aruba ClearPass Policy Manager.



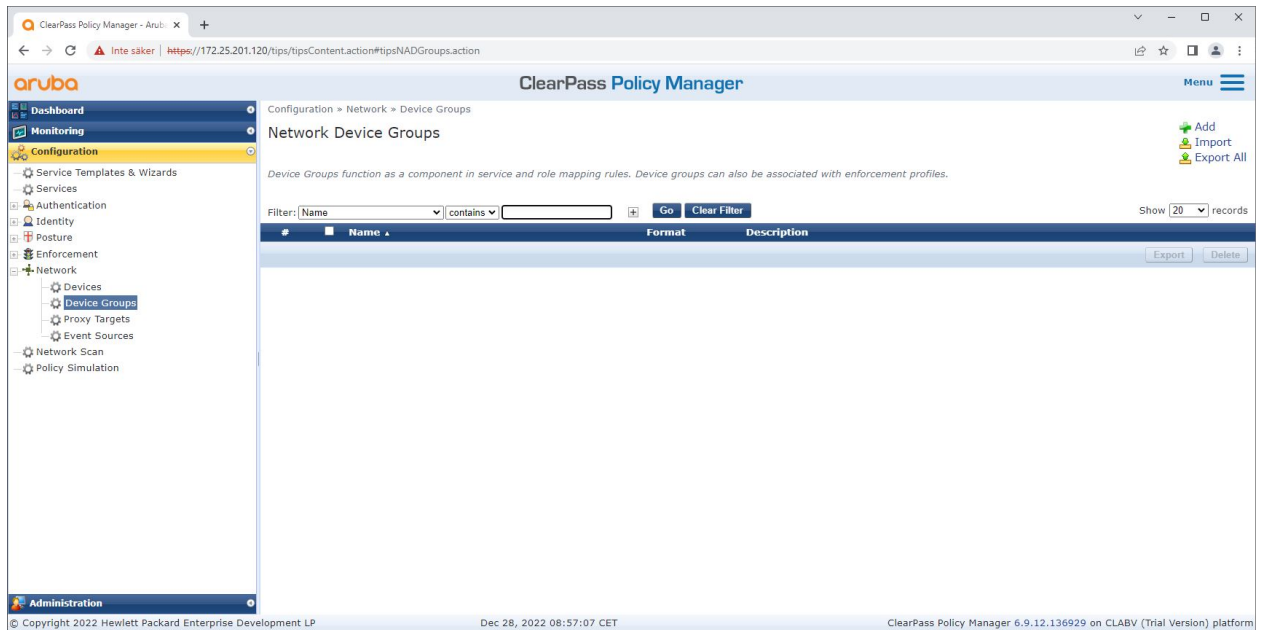
Hinzufügen des Aruba Access Switch als vertrauenswürdiges Netzwerkgerät im Aruba ClearPass Policy Manager. Bitte beachten Sie, dass das gemeinsame RADIUS-Geheimnis mit der spezifischen IEEE 802.1X-Konfiguration des Switches übereinstimmen muss.

Secure integration of Axis devices into Aruba networks

Sicheres Onboarding – IEEE 802.1AR/802.1X



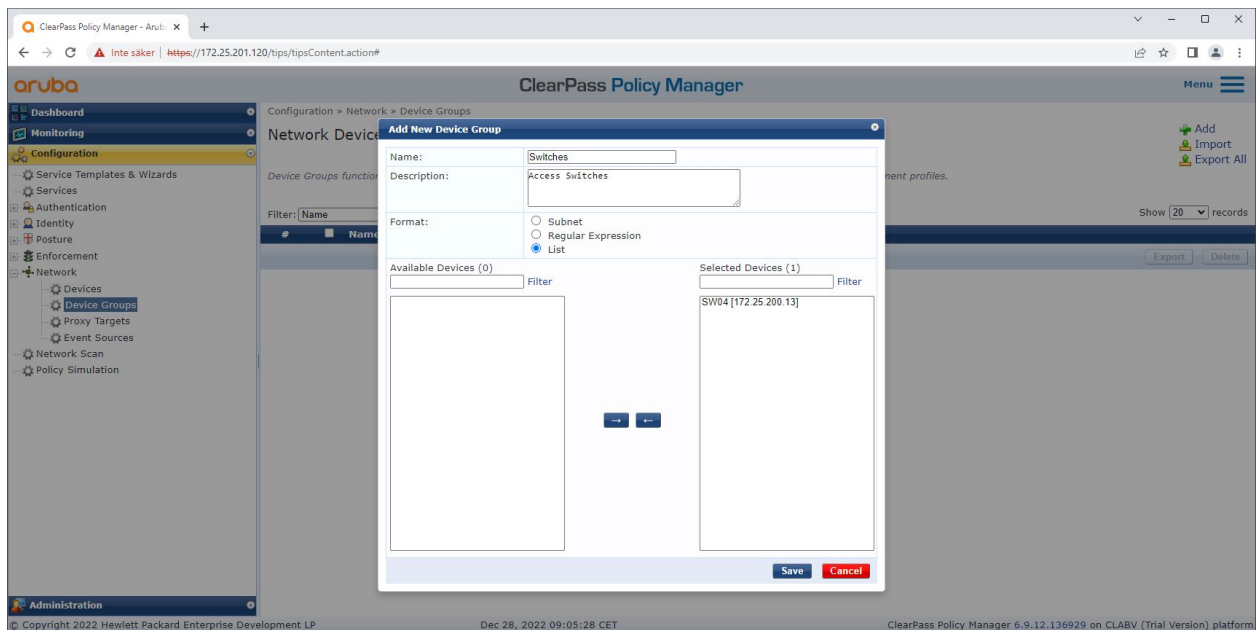
Der Aruba ClearPass Policy Manager mit einem konfigurierten vertrauenswürdigen Netzwerkgerät.



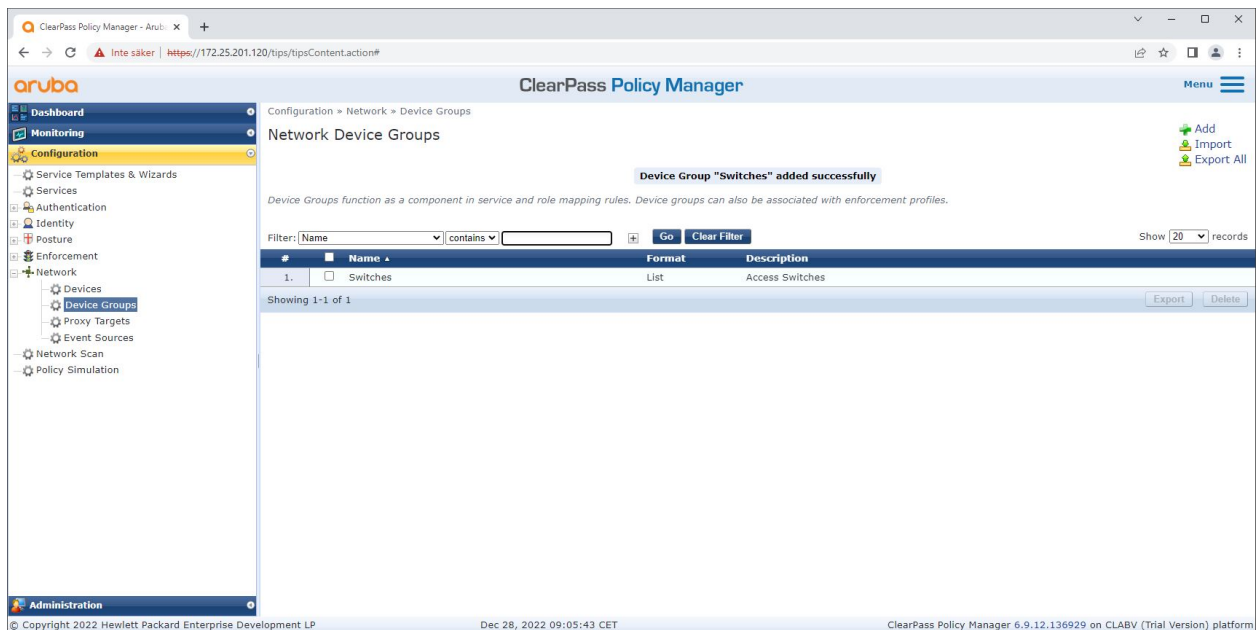
Die Schnittstelle für vertrauenswürdige Netzwerkgerätegruppen im Aruba ClearPass Policy Manager.

Secure integration of Axis devices into Aruba networks

Sicheres Onboarding – IEEE 802.1AR/802.1X



Hinzufügen eines vertrauenswürdigen Netzwerkzugriffsgärts zu einer neuen Gerätgruppe im Aruba ClearPass Policy Manager.



Der Aruba ClearPass Policy Manager mit konfigurierter Netzwerkgerätgruppe, die ein oder mehrere vertrauenswürdige Netzwerkgeräte umfasst.

Konfiguration des Gerätefingerabdrucks

Das Axis Gerät kann gerätespezifische Informationen wie MAC Adresse und Firmware-Version über Netzwerkerkennung weiterleiten. Ein Gerätefingerabdruck kann über die Benutzeroberfläche für Gerätefingerabdrücke im Aruba ClearPass Policy Manager erstellt werden. Es ist möglich, den Gerätefingerabdruck zu aktualisieren und zu verwalten. Je nach AXIS OS Version kann unter anderem der Zugriff gewährt oder verweigert werden.

Secure integration of Axis devices into Aruba networks

Sicheres Onboarding – IEEE 802.1AR/802.1X

Es ist möglich, den Gerätefingerabdruck zu aktualisieren und zu verwalten. Je nach AXIS OS Version kann unter anderem der Zugriff gewährt oder verweigert werden.

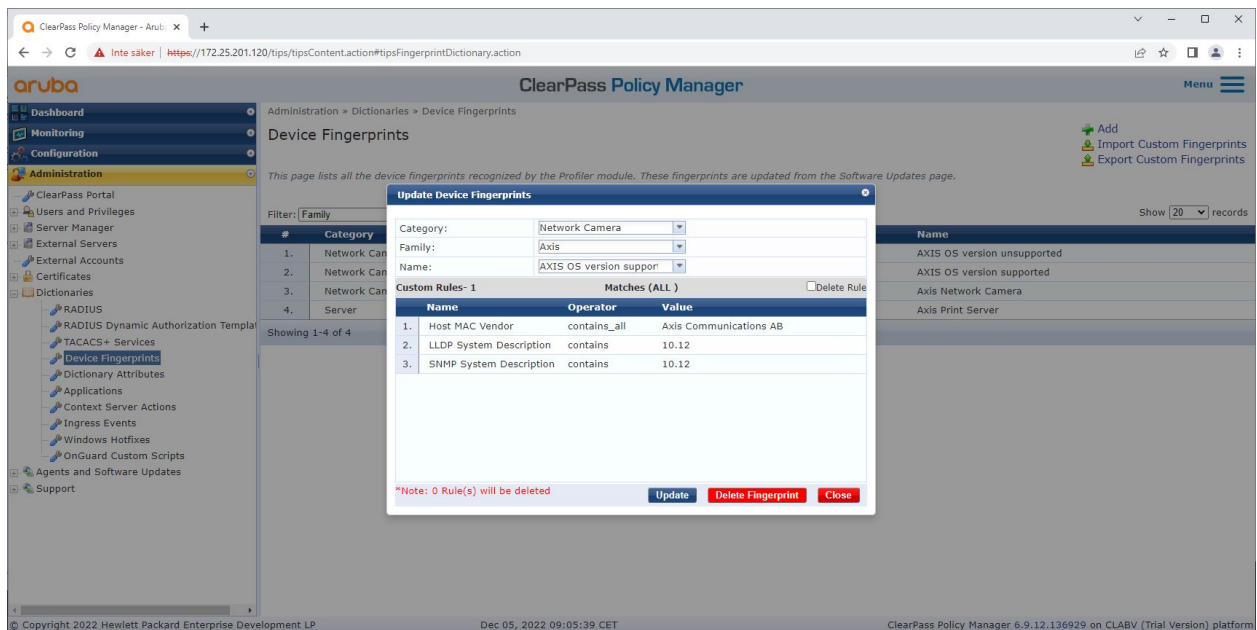
1. Gehen Sie zu Administration > Dictionaries > Device Fingerprints (Verwaltung > Wörterbücher > Gerätefingerabdrücke).
2. Wählen Sie einen vorhandenen Gerätefingerabdruck aus oder erstellen Sie einen neuen Gerätefingerabdruck.
3. Legen Sie die Einstellungen für den Gerätefingerabdruck fest.

The screenshot shows the Aruba ClearPass Policy Manager interface. The main window displays the 'Device Fingerprints' configuration page. A modal dialog box titled 'Update Device Fingerprints' is open, showing configuration options for a device fingerprint. The dialog box includes fields for Category (Network Camera), Family (Axis), and Name (AXIS OS version unsupp). Below these fields is a table of custom rules with columns for Name, Operator, and Value. The table shows three rules: 1. Host MAC Vendor (contains_all, Axis Communications AB), 2. LLDP System Description (not_contains, 10.12), and 3. SNMP System Description (not_contains, 10.12). The dialog box also has buttons for Update, Delete Fingerprint, and Close. A note at the bottom of the dialog box states: '*Note: 0 Rule(s) will be deleted'.

Die Konfiguration des Gerätefingerabdrucks im Aruba ClearPass Policy Manager. Axis Geräte mit einer anderen Firmware-Version als 10.12 gelten als nicht unterstützt.

Secure integration of Axis devices into Aruba networks

Sicheres Onboarding – IEEE 802.1AR/802.1X



Die Konfiguration des Gerätefingerabdrucks im Aruba ClearPass Policy Manager. Axis Geräte mit Firmware 10.12 gelten im obigen Beispiel als unterstützt.

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

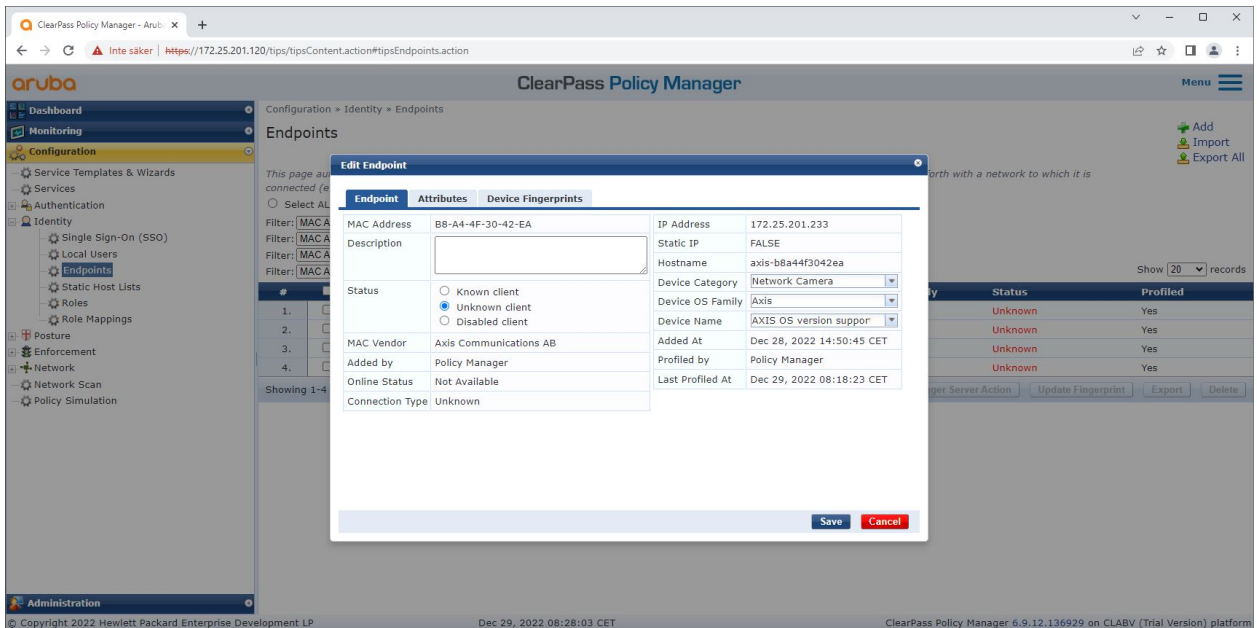
1. Gehen Sie zu **Configuration > Identity > Endpoints (Konfiguration > Identität > Endpunkte)**.
2. Wählen Sie das Gerät, das Sie ansehen möchten.
3. Klicken Sie auf die Registerkarte Gerätefingerabdrücke.

Hinweis

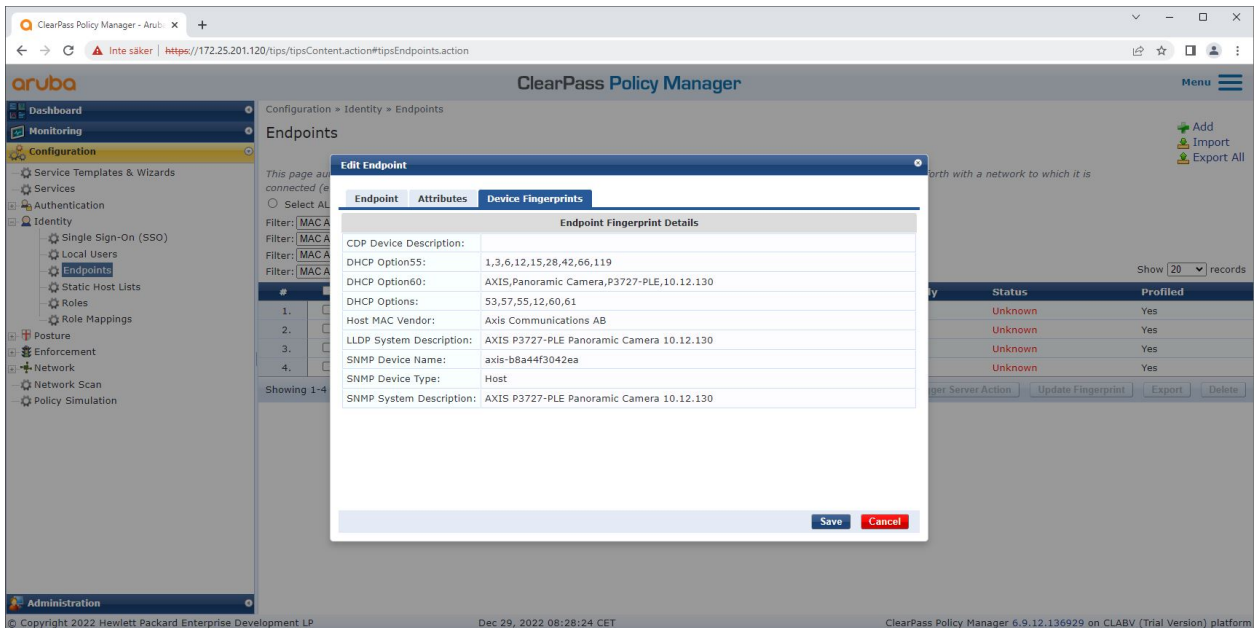
SNMP ist in Axis Geräten standardmäßig deaktiviert und wird vom Aruba-Zugangsschalter erfasst.

Secure integration of Axis devices into Aruba networks

Sicheres Onboarding – IEEE 802.1AR/802.1X



Ein Axis Gerät, das vom Aruba ClearPass Policy Manager profiliert wurde.



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 im werkseitigen Standardzustand gemeinsam genutzt und vom Aruba-Zugriffsschalter an den ClearPass Policy Manager weitergeleitet.

Konfiguration des Durchsetzungsprofils

Das Durchsetzungsprofil wird verwendet, um dem Aruba ClearPass Policy Manager zu ermöglichen, einem Zugriffsport am Switch eine bestimmte VLAN-ID zuzuweisen. Es handelt sich um eine richtlinienbasierte Entscheidung, die für die Netzwerkgeräte in der Gerätegruppe „Switches“ gilt. Die erforderliche Anzahl an Durchsetzungsprofilen hängt von der Anzahl der verwendeten VLANs ab. In unserem Setup gibt es insgesamt drei VLANs (VLAN 201, 202, 203), die drei Durchsetzungsprofilen entsprechen.

Secure integration of Axis devices into Aruba networks

Sicheres Onboarding – IEEE 802.1AR/802.1X

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

The screenshot shows the 'ClearPass Policy Manager' interface. The left sidebar contains navigation options: Dashboard, Monitoring, Configuration, and Administration. The 'Configuration' menu is expanded, showing 'Enforcement' > 'Profiles'. The main content area displays the configuration for 'Enforcement Profiles - Allow_VLAN_201'. The 'Profile' tab is active, showing the following details:

- Name: Allow_VLAN_201
- Description:
- Type: RADIUS
- Action: Accept
- Device Group List: 1. Switches

Below the profile details is a table of attributes:

Type	Name	Value
Radius:IETF	Session-Timeout	= 10800
Radius:IETF	Termination-Action	= RADIUS-Request (1)
Radius:IETF	Tunnel-Type	= VLAN (13)
Radius:IETF	Tunnel-Medium-Type	= IEEE-802 (6)
Radius:IETF	Tunnel-Private-Group-Id	= 201

At the bottom of the configuration page, there are buttons for 'Copy', 'Save', and 'Cancel', and a 'Back to Enforcement Profiles' link.

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

The screenshot shows the 'ClearPass Policy Manager' interface. The left sidebar contains navigation options: Dashboard, Monitoring, Configuration, and Administration. The 'Configuration' menu is expanded, showing 'Enforcement' > 'Policies'. The main content area displays the configuration for 'Enforcement Policies - Axis Radius policy'. The 'Rules' tab is active, showing the following details:

- Name: Axis Radius policy
- Description:
- Enforcement Type: RADIUS
- Default Profile: Allow_VLAN_203
- Rules Evaluation Algorithm: First applicable

Below the policy details is a table of rules with conditions and actions:

Conditions	Actions
1. (Certificate:Issuer-CN CONTAINS Axis device ID Intermediate CA) AND (Certificate:Issuer-O EQUALS Axis Communications AB) AND (Certificate:Subject-O EQUALS Axis Communications AB) AND (Certificate:Subject-L EQUALS Lund) AND (Certificate:Subject-C EQUALS SE) AND (Connection:Client-Mac-Address-NoDelim EQUALS %(Certificate:Subject-serialNumber))	Allow_VLAN_201
2. (Certificate:Issuer-CN CONTAINS Production CA Certificate) AND (Certificate:Subject-CN CONTAINS %(Connection:Client-Mac-Address-NoDelim)) AND (Authorization:[Endpoints Repository]:Device Name EQUALS AXIS OS version unsupported)	Allow_VLAN_201
3. (Certificate:Issuer-CN CONTAINS Production CA certificate) AND (Certificate:Subject-CN CONTAINS %(Connection:Client-Mac-Address-NoDelim)) AND (Authorization:[Endpoints Repository]:Device Name EQUALS AXIS OS version supported)	Allow_VLAN_202

At the bottom of the configuration page, there are buttons for 'Copy', 'Save', and 'Cancel', and a 'Back to Enforcement Policies' link.

Die Konfiguration für die Durchsetzungsrichtlinie im Aruba ClearPass Policy Manager.

Die vier Durchsetzungsrichtlinien und ihre Maßnahmen sind unten aufgeführt:

Netzwerkzugriff verweigert

Secure integration of Axis devices into Aruba networks

Sicheres Onboarding – IEEE 802.1AR/802.1X

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

Gastnetzwerk (VLAN 203)

Dem Axis Gerät wird Zugriff auf ein begrenztes, isoliertes Netzwerk gewährt, wenn die IEEE 802.1X-Authentifizierung der Netzwerkzugriffskontrolle fehlschlägt. Um entsprechende Maßnahmen ergreifen zu können, ist eine manuelle Inspektion des Geräts erforderlich.

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 Firmware-Updates, Produktionszertifikaten und anderen Konfigurationen zu konfigurieren. Die folgenden Bedingungen werden vom Aruba ClearPass Policy Manager überprüft:

- Die Firmware-Version des Axis Geräts.
- Die MAC Adresse des Geräts stimmt mit dem herstellerspezifischen Axis MAC Adressen-Schema mit dem Seriennummernattribut des Axis Geräte-ID-Zertifikats 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 Zugriff auf das Produktionsnetzwerk gewährt, in dem das Axis Gerät betrieben wird. Der Zugriff wird gewährt, nachdem die Gerätebereitstellung innerhalb des Bereitstellungsnetzwerks (VLAN 201) abgeschlossen ist. Die folgenden Bedingungen werden vom Aruba ClearPass Policy Manager überprüft:

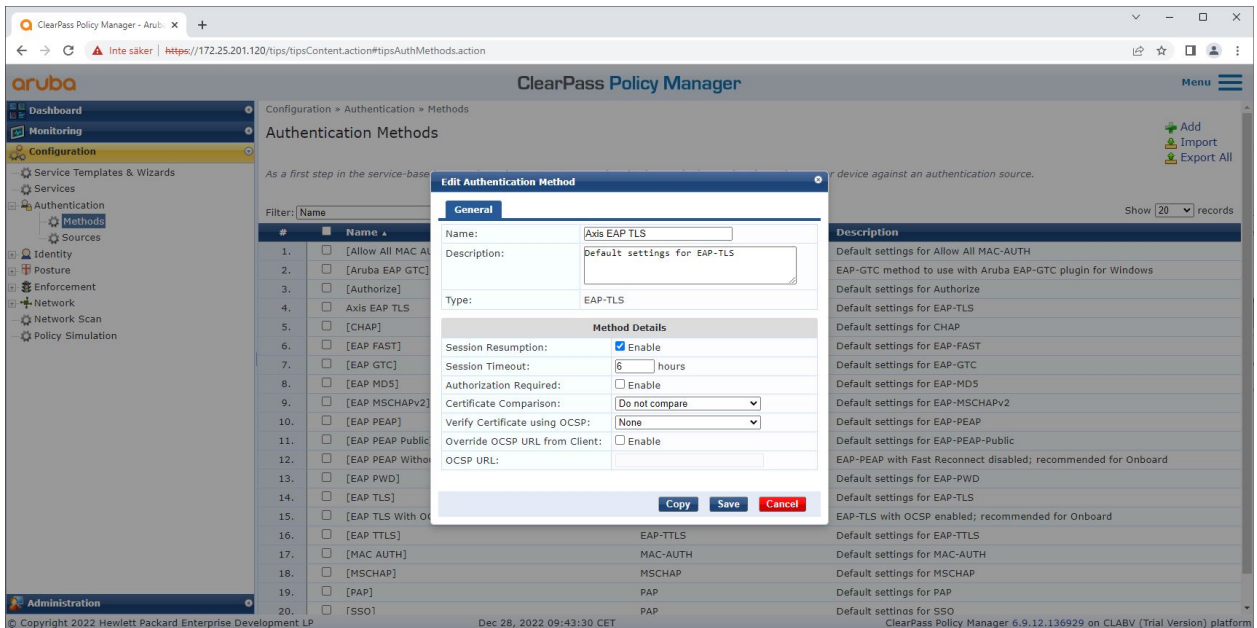
- Die MAC Adresse des Geräts stimmt mit dem herstellerspezifischen Axis MAC Adressen-Schema mit dem Seriennummernattribut des Axis Geräte-ID-Zertifikats überein.
- Die Firmware-Version des Axis Geräts.
- Das Produktionszertifikat kann vom vertrauenswürdigen Zertifikatsspeicher überprüft werden.

Konfiguration der Authentifizierungsmethode

In der Authentifizierungsmethode wird definiert, wie ein Axis Gerät versucht, sich gegenüber dem Aruba-Netzwerk zu authentifizieren. Die bevorzugte Authentifizierungsmethode sollte IEEE 802.1X EAP-TLS sein, da bei Axis Geräten mit Unterstützung für Axis Edge Vault standardmäßig IEEE 802.1X EAP-TLS aktiviert ist.

Secure integration of Axis devices into Aruba networks

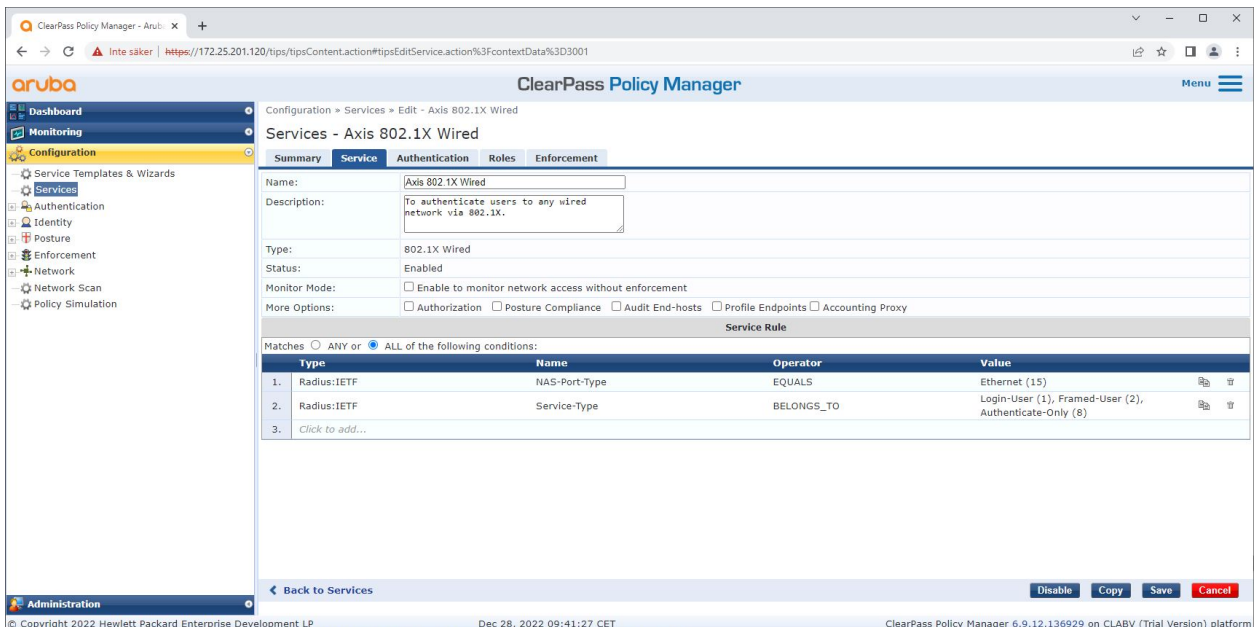
Sicheres Onboarding – IEEE 802.1X/802.1X



Die Authentifizierungsmethoden-Schnittstelle des Aruba ClearPass Policy Managers, in der die EAP-TLS-Authentifizierungsmethode für Axis Geräte definiert wird.

Servicekonfiguration

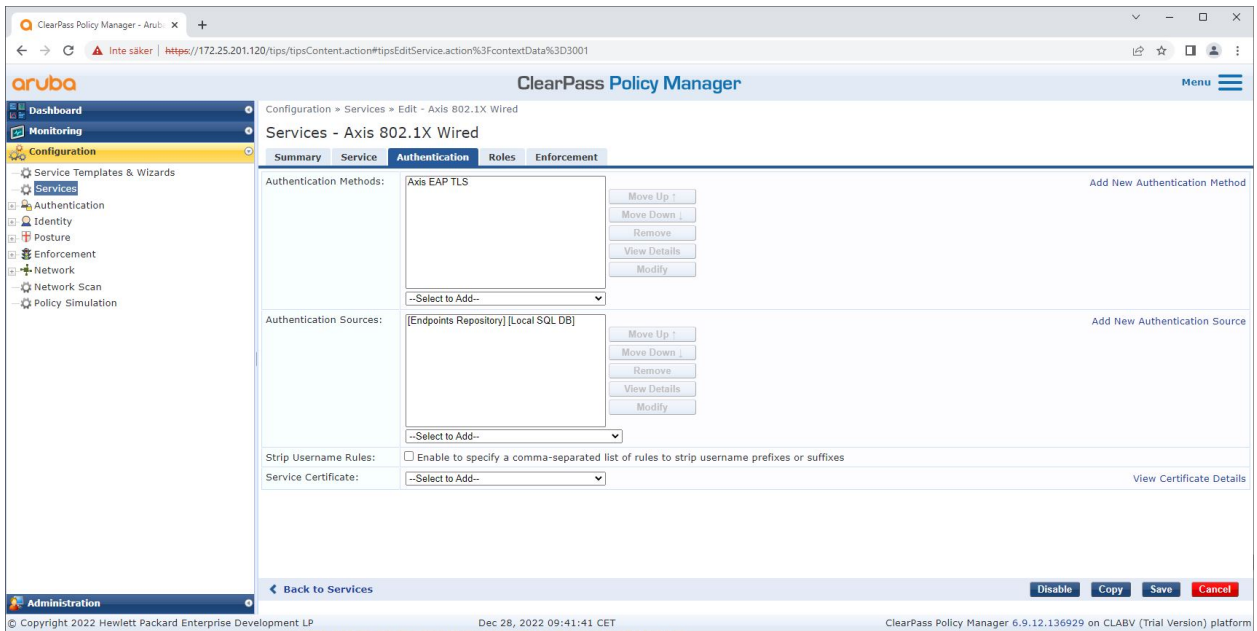
In der Services-Schnittstelle werden die Konfigurationsschritte in einem einzigen Dienst zusammengefasst, der die Authentifizierung und Autorisierung von Axis Geräten in Aruba-Netzwerken übernimmt.



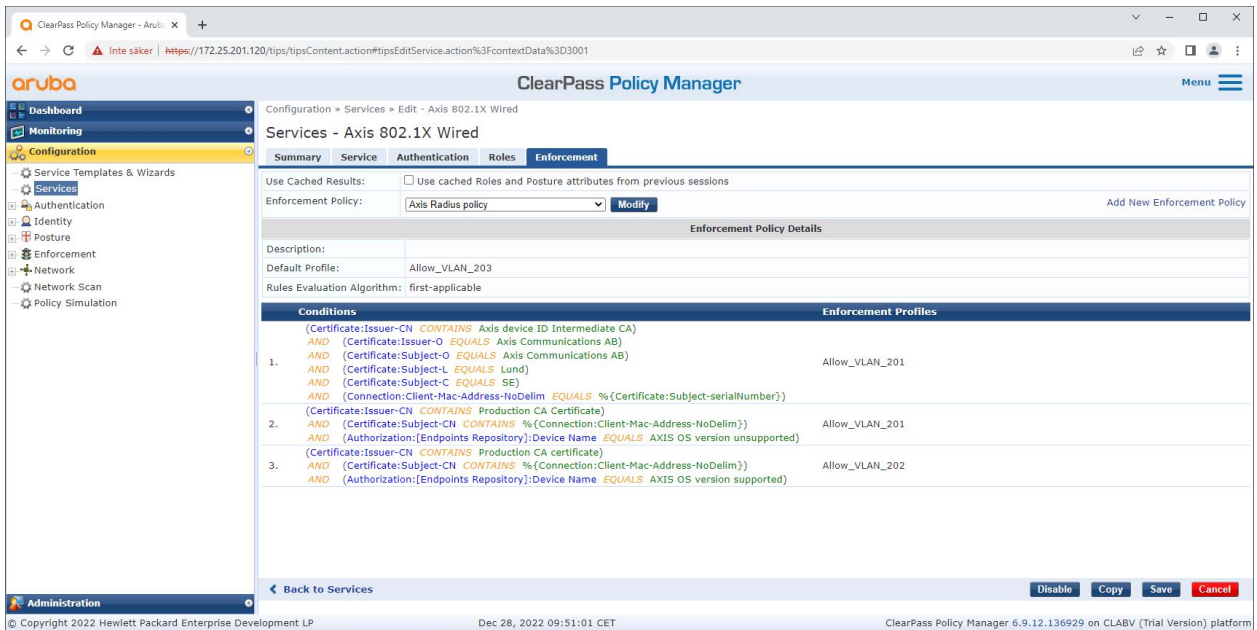
Es wird ein dedizierter Axis Dienst erstellt, der IEEE 802.1X als Verbindungsmethode definiert.

Secure integration of Axis devices into Aruba networks

Sicheres Onboarding – IEEE 802.1X/802.1X



Im nächsten Schritt wird die zuvor erstellte EAP-TLS-Authentifizierungsmethode für den Dienst konfiguriert.



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

Aruba-Zugangsschalter

Axis Geräte werden entweder direkt mit PoE-fähigen Aruba-Zugangsschalter oder über kompatible Axis PoE-Midspans verbunden. Um Axis Geräte sicher in Aruba-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 Aruba ClearPass Policy Manager weiter, der als RADIUS-Server fungiert.

Secure integration of Axis devices into Aruba networks

Sicheres Onboarding – IEEE 802.1AR/802.1X

Hinweis

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

Sehen Sie sich das folgende Beispiel einer globalen und Portkonfiguration für Aruba-Zugangsschalter an.

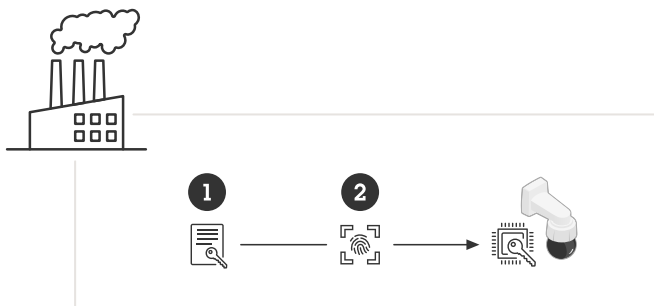
```
radius-server host MyRADIUSIPAddress key "MyRADIUSKey"

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

Konfiguration Axis

Axis Netzwerkgerät

Axis Geräte mit Unterstützung für *Axis Edge Vault* werden mit einer sicheren Geräteidentität hergestellt, der sogenannten Axis Geräte-ID. Die Axis Geräte-ID basiert auf dem internationalen Standard IEEE 802.1AR, der eine Methode zur automatisierten, sicheren Geräteidentifizierung und Netzwerkeinbindung 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-Schlüsselinfrastruktur (PKI)
- 2 Axis Geräte-ID

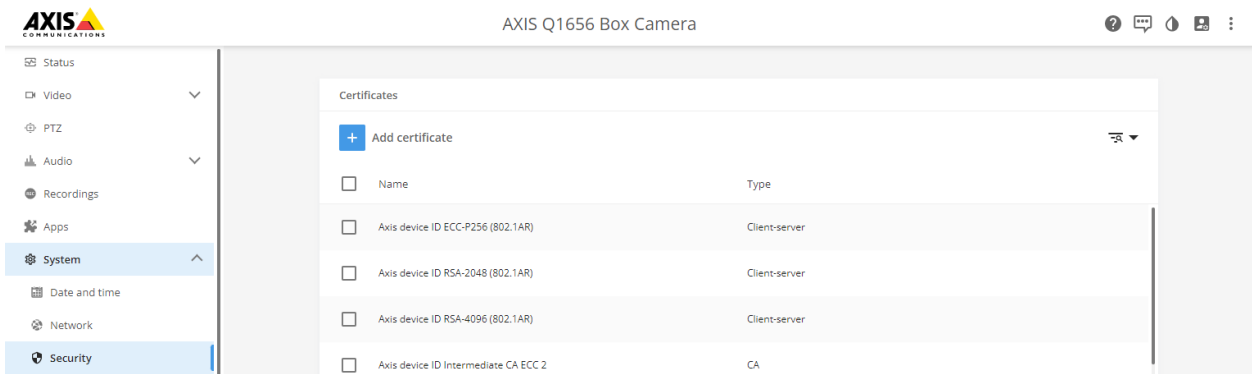
Der hardwaregeschützte sichere Schlüsselspeicher, der von einem sicheren Element des Axis Geräts bereitgestellt wird, ist werkseitig mit einem gerätespezifischen Zertifikat und entsprechenden Schlüsseln (Axis Geräte-ID) ausgestattet, die die Authentizität des Axis Geräts global nachweisen können. Der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

Hinweis

Die Seriennummer eines Axis Geräts ist seine MAC Adresse.

Secure integration of Axis devices into Aruba networks

Sicheres Onboarding – IEEE 802.1AR/802.1X



Der Zertifikatspeicher des Axis Geräts im werkseitigen Standardzustand mit der Axis Geräte-ID.

Das IEEE 802.1AR-konforme Axis Geräte-ID-Zertifikat enthält Informationen zur Seriennummer und andere herstellerspezifische Informationen von Axis. Die Informationen werden vom Aruba ClearPass Policy Manager zur Analyse und Entscheidungsfindung zur Gewährung des Zugriffs auf das Netzwerk verwendet. Bitte beachten Sie die folgenden Informationen, die einem Axis Geräte-ID-Zertifikat entnommen werden können

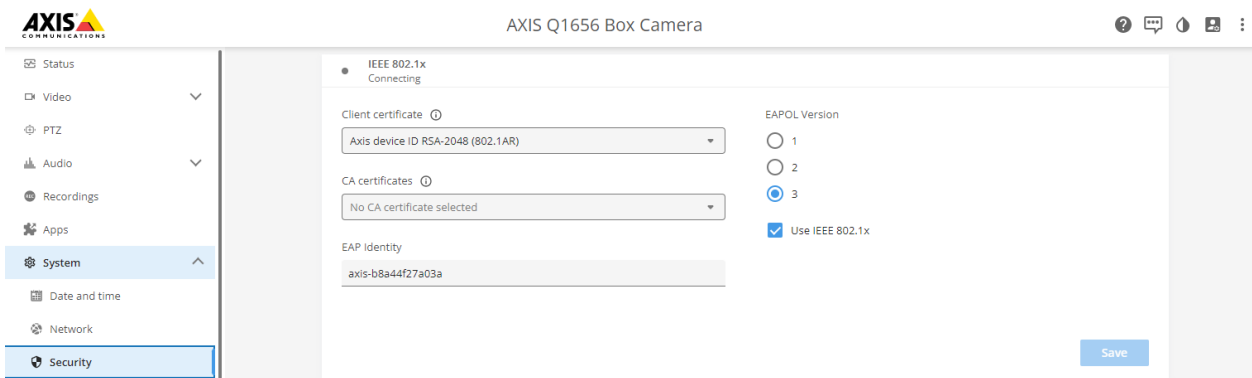


Country (Land)	SE
Standort	Lund
Ausstellerorganisation	Axis Communications AB
Allgemeiner Name des Ausstellers	Axis Geräte-ID intermediär
Organisation	Axis Communications AB
Einfacher Name	axis-b8a44f279511-eccp256-1
Seriennummer	b8a44f279511

Der gebräuchliche Name setzt sich aus einer Kombination aus dem Firmennamen von Axis, der Seriennummer des Geräts und dem verwendeten Kryptoalgorithmus (ECC P256, RSA 2048, RSA 4096) zusammen. Seit AXIS OS 10.1 (2020-09 ist IEEE 802.1X standardmäßig mit vorkonfigurierter Axis Geräte-ID aktiviert. Dadurch kann sich das Axis Gerät in IEEE 802.1X-fähigen Netzwerken authentifizieren.

Secure integration of Axis devices into Aruba networks

Sicheres Onboarding – IEEE 802.1AR/802.1X



Das Axis Gerät im werkseitigen Standardzustand mit aktiviertem IEEE 802.1X und vorab ausgewähltem Axis Geräte-ID-Zertifikat.

Axis Device Manager

AXIS Device Manager und AXIS Device Manager Extend können im Netzwerk verwendet werden, um mehrere Axis Geräte kostengünstig zu konfigurieren und zu verwalten. Axis Device Manager ist eine auf Microsoft Windows basierende Anwendung, die lokal auf einer Maschine im Netzwerk installiert werden kann, während Axis Device Manager Extend für die Geräteverwaltung an mehreren Standorten auf eine Cloud-Infrastruktur angewiesen ist. Beide bieten einfache Verwaltungs- und Konfigurationsfunktionen für Axis Geräte wie:

- Installation von Firmware-Updates.
- Anwendung von Cybersicherheitskonfigurationen wie HTTPS- und IEEE 802.1X-Zertifikaten.
- Konfiguration gerätespezifischer Einstellungen wie Bildeinstellungen und andere.

Secure integration of Axis devices into Aruba networks

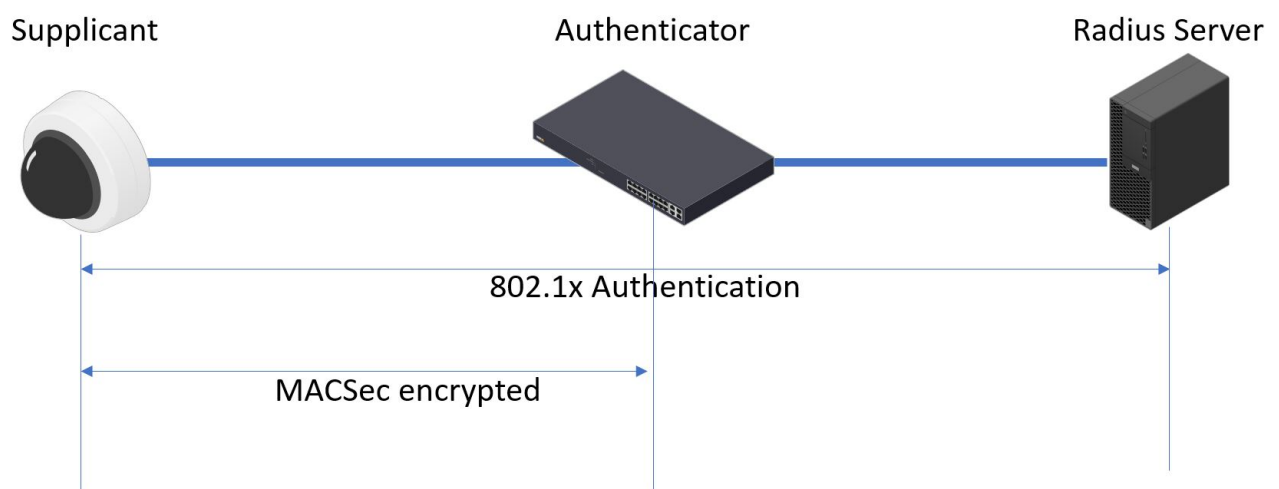
Sicherer Netzwerkbetrieb – IEEE 802.1AE MACsec

Sicherer Netzwerkbetrieb – IEEE 802.1AE MACsec

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



In AXIS OS 10.1 (2020-09) und später, ist IEEE 802.1X standardmäßig für Geräte aktiviert, die mit der Axis Geräte-ID kompatibel sind. In AXIS OS 11.8 und höher unterstützen wir MACsec mit automatischem dynamischen Modus unter Verwendung von standardmäßig aktiviertem IEEE 802.1X EAP-TLS. Wenn Sie ein Axis Gerät mit werkseitigen Standardwerten anschließen, wird die IEEE 802.1X-Netzwerkauthentifizierung durchgeführt und bei Erfolg wird auch der MACsec Dynamische CAK-Modus ausprobiert.

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

Für IEEE 802.1AE MACsec sind sowohl Konfigurationsvorbereitungen für den Aruba-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.

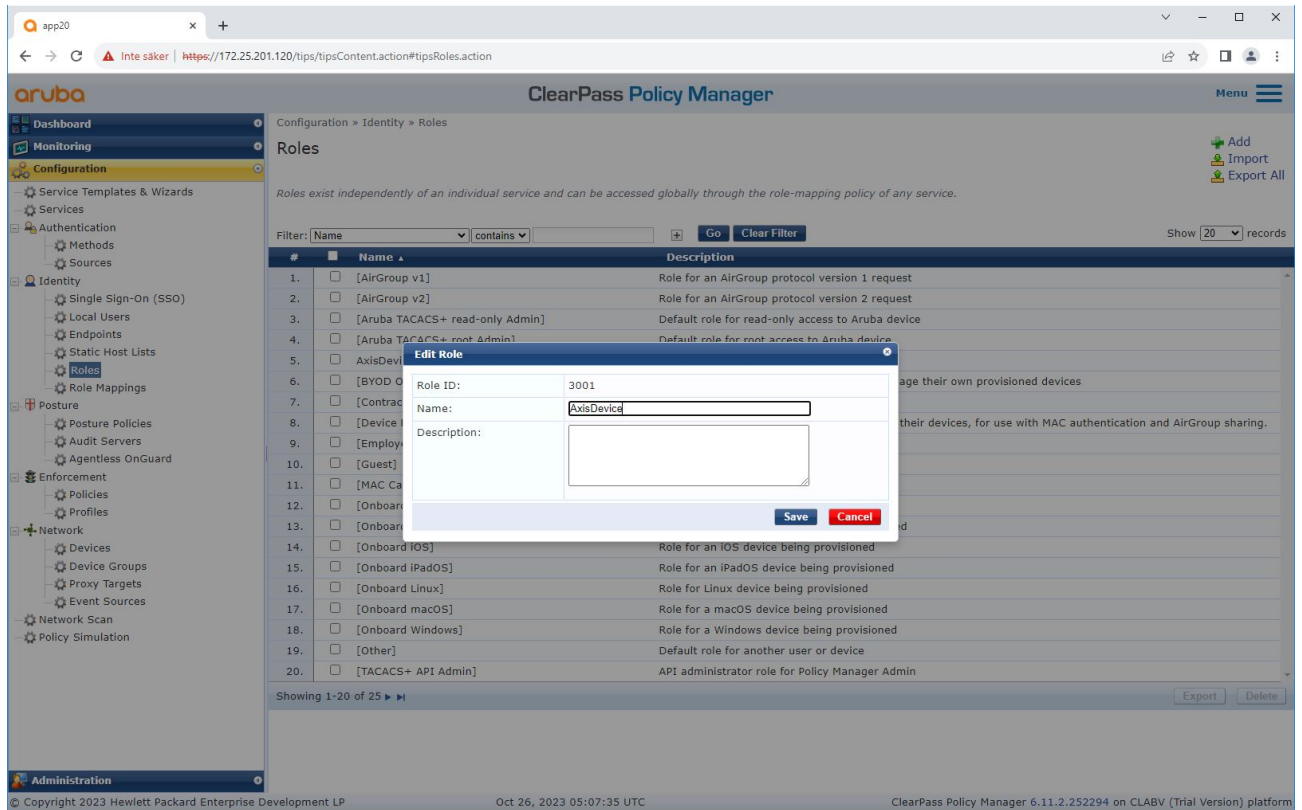
Wenn der Aruba-Zugangsschalter MACsec mit EAP-TLS nicht unterstützt, kann der Pre-Shared Key-Modus verwendet und manuell konfiguriert werden.

Secure integration of Axis devices into Aruba networks

Sicherer Netzwerkbetrieb – IEEE 802.1AE MACsec

Aruba ClearPass Policy Manager

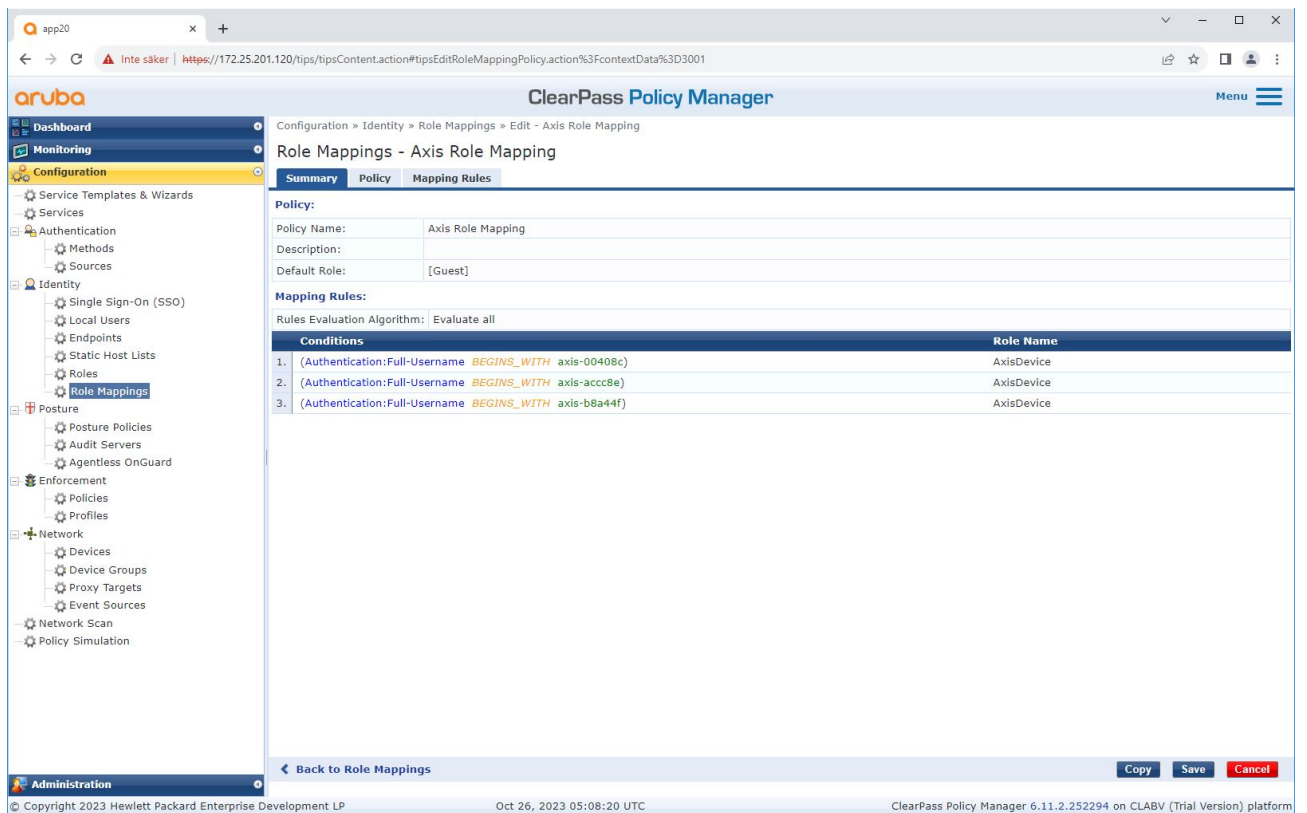
Rollen- und Rollenzuordnungsrichtlinie



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

Secure integration of Axis devices into Aruba networks

Sicherer Netzwerkbetrieb – IEEE 802.1AE MACsec



The screenshot shows the Aruba ClearPass Policy Manager web interface. The navigation menu on the left includes Dashboard, Monitoring, Configuration, and Administration. The Configuration menu is expanded, showing options like Service Templates & Wizards, Services, Authentication, Identity, Posture, Enforcement, and Network. The main content area is titled "Role Mappings - Axis Role Mapping" and has tabs for Summary, Policy, and Mapping Rules. The Mapping Rules tab is active, showing a table of conditions and role names.

Conditions	Role Name
1. (Authentication:Full-Username <i>BEGINS_WITH</i> axis-00408c)	AxisDevice
2. (Authentication:Full-Username <i>BEGINS_WITH</i> axis-acc89e)	AxisDevice
3. (Authentication:Full-Username <i>BEGINS_WITH</i> axis-b8a44f)	AxisDevice

Hinzufügen einer Axis Rollenzuordnungsrichtlinie für die zuvor erstellte Axis Geräterolle. Die definierten Bedingungen sind erforderlich, damit ein Gerät der Axis Geräterolle zugeordnet werden kann. Wenn die Bedingungen nicht erfüllt sind, wird das Gerät Teil der Rolle [Gast] sein.

Standardmäßig verwenden Axis Geräte das EAP-Identitätsformat „axis-serialnumber“. Die Seriennummer eines Axis Geräts ist seine MAC Adresse. Zum Beispiel „axis-b8a44f45b4e6“.

Secure integration of Axis devices into Aruba networks

Sicherer Netzwerkbetrieb – IEEE 802.1AE MACsec

Servicekonfiguration

The screenshot displays the Aruba ClearPass Policy Manager web interface. The left sidebar shows the navigation menu with categories like Dashboard, Monitoring, Configuration, and Administration. The main content area is titled 'Services - Axis 802.1X Wired' and shows the configuration for a role mapping policy named 'Axis Role Mapping'. The policy details include a description, default role of '[Guest]', and a rules evaluation algorithm of 'evaluate-all'. A table lists three conditions for role assignment, all leading to the 'AxisDevice' role.

Conditions	Role
1. (Authentication:Full-Username BEGINS_WITH axis-00408c)	AxisDevice
2. (Authentication:Full-Username BEGINS_WITH axis-acc08e)	AxisDevice
3. (Authentication:Full-Username BEGINS_WITH axis-b8a44f)	AxisDevice

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

Secure integration of Axis devices into Aruba networks

Sicherer Netzwerkbetrieb – IEEE 802.1AE MACsec

The screenshot shows the ClearPass Policy Manager interface for editing the 'Axis 802.1X Wired' service. The 'Enforcement' tab is selected, showing the following configuration:

- Use Cached Results: Use cached Roles and Posture attributes from previous sessions
- Enforcement Policy: Axis Radius policy (Modify)
- Enforcement Policy Details:
 - Description:
 - Default Profile: Allow_VLAN_203
 - Rules Evaluation Algorithm: evaluate-all
- Conditions and Enforcement Profiles table:

Conditions	Enforcement Profiles
1. (Certificate:Issuer-CN CONTAINS Axis device ID Intermediate CA) AND (Certificate:Issuer-O EQUALS Axis Communications AB) AND (Certificate:Subject-O EQUALS Axis Communications AB) AND (Connection:Client-Mac-Address-NoDelim EQUALS %(Certificate:Subject-serialNumber)) AND (Tips:Role EQUALS AxisDevice)	Allow_VLAN_201
2. unsupported) (Certificate:Issuer-CN CONTAINS Production CA) AND (Authorization:[Endpoints Repository]:Device Name EQUALS AXIS OS version AND (Certificate:Subject-CN CONTAINS Production XYZ) AND (Tips:Role EQUALS AxisDevice)	Allow_VLAN_201
3. supported) (Certificate:Issuer-CN CONTAINS Production CA) AND (Authorization:[Endpoints Repository]:Device Name EQUALS AXIS OS version AND (Certificate:Subject-CN CONTAINS Production XYZ) AND (Tips:Role EQUALS AxisDevice)	Allow_VLAN_202

At the bottom of the interface, there are buttons for 'Disable', 'Copy', 'Save', and 'Cancel'. The footer shows 'Copyright 2023 Hewlett Packard Enterprise Development LP', 'Oct 26, 2023 05:11:50 UTC', and 'ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform'.

Hinzufügen des Axis Rollennamens als Bedingung zu den vorhandenen Richtliniendefinitionen.

Secure integration of Axis devices into Aruba networks

Sicherer Netzwerkbetrieb – IEEE 802.1AE MACsec

Durchsetzungsprofil

The screenshot shows the Aruba ClearPass Policy Manager web interface. The left sidebar contains a navigation menu with categories: Dashboard, Monitoring, Configuration, and Administration. The 'Configuration' menu is expanded, showing sub-items like Service Templates & Wizards, Services, Authentication, Identity, Posture, Enforcement, Network, and Policy Simulation. The 'Enforcement' sub-menu is further expanded to show 'Profiles'. The main content area displays the configuration for an enforcement profile named 'Allow_VLAN_201'. The profile details are as follows:

Profile:		
Name:	Allow_VLAN_201	
Description:		
Type:	RADIUS	
Action:	Accept	
Device Group List:	1. Switches	

Attributes:		
Type	Name	Value
1. Radius:IETF	Session-Timeout	= 10800
2. Radius:IETF	Termination-Action	= RADIUS-Request (1)
3. Radius:IETF	Tunnel-Type	= VLAN (13)
4. Radius:IETF	Tunnel-Medium-Type	= IEEE-802 (6)
5. Radius:IETF	Tunnel-Private-Group-id	= 201
6. Radius:Aruba	Aruba-User-Role	= AxisDevice

At the bottom of the interface, there are buttons for 'Copy', 'Save', and 'Cancel', and a 'Back to Enforcement Profiles' link. The footer of the page includes copyright information for Hewlett Packard Enterprise Development LP, the date 'Oct 26, 2023 05:13:21 UTC', and the version 'ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform'.

Hinzufügen des Axis Rollenamens als Attribut zu den Durchsetzungsprofilen, die im IEEE 802.1X-Onboarding-Dienst zugewiesen sind.

Aruba-Zugangsschalter

Zusätzlich zur sicheren Onboarding-Konfiguration, die in *Aruba-Zugangsschalter auf Seite 16* beschrieben wird, finden Sie weitere Informationen in der folgenden Beispiel-Portkonfiguration für den zu konfigurierenden Aruba-Zugriffsschalter IEEE 802.1AE MACsec.

```
macsec policy macsec-eap
cipher-suite gcm-aes-128
```

```
port-access role AxisDevice
associate macsec-policy macsec-eap
auth-mode client-mode
```

```
aaa authentication port-access dot1x authenticator
macsec
mkacac-length 16
enable
```

Secure integration of Axis devices into Aruba networks

Legacy-Onboarding – MAC-Authentifizierung

Legacy-Onboarding – MAC-Authentifizierung

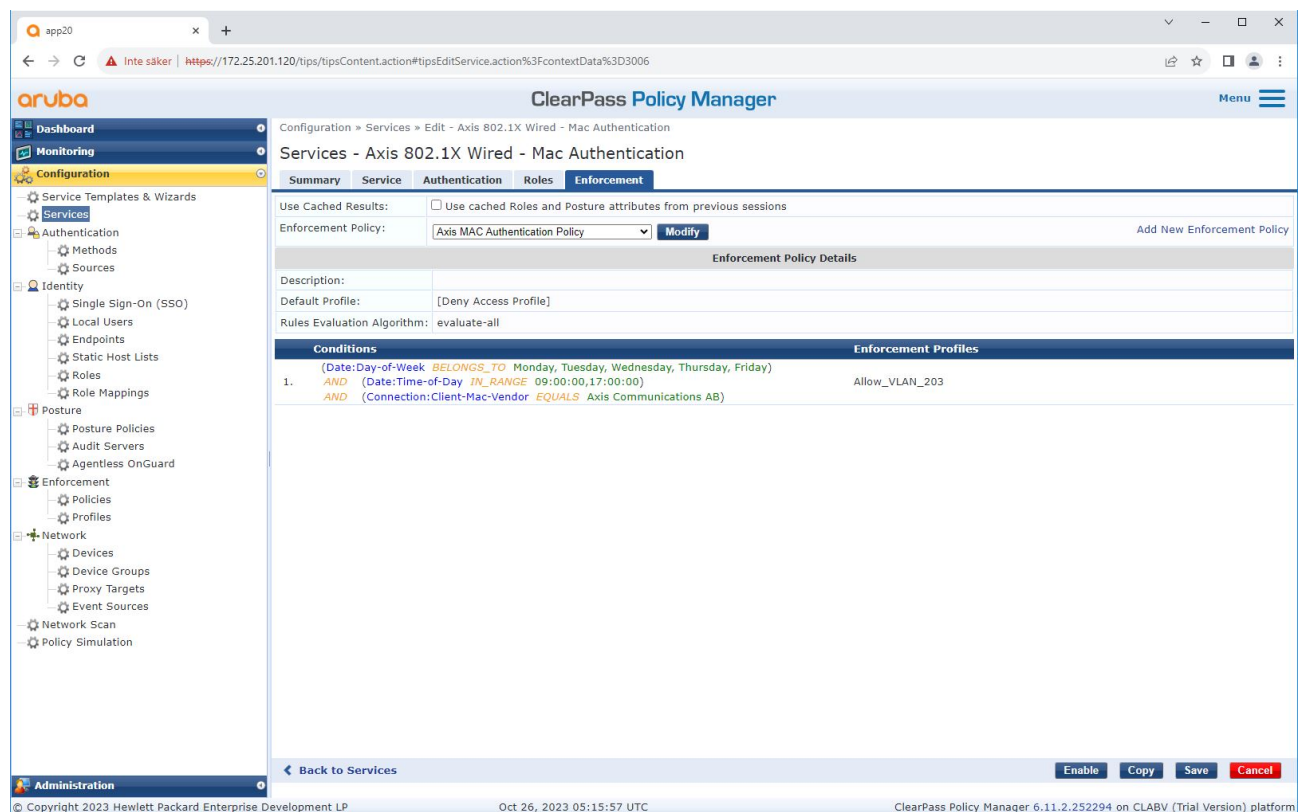
Sie können MAC Authentifizierungs-Bypass (MAB) verwenden, um Axis Geräte einzubinden, die IEEE 802.1AR Onboarding mit dem Axis Geräte-ID-Zertifikat und im Werkzustand aktiviertem IEEE 802.1X nicht unterstützen. Wenn die 802.1X-Einbindung fehlschlägt, validiert Aruba ClearPass Policy Manager die MAC Adresse des Axis Geräts und gewährt Zugriff auf das Netzwerk.

Für MAB sind sowohl Konfigurationsvorbereitungen für den Aruba Access Switch als auch für den ClearPass Policy Manager erforderlich. Auf dem Axis Gerät ist keine Konfiguration erforderlich, um MAB für die Einbindung zu ermöglichen.

Aruba ClearPass Policy Manager

Durchsetzungsrichtlinie

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



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:

- Es ist ein Wochentag zwischen Montag und Freitag
- Es ist zwischen 09:00 und 17:00 Uhr

Secure integration of Axis devices into Aruba networks

Legacy-Onboarding – MAC-Authentifizierung

- Der Anbieter der MAC Adresse stimmt mit Axis Communications AB überein.

Da MAC Adressen gefälscht werden können, wird kein Zugriff auf das reguläre Bereitstellungsnetzwerk gewährt. Wir empfehlen, dass Sie MAB nur für das erste Onboarding und zur weiteren manuellen Überprüfung des Geräts verwenden.

Quellenkonfiguration

In der Quellenschnittstelle wird eine neue Authentifizierungsquelle erstellt, um nur manuell importierte MAC Adressen zuzulassen.

Configuration » Authentication » Sources

Authentication Sources

An authentication source is the identity store (Active Directory, LDAP directory, etc.) against which users and devices are authenticated.

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

#	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

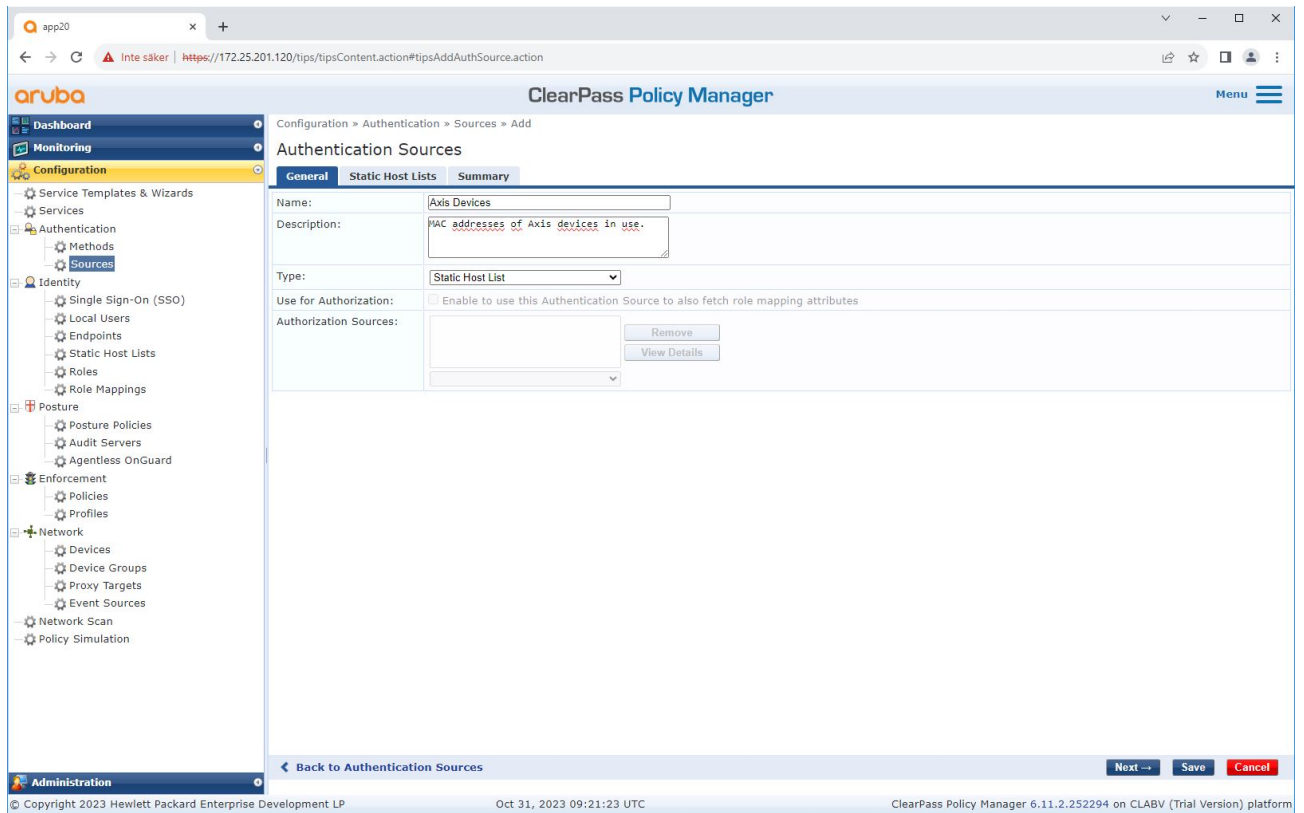
Showing 1-11 of 11

Copy Export Delete

© Copyright 2023 Hewlett Packard Enterprise Development LP Oct 31, 2023 09:13:53 UTC ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform

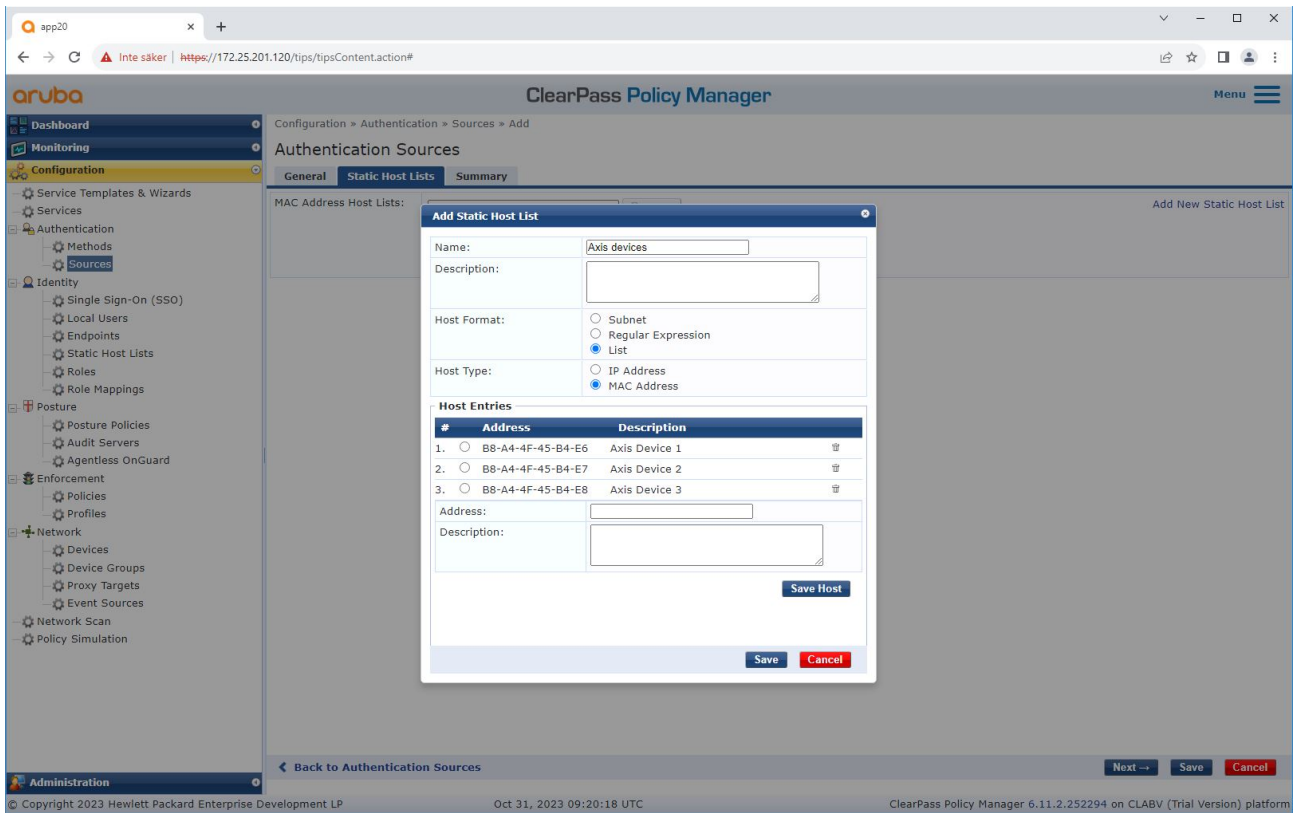
Secure integration of Axis devices into Aruba networks

Legacy-Onboarding – MAC-Authentifizierung



Secure integration of Axis devices into Aruba networks

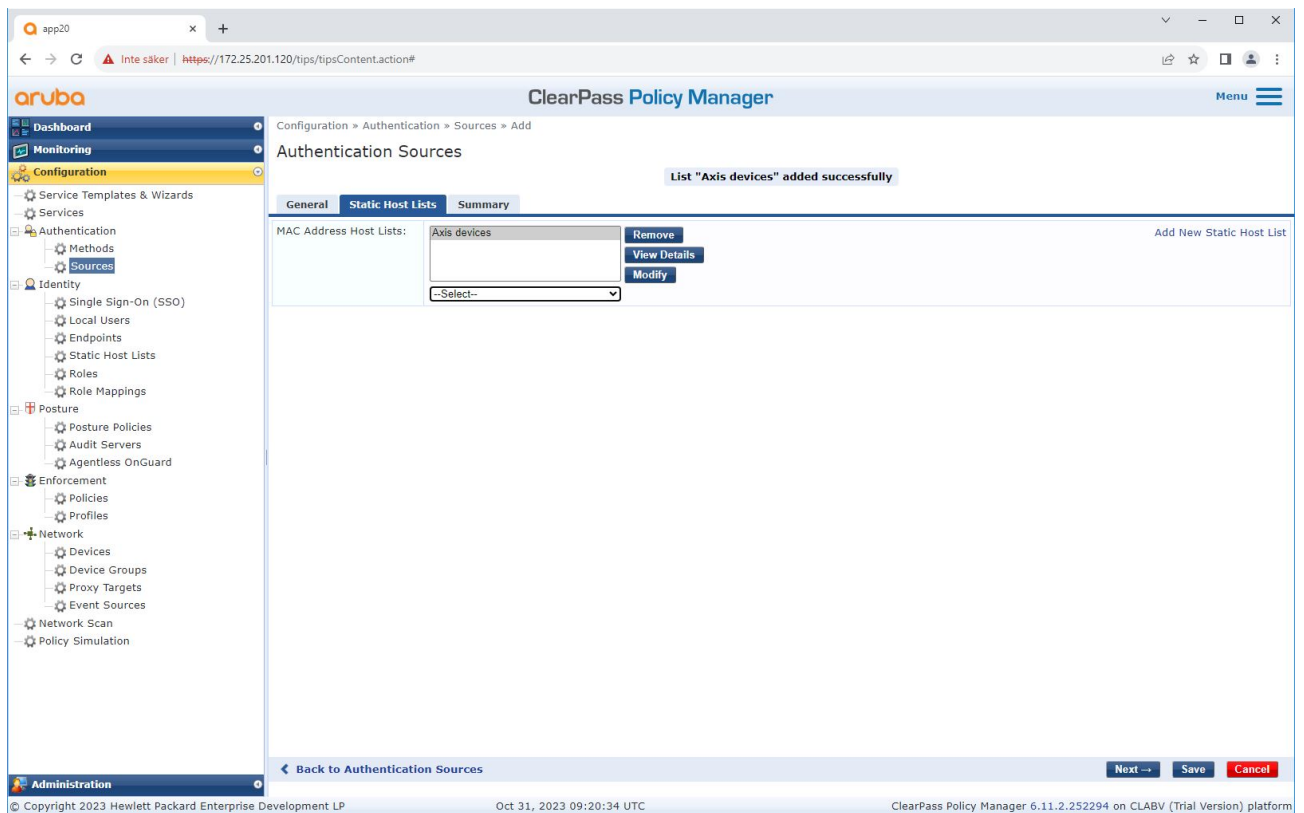
Legacy-Onboarding – MAC-Authentifizierung



Es wird eine statische Hostliste erstellt, die Axis MAC Adressen enthält.

Secure integration of Axis devices into Aruba networks

Legacy-Onboarding – MAC-Authentifizierung



Servicekonfiguration

In der Services-Schnittstelle werden die Konfigurationsschritte in einem einzigen Dienst zusammengefasst, der die Authentifizierung und Autorisierung von Axis Geräten in Aruba-Netzwerken übernimmt.

Secure integration of Axis devices into Aruba networks

Legacy-Onboarding – MAC-Authentifizierung

The screenshot shows the Aruba ClearPass Policy Manager interface. The left sidebar contains navigation menus for Dashboard, Monitoring, Configuration, and Administration. The main content area is titled 'Services' and displays a list of configured services. A filter is set to 'Name' containing 'Axis'. The table below shows the details of these services, including their order, names, types, templates, hit counts, and status.

#	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

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

Secure integration of Axis devices into Aruba networks

Legacy-Onboarding – MAC-Authentifizierung

The screenshot displays the Aruba ClearPass Policy Manager web interface. The left sidebar shows a navigation menu with categories like 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 'Service' tab is active, showing the following configuration details:

- 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

Below these details is a 'Service Rule' section with a table of conditions:

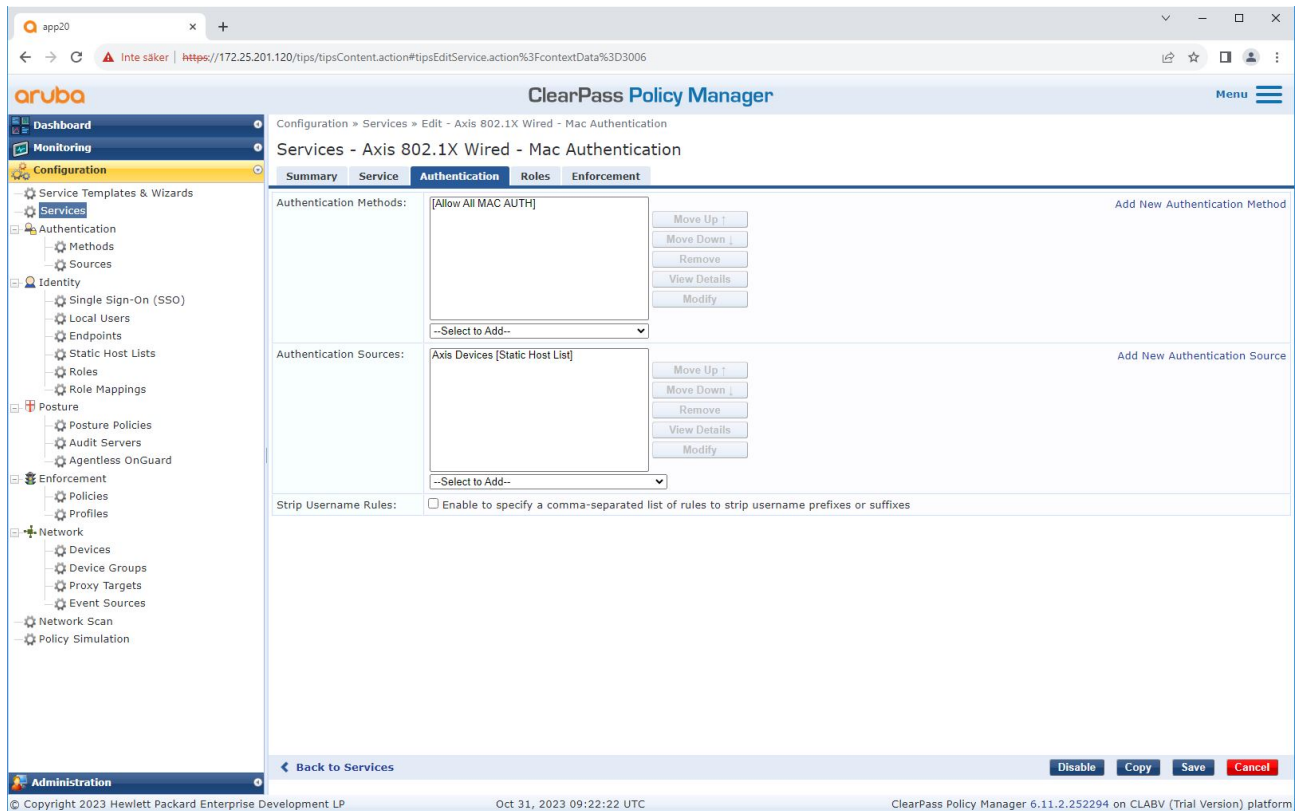
Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	BELONGS_TO Ethernet (15)
2.	Radius:IETF	Service-Type	BELONGS_TO Login-User (1), Call-Check (10)
3.	Connection	Client-Mac-Address	EQUALS % {Radius:IETF:User-Name}
4.	Click to add...		

At the bottom of the configuration area, there are buttons for 'Enable', 'Copy', 'Save', and 'Cancel'. The footer of the interface shows copyright information for Hewlett Packard Enterprise Development LP and the version of the ClearPass Policy Manager (6.11.2.252294).

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

Secure integration of Axis devices into Aruba networks

Legacy-Onboarding – MAC-Authentifizierung



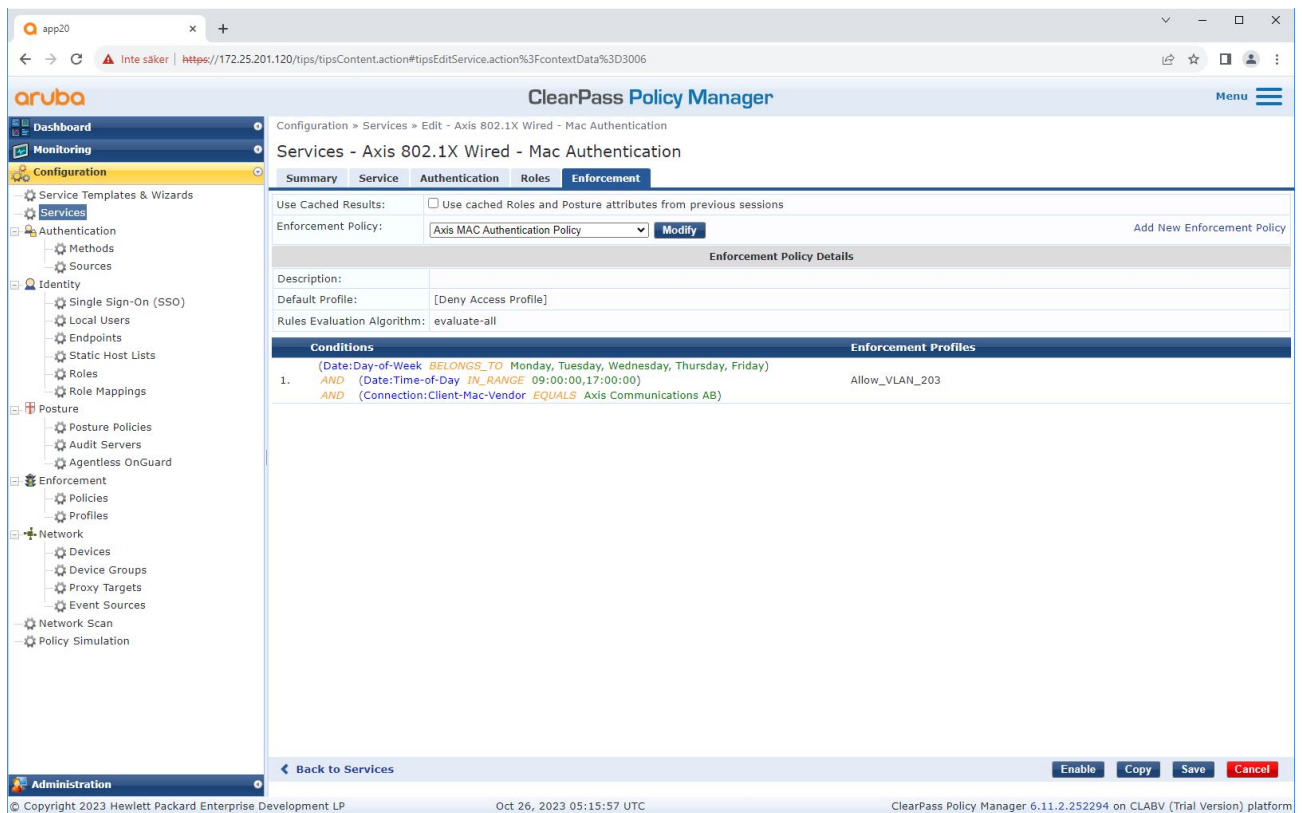
Die vorkonfigurierte MAC-Authentifizierungsmethode ist für den Dienst konfiguriert. Außerdem wird die zuvor erstellte Authentifizierungsquelle ausgewählt, die eine Liste der Axis MAC Adressen enthält.

Axis Communications AB verwendet die folgenden MAC Adressen-OUIs:

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

Secure integration of Axis devices into Aruba networks

Legacy-Onboarding – MAC-Authentifizierung



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

Aruba-Zugangsschalter

Zusätzlich zur sicheren Onboarding-Konfiguration, die in *Aruba-Zugangsschalter auf Seite 16* beschrieben wird, finden Sie weitere Informationen in der folgenden Beispiel-Portkonfiguration für den zu konfigurierenden Aruba-Zugriffsschalter für MAB.

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

