HPE Aruba Networking

Integrationsanleitung

HPE Aruba Networking

Inhalt

HPE Aruba Networking

Einführung

Einführung

Dieser Integrationsleitfaden soll die Best-Practice-Konfiguration für die Einbindung und den Betrieb von Axis Geräten in HPE 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 HPE Aruba-Netzwerk-Infrastruktur und -Anwendungen. Im Folgenden sind nur einige Vorteile aufgeführt, die durch die Kombination von Axis Geräten und Software mit einer HPE Aruba-Netzwerk-Infrastruktur 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 HPE 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 Unternehmensnetzwerks mit HPE Aruba Networking, einschließlich Aruba Access Switches und HPE Aruba Networking ClearPass Policy Manager.
- Fachkenntnisse in modernen Netzwerkzugriffskontrolltechniken und Netzwerk-Sicherheitsrichtlinien.
- Grundkenntnisse über Axis Produkte sind wünschenswert, werden aber im gesamten Handbuch vermittelt.

Sicheres Onboarding – IEEE 802.1AR/802.1X

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

help.axis.com/?&tpiId=&tsection=secure-onboarding-ieee802-1ar-802-1x

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

Erstauthentifizierung

Schließen Sie das von Axis Edge Vault unterstützte Axis Gerät an, um das Gerät gegenüber dem 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 ClearPass Policy Manager die Axis Geräte-ID zusammen mit anderen gerätespezifischen Fingerabdrücken. Die Informationen, wie MAC Adresse und laufendes AXIS OS, werden verwendet, um eine richtlinienbasierte Entscheidung zu treffen.

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

Das Axis Gerät authentifiziert sich beim HPE 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 wechselt das Axis Gerät in das Bereitstellungsnetzwerk (VLAN201), in dem der AXIS Device Manager installiert ist. Über den AXIS Device Manager können Gerätekonfiguration, Sicherheitshärtung und AXIS OS-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 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 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.

Dem Axis Gerät wird Zugriff auf das Produktionsnetzwerk gewährt.

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

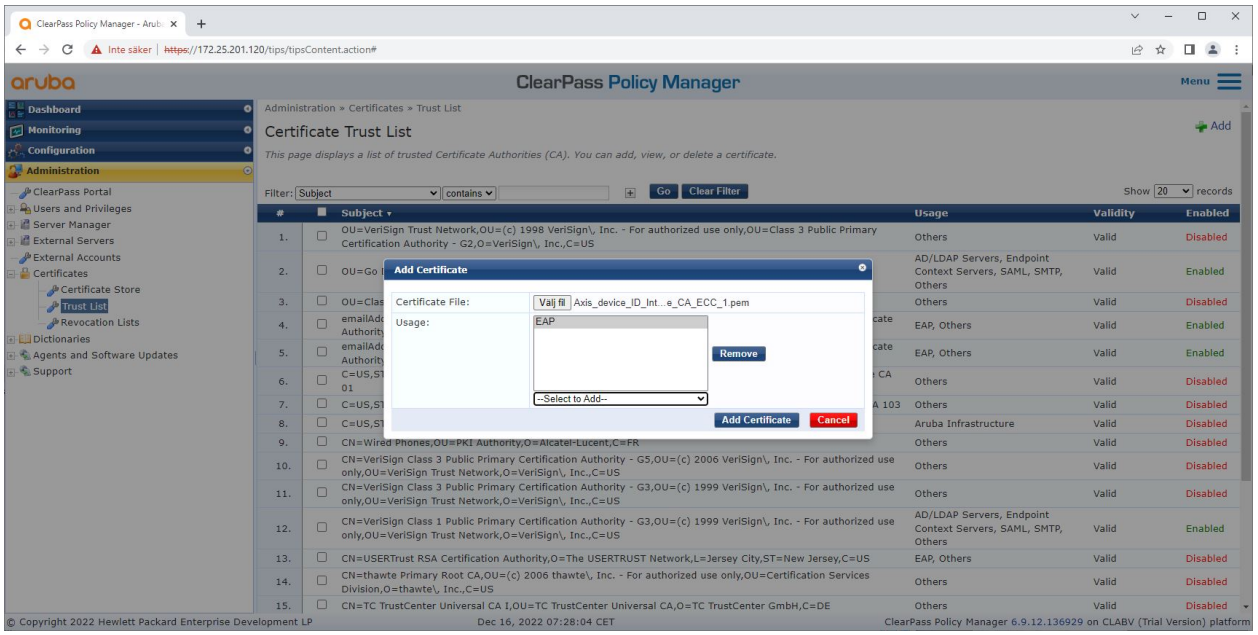
Konfiguration von HPE Aruba Networking

HPE Aruba Networking ClearPass Policy Manager

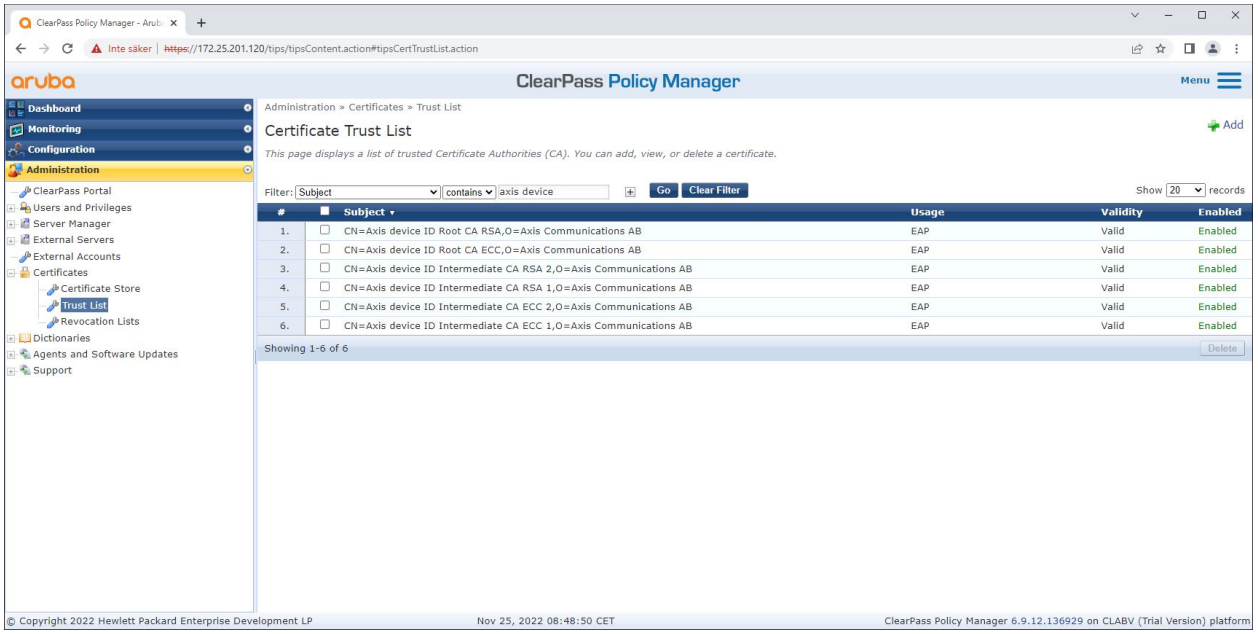
Der ClearPass Policy Manager bietet rollen- und gerätebasierte sichere Netzwerkzugriffskontrolle für IoT, BYOD, Unternehmensgeräte, Mitarbeiter, Auftragnehmer und Gäste in der kabelgebundenen, kabellosen und VPN-Infrastruktur mehrerer Anbieter.

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-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.



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



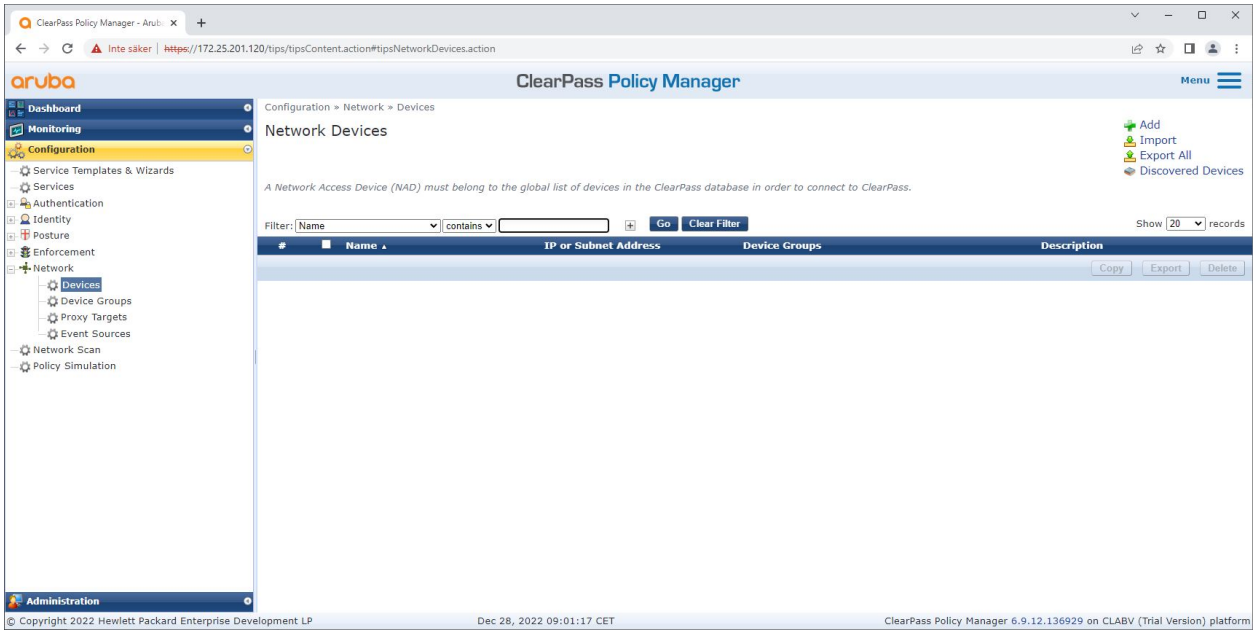
Der vertrauenswürdige Zertifikatsspeicher im ClearPass Policy Manager mit für Axis spezifischer IEEE 802.1AR-Zertifikatskette.

Netzwerkgeräte-/Gruppenkonfiguration

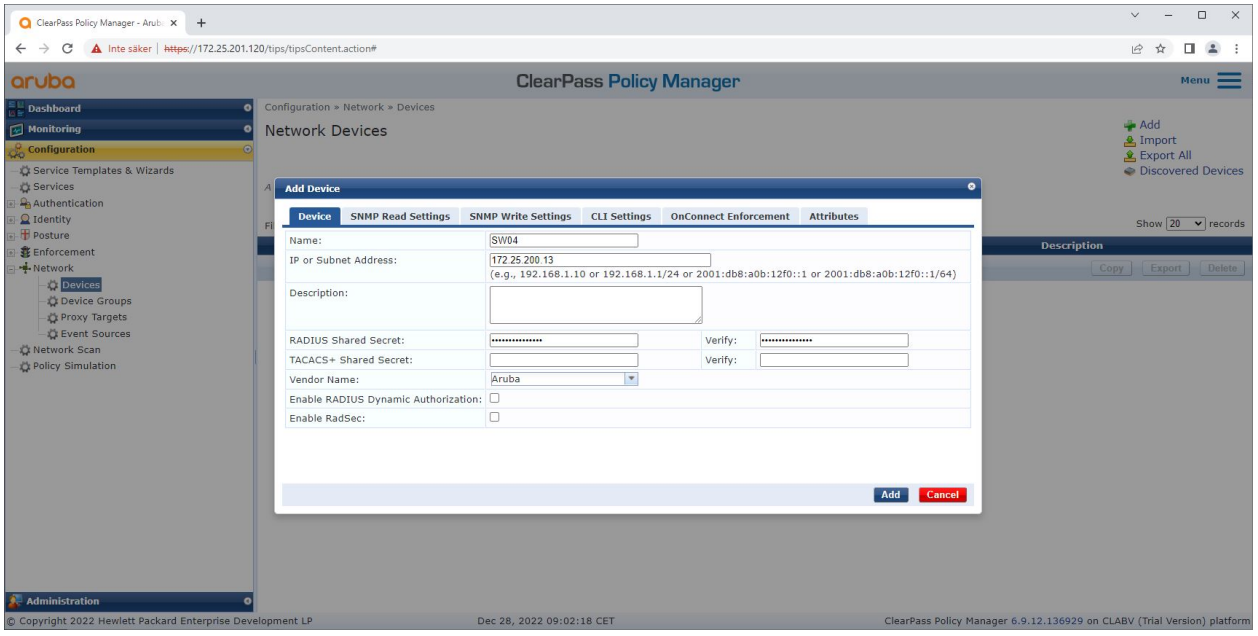
1. Fügen Sie dem ClearPass Policy Manager vertrauenswürdige Netzwerkzugriffsgeräte wie HPE Aruba Netzwerk Access Switches hinzu. Der ClearPass Policy Manager muss wissen, welche Access Switches im Netzwerk für die IEEE 802.1X-Kommunikation verwendet werden.

2. Verwenden Sie die Netzwerkgerätegruppenkonfiguration, um mehrere vertrauenswürdige Netzwerkzugriffsgeräte zu gruppieren. Das Gruppieren vertrauenswürdiger Netzwerkzugriffsgeräte ermöglicht eine einfachere Richtlinienkonfiguration.

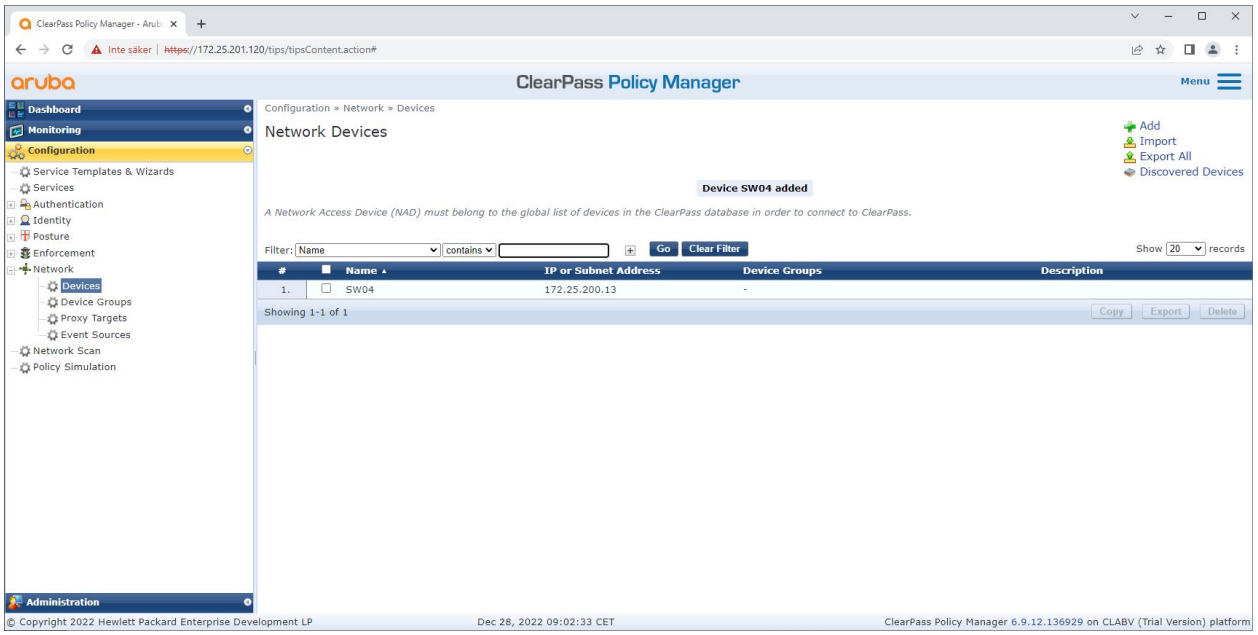
3. Das gemeinsame RADIUS-Geheimnis muss mit der spezifischen IEEE 802.1X-Konfiguration des Switches übereinstimmen.



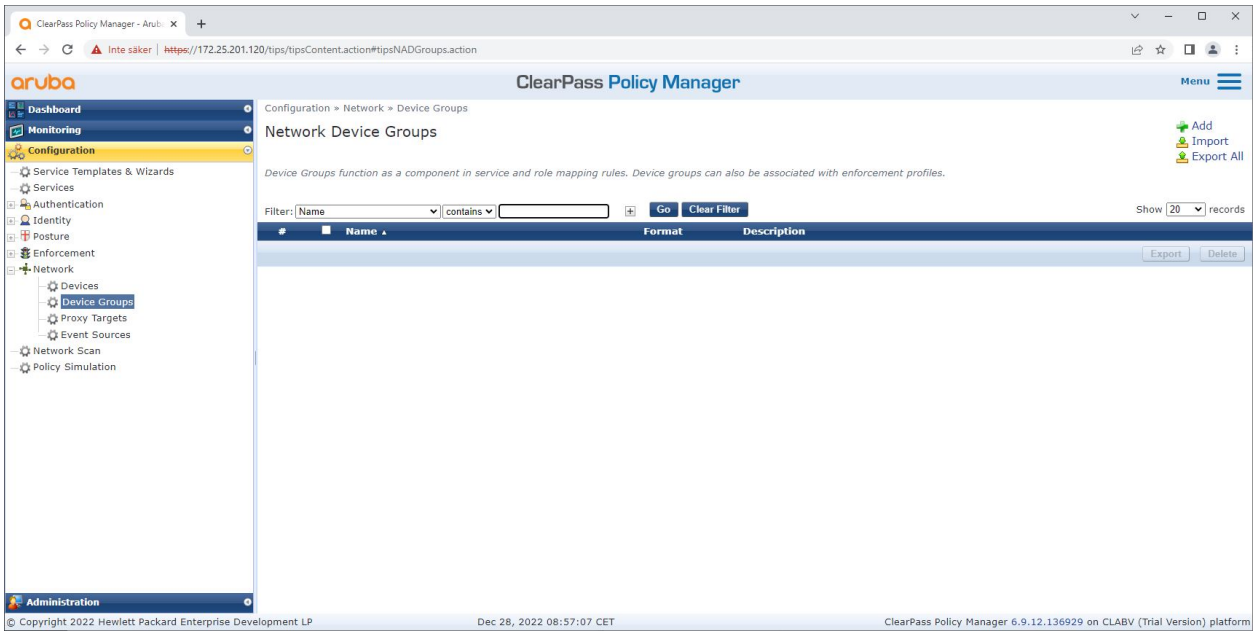
Die Schnittstelle für vertrauenswürdige Netzwerkgeräte im ClearPass Policy Manager.



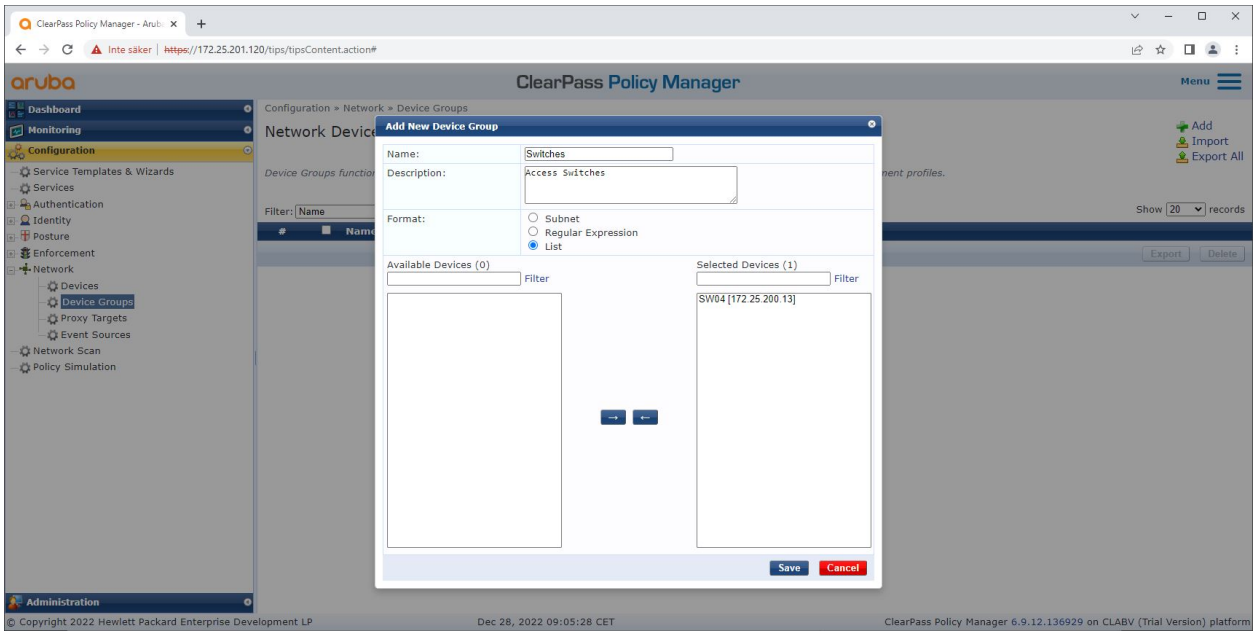
Hinzufügen des HPE Aruba Netzwerk Access Switch als vertrauenswürdiges Netzwerkgerät im ClearPass Policy Manager. Bitte beachten Sie, dass das gemeinsame RADIUS-Geheimnis mit der spezifischen IEEE 802.1X-Konfiguration des Switches übereinstimmen muss.



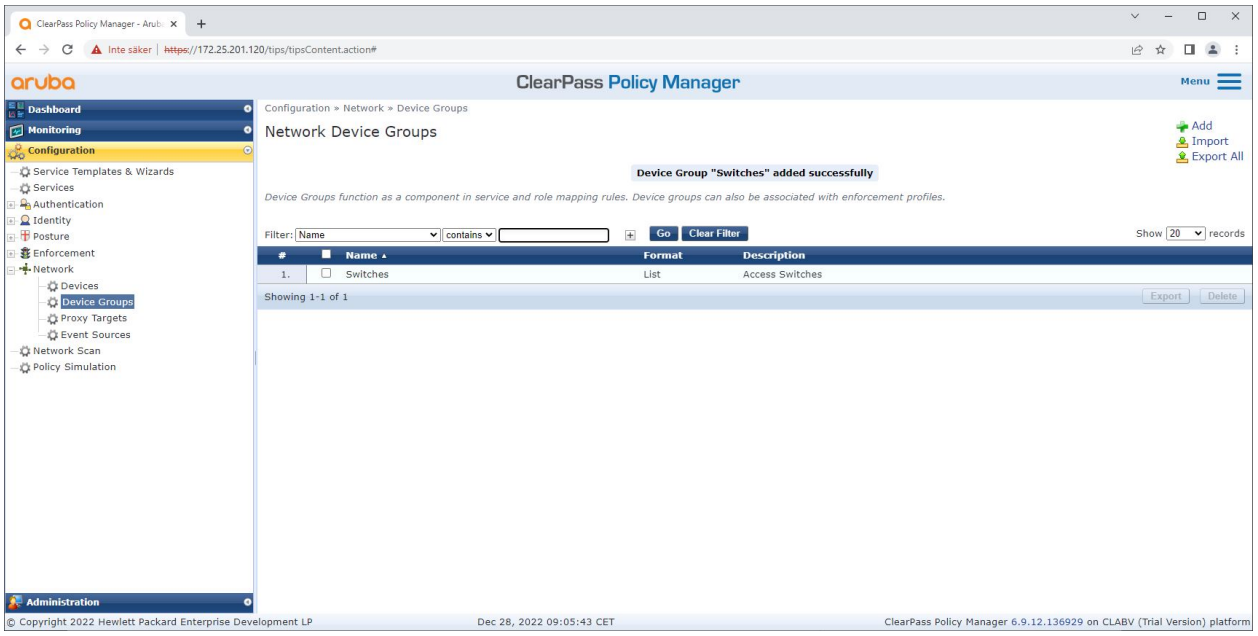
Der ClearPass Policy Manager mit einem konfigurierten vertrauenswürdigen Netzwerkgerät.



Die Schnittstelle für vertrauenswürdige Netzwerkgerätegruppen im ClearPass Policy Manager.



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



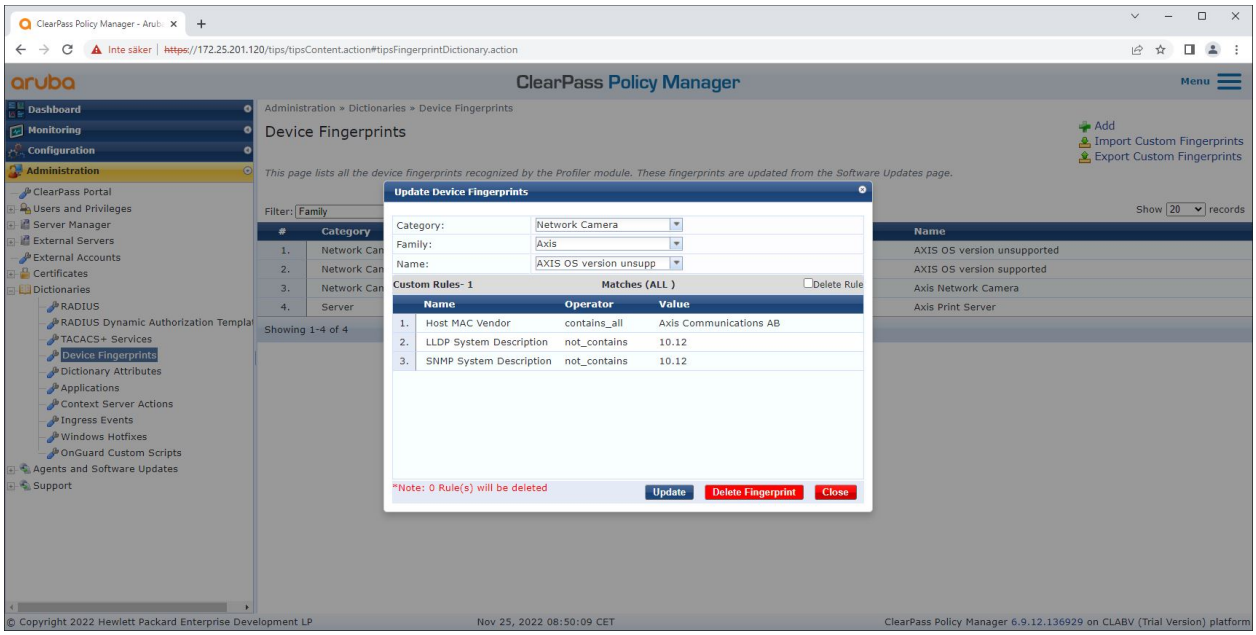
ClearPass Policy Manager mit konfigurierter Netzwerkgerätegruppe, die ein oder mehrere vertrauenswürdige Netzwerkgeräte umfasst.

Konfiguration des Gerätefingerabdrucks

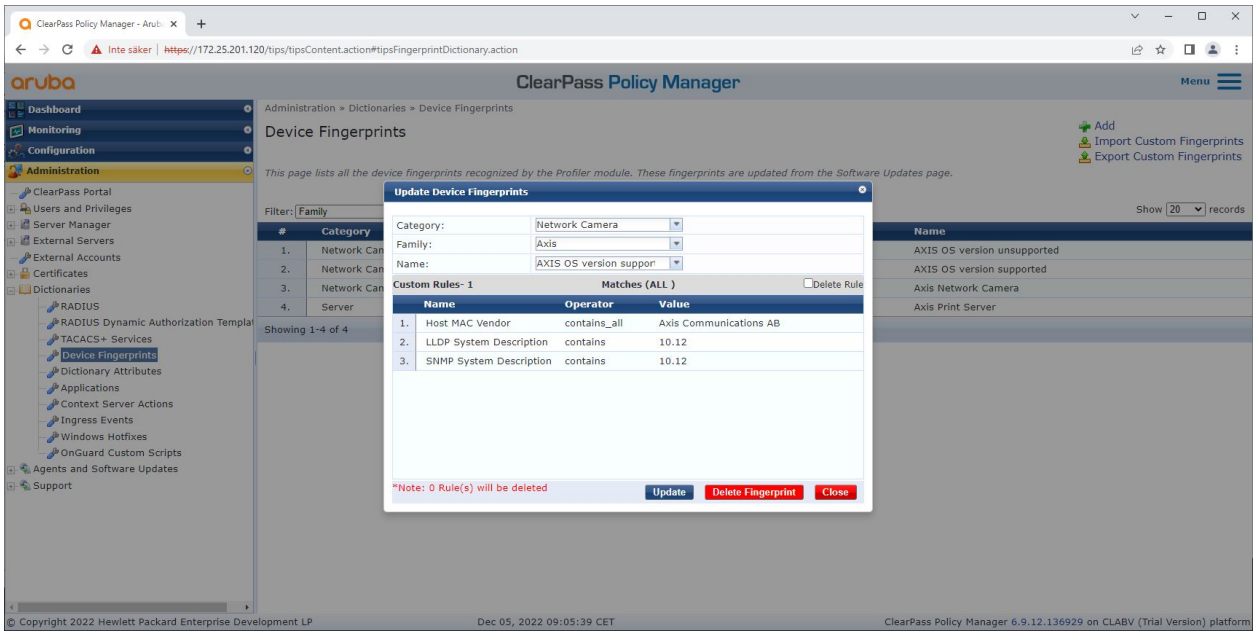
Das Axis Gerät kann gerätespezifische Informationen wie MAC Adresse und Gerätesoftware-Version über Netzwerkerkennung weiterleiten. Verwenden Sie diese Informationen, um im ClearPass Policy Manager einen Geräte-Fingerabdruck zu erstellen, zu aktualisieren oder zu verwalten. Dort können Sie den Zugriff 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. Legen Sie die Einstellungen für den Gerätefingerabdruck fest.



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



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

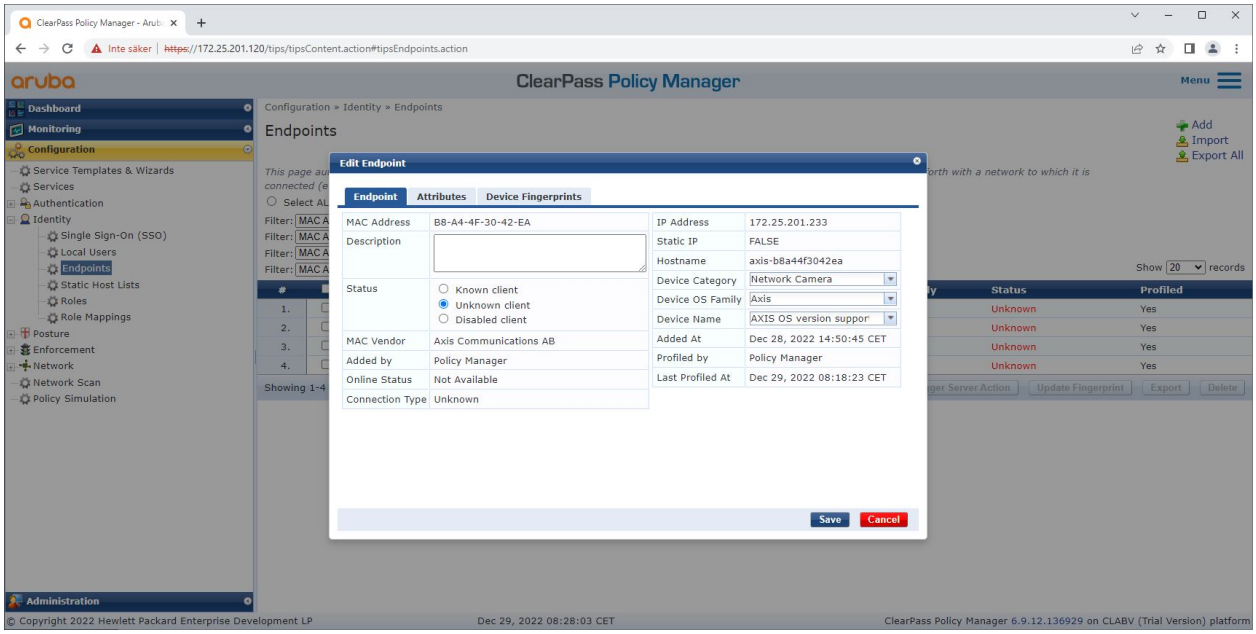
Informationen zum Geräte-Fingerabdruck, der von ClearPass Policy Manager erfasst wurde, finden Sie im Abschnitt „Endpunkte".

1. Gehen Sie zu **Configuration > Identity > Endpoints (Konfiguration > Identität > Endpunkte)**.

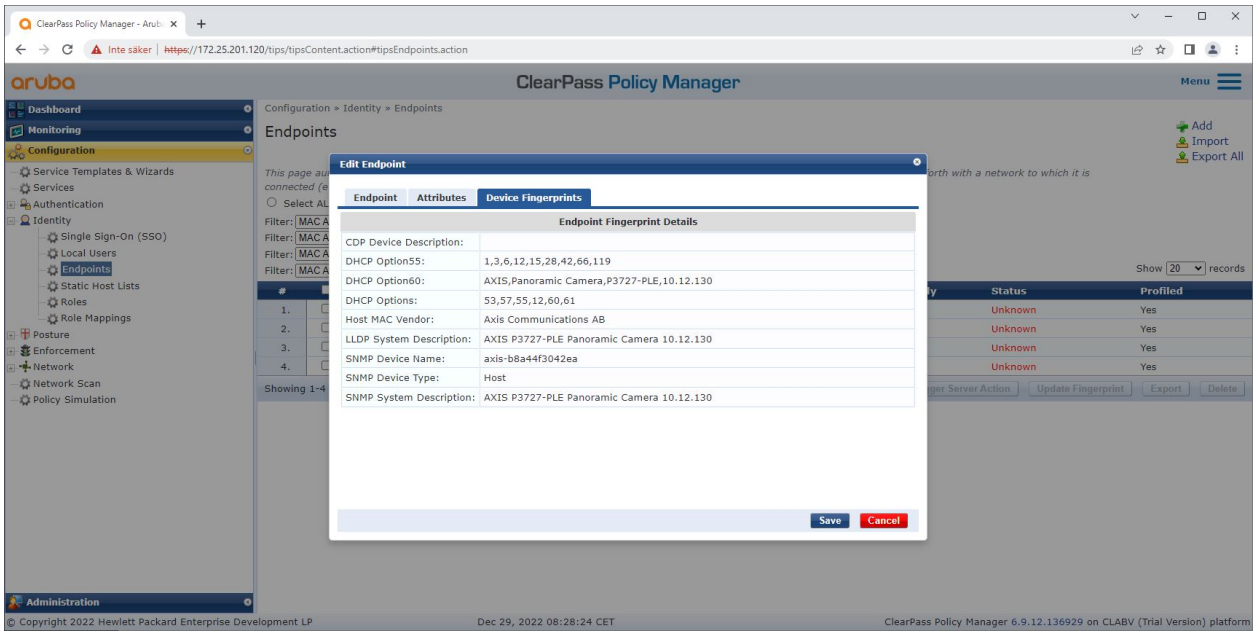
2. Wählen Sie das Gerät, das Sie ansehen möchten.
3. Klicken Sie auf die Registerkarte **Device Fingerprints (Gerätefingerabdrücke)**.

Hinweis

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



Ein von ClearPass Policy Manager profiliertes Axis Gerät.

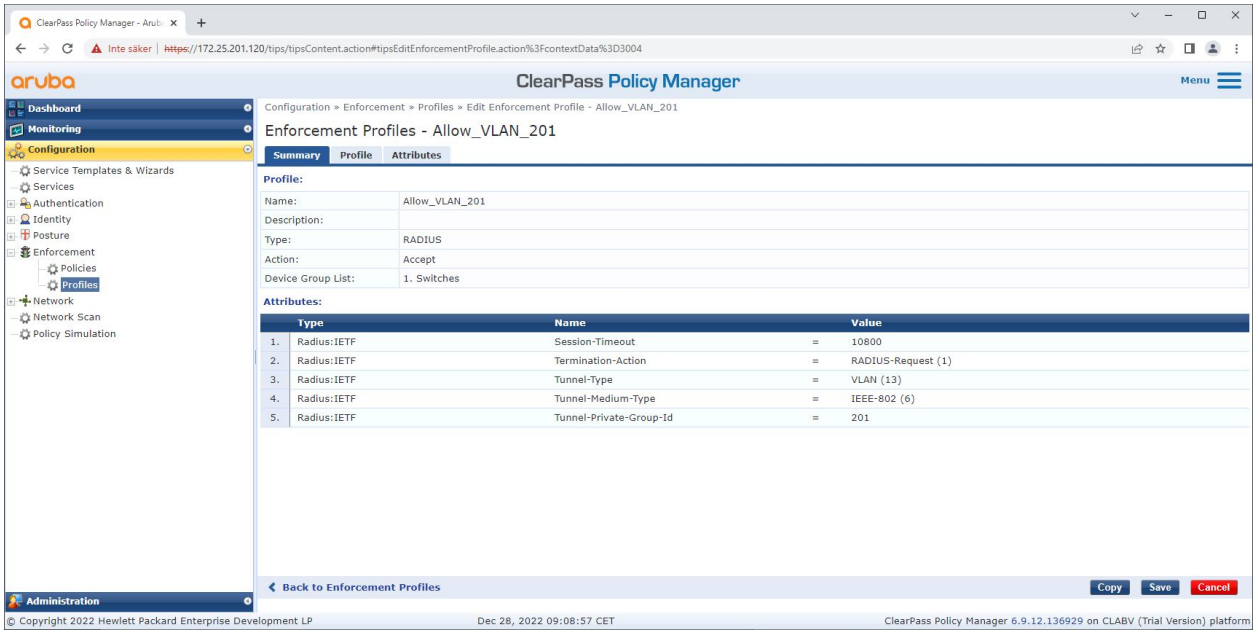


Die detaillierten Gerätefingerabdrücke eines profilierten Axis Geräts. Bitte beachten Sie, dass SNMP in Axis Geräten standardmäßig deaktiviert ist. LLDP-, CDP- und DHCP-spezifische Erkennungsinformationen werden vom Axis Gerät im werkseitigen Standardzustand gemeinsam genutzt und vom HPE Aruba Netzwerk-Zugriffsschalter an den ClearPass Policy Manager weitergeleitet.

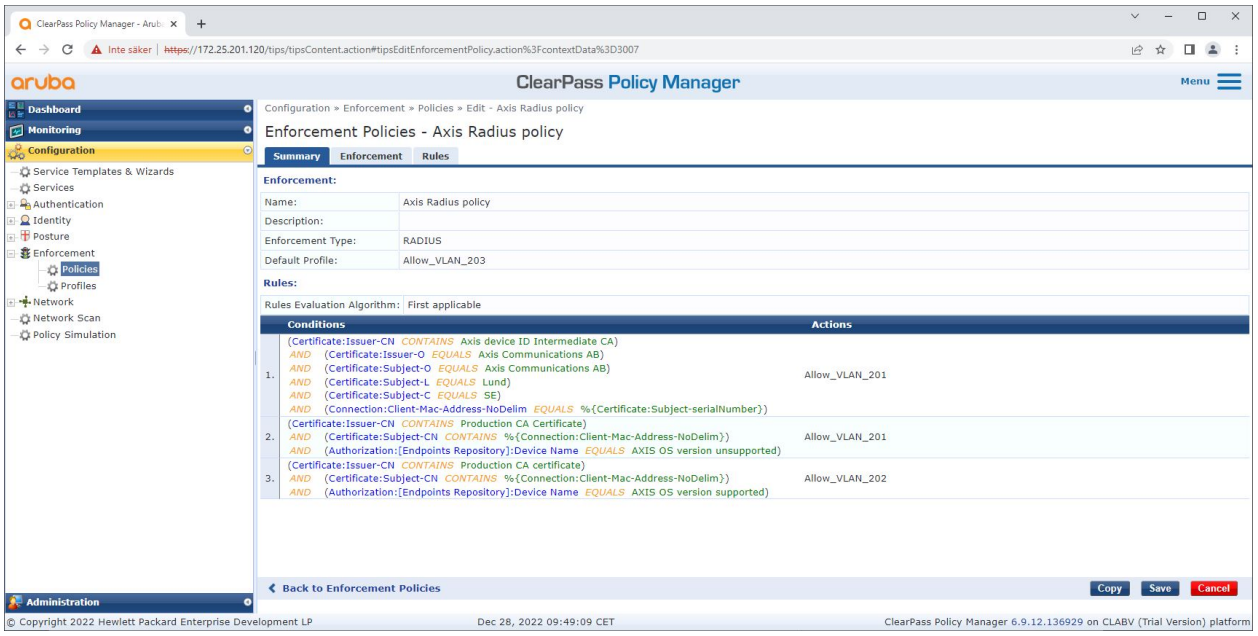
Konfiguration des Durchsetzungsprofils

Enforcement Profile (Durchsetzungsprofil) wird verwendet, um dem 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.

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-Netzwerkunterstützte 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 unten aufgeführt:

Netzwerkzugriff verweigert

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

- Die AXIS OS-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)

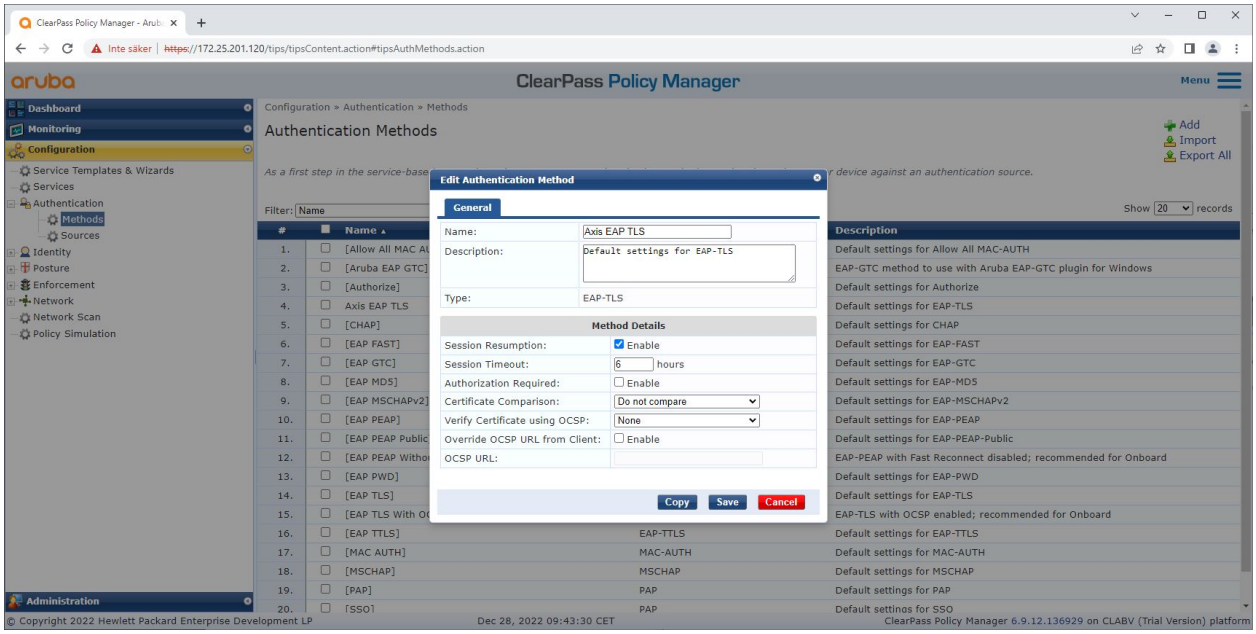
Das Axis Gerät erhält Zugriff auf das Produktionsnetzwerk, in dem das Axis Gerät betrieben werden soll. Der Zugriff wird gewährt, nachdem die Gerätebereitstellung im Bereitstellungsnetzwerk (VLAN 201) abgeschlossen wurde. Die folgenden Bedingungen werden vom ClearPass Policy Manager überprüft:

- Die MAC-Adresse des Geräts stimmt mit dem herstellerspezifischen Axis MAC-Adressen-Schema mit dem Seriennummernattribut des Axis Geräte-ID-Zertifikats überein.

- Die AXIS OS-Version des Axis Geräts.
- Das Produktionszertifikat kann vom vertrauenswürdigen Zertifikatsspeicher überprüft werden.

Konfiguration der Authentifizierungsmethode

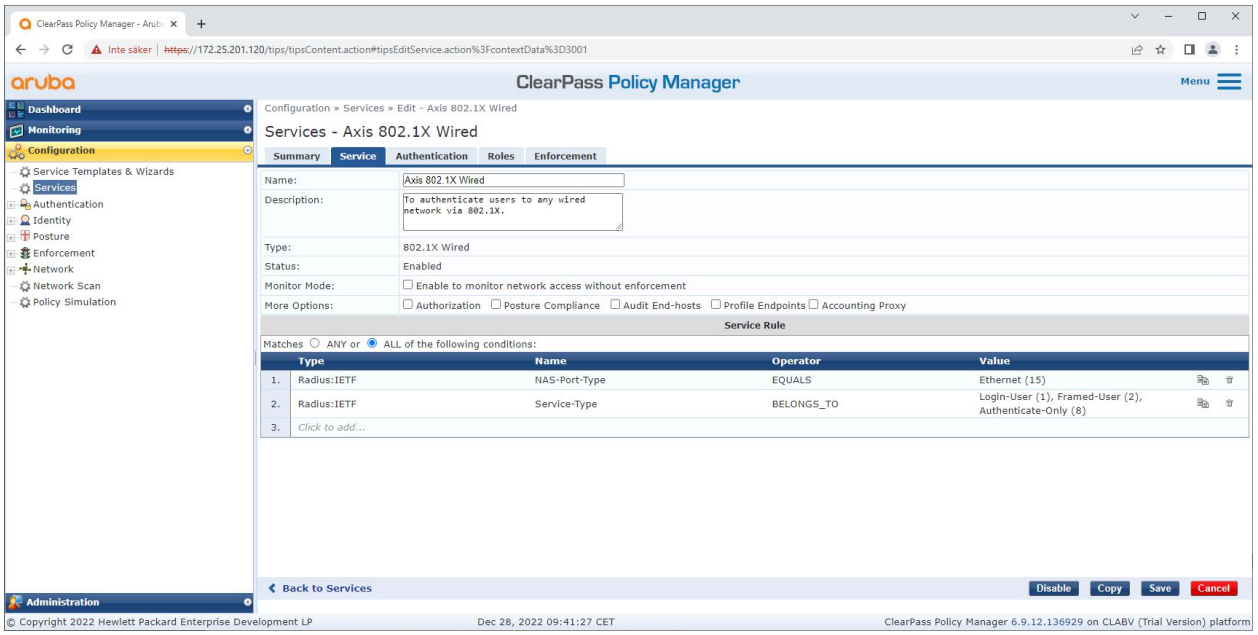
In der Authentifizierungsmethode wird definiert, wie ein Axis Gerät versucht, sich gegenüber dem Netzwerk zu authentifizieren. Die bevorzugte Authentifizierungsmethode sollte IEEE 802.1X EAP-TLS sein, da bei Axis Geräten mit Unterstützung für Axis Edge Vault standardmäßig IEEE 802.1X EAP-TLS aktiviert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



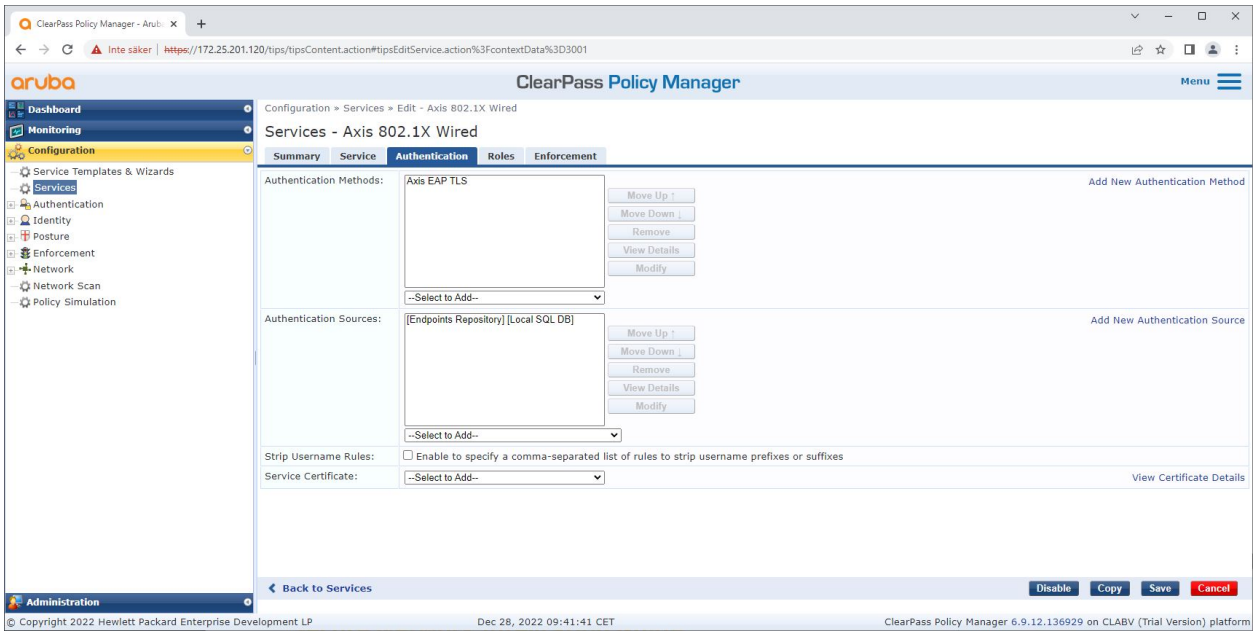
Die Authentifizierungsmethoden-Schnittstelle des ClearPass Policy Managers, in der die EAP-TLS-Authentifizierungsmethode für Axis Geräte definiert wird.

Servicekonfiguration

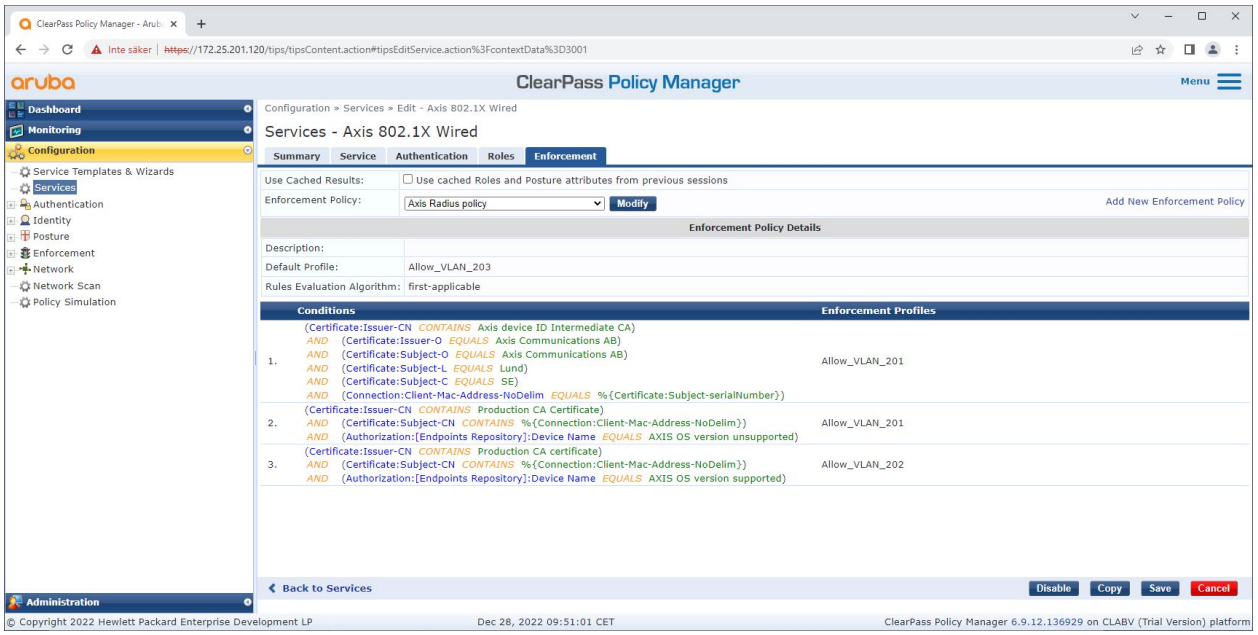
Auf der **Services**-Seite werden die Konfigurationsschritte in einem einzigen Dienst zusammengefasst, der die Authentifizierung und Autorisierung von Axis Geräten in HPE Aruba-Netzwerken übernimmt.



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



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.

HPE Aruba Networking Zugangsschalter

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

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 HPE Aruba Netzwerk-Zugangsschalter an.

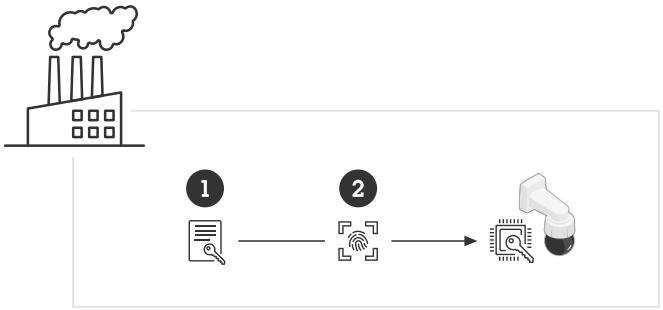
```
radius-server host MyRADIUSIPAddress key "MyRADIUSKey"

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.

Sicheres Onboarding – IEEE 802.1AR/802.1X



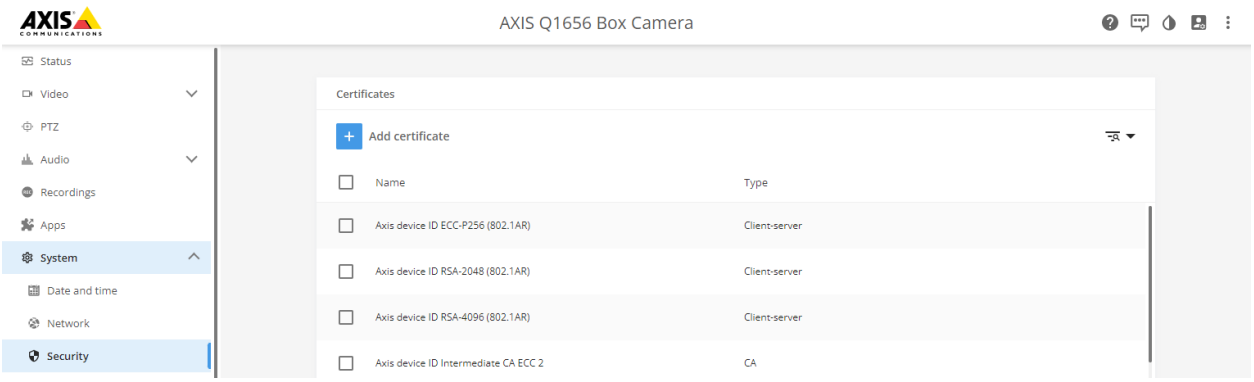
Axis Geräte werden mit dem IEEE 802.1AR-konformen Axis Geräte-ID-Zertifikat für vertrauenswürdige Geräteidentitätsdienste hergestellt

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.

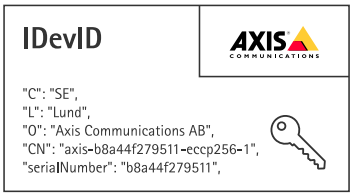
Hinweis

Die Seriennummer eines Axis Geräts ist seine MAC Adresse.



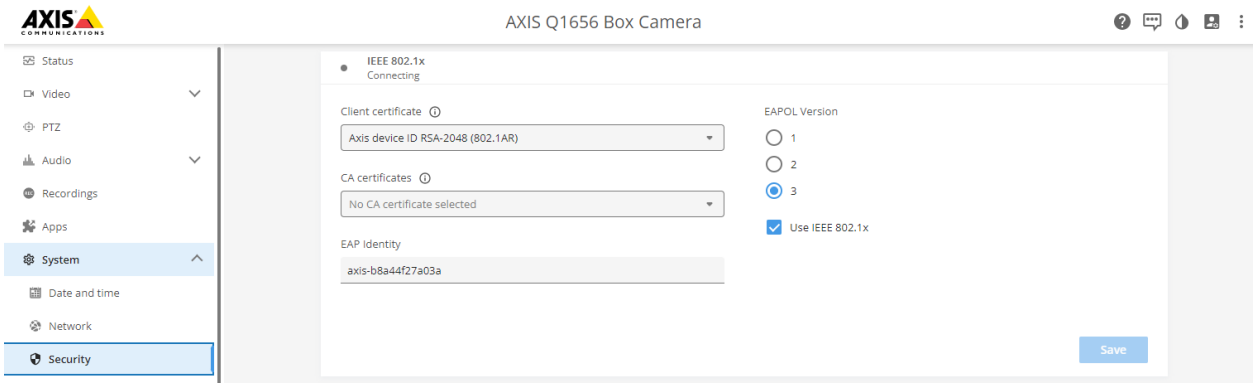
Der Zertifikatspeicher des Axis Geräts im werkseitigen Standardzustand mit der Axis Geräte-ID.

Das IEEE 802.1AR-konforme Axis Geräte-ID-Zertifikat enthält Informationen zur Seriennummer und andere herstellerspezifische Informationen von Axis. Die Informationen werden vom 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.



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

Sicherer Netzwerkbetrieb – IEEE 802.1AE MACsec

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

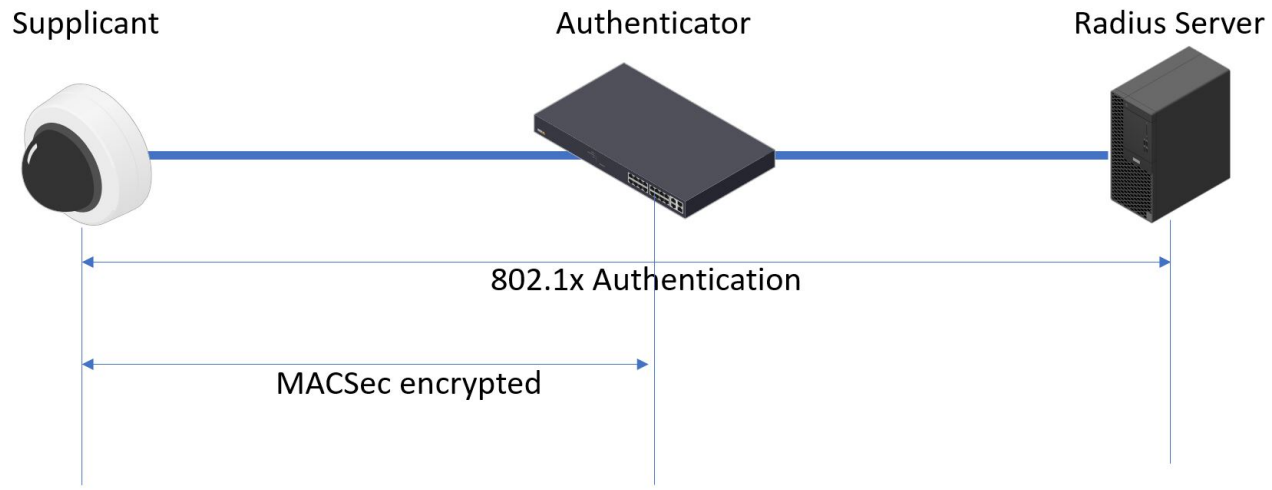
help.axis.com/?&piaId=&section=secure-network-operation-ieee-802-1ae-macsec

Zero-Trust-Netzwerkverschlüsselung mit Sicherheitsstufe IEEE 802.1AE IEEECsec 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



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 Netzwerk (4, 5) durch IEEE 802.1X portbasierte EAP-TLS-Netzwerkzugriffskontrolle (2) verwendet. Über die EAP-TLS-Sitzung werden

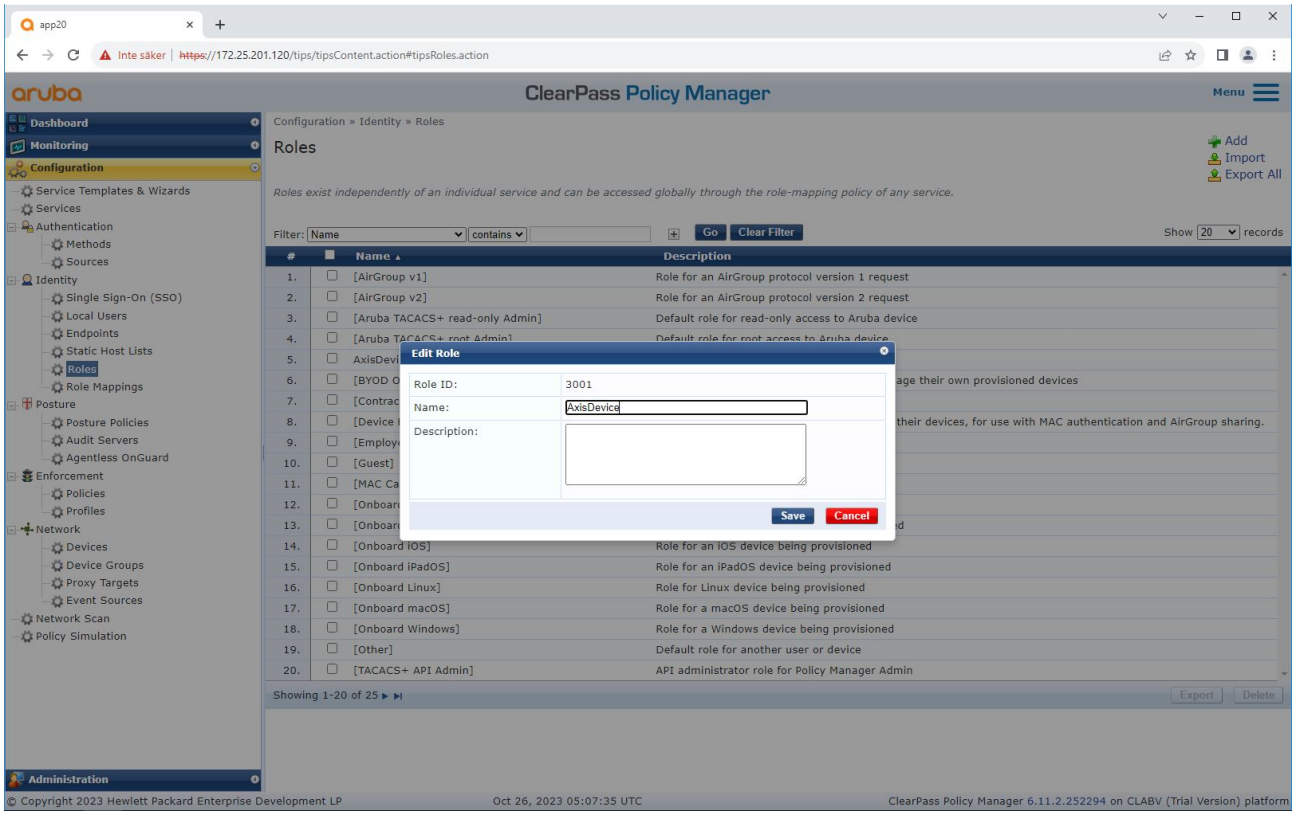
MACsec-Schlüssel automatisch ausgetauscht, um eine sichere Verbindung einzurichten (3), die den gesamten Netzwerkverkehr vom Axis Gerät zum HPE Aruba Netzwerk-Switch schützt.

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.

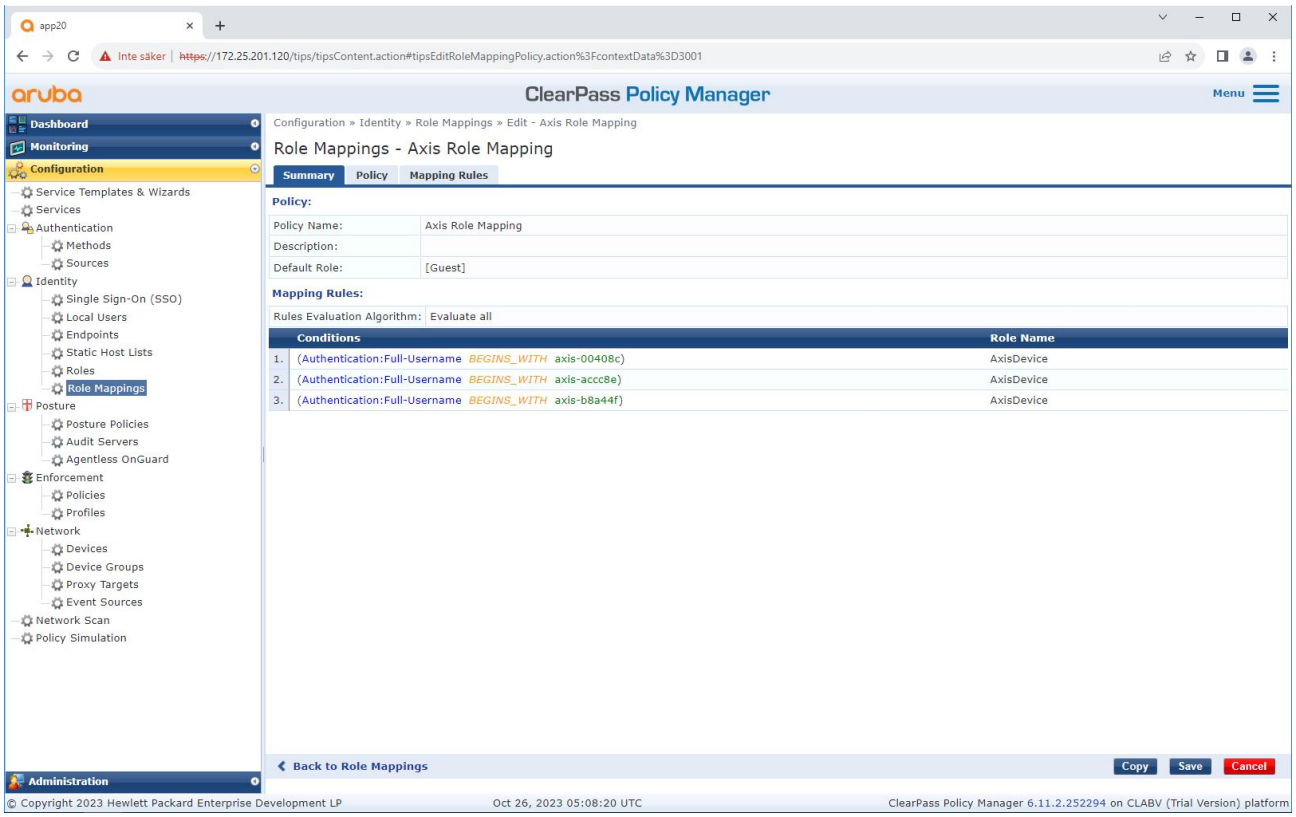
Wenn der HPE Aruba Netzwerk-Zugangsschalter MACsec mit EAP-TLS nicht unterstützt, kann der Pre-Shared Key-Modus verwendet und manuell konfiguriert werden.

HPE Aruba Networking ClearPass Policy Manager

Rollen- und Rollenzuordnungsrichtlinie



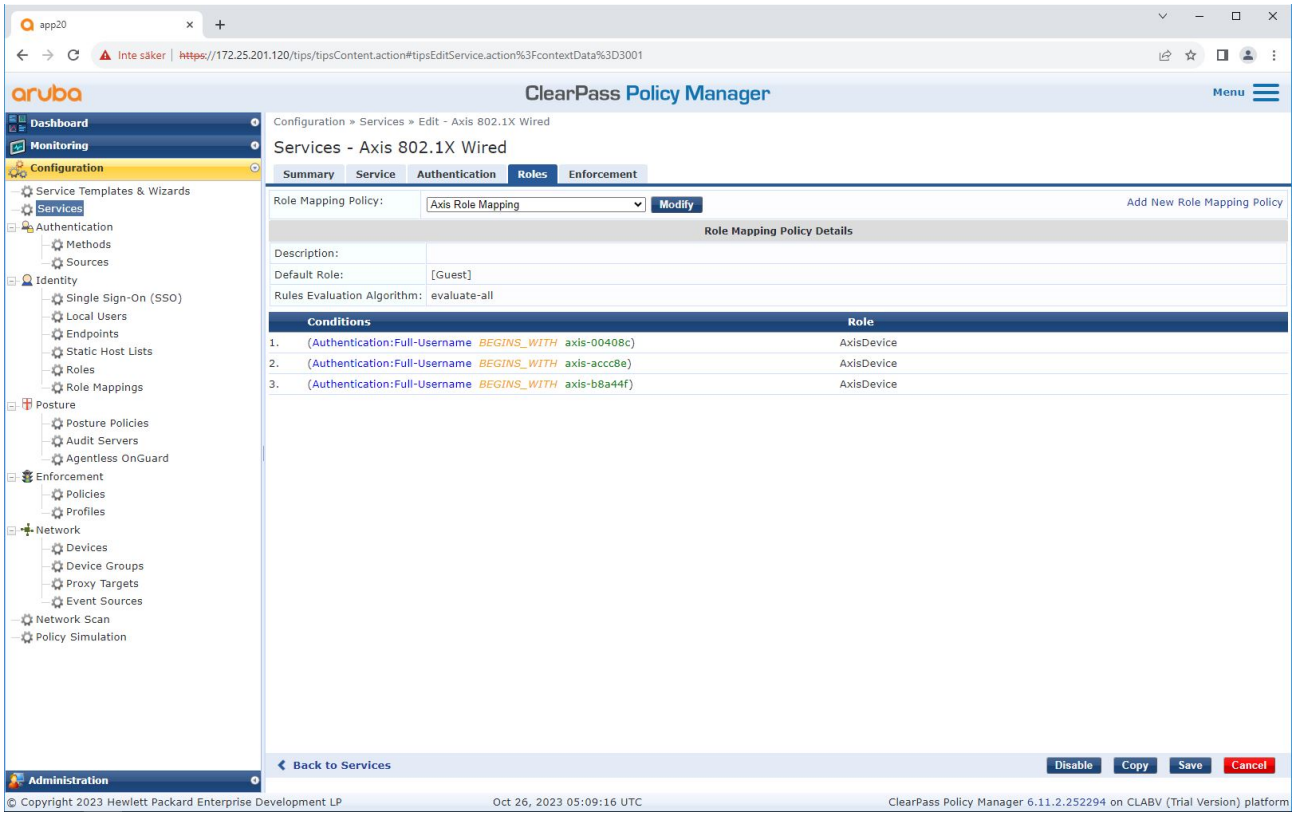
Hinzufügen eines Rollennamens für Axis Geräte. Der Name ist der Name der Port-Zugriffsrolle in der Zugangsschalter-Konfiguration.



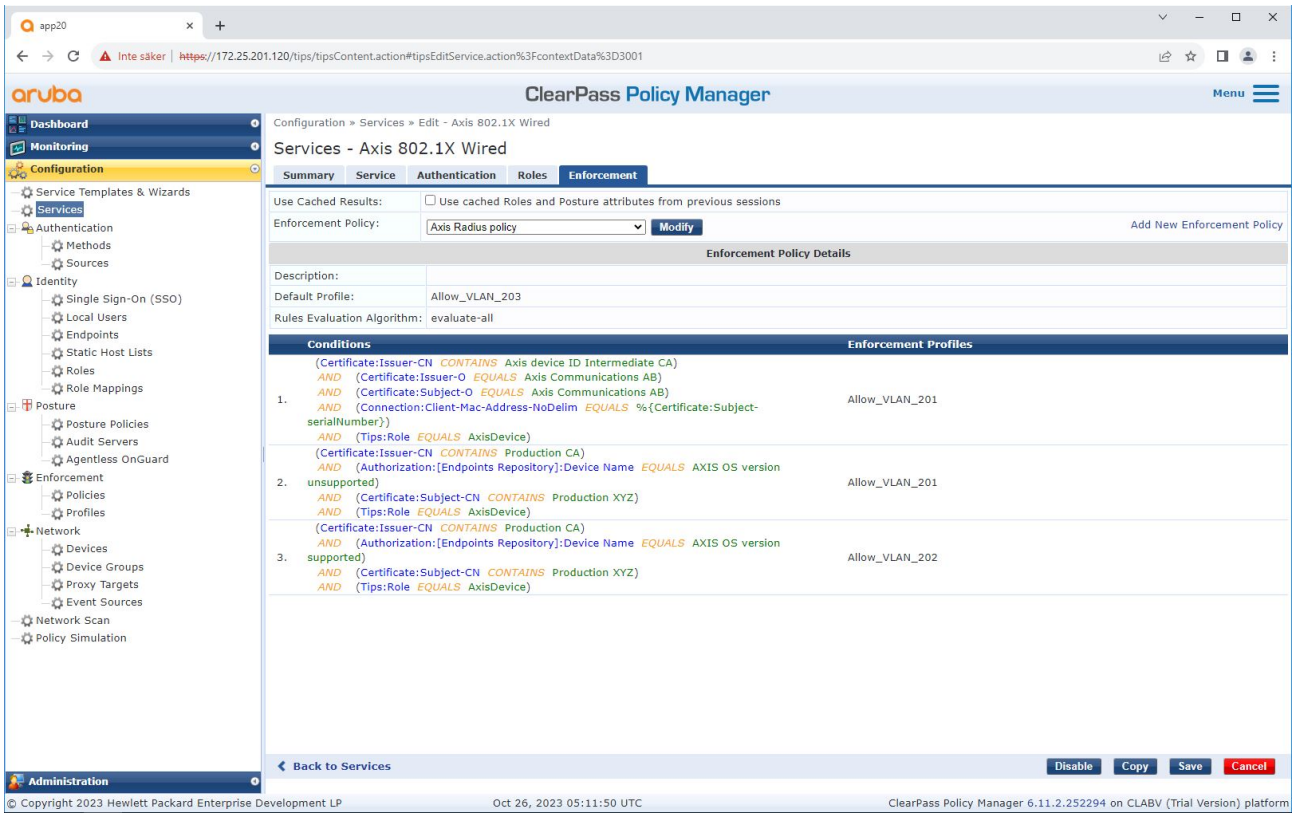
Hinzufügen einer Axis Rollenzuordnungsrichtlinie für die zuvor erstellte Axis Geräterolle. Die definierten Bedingungen sind erforderlich, damit ein Gerät der Axis Geräterolle zugeordnet werden kann. Wenn die Bedingungen nicht erfüllt sind, wird das Gerät Teil der Rolle [Gast] sein.

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

Servicekonfiguration

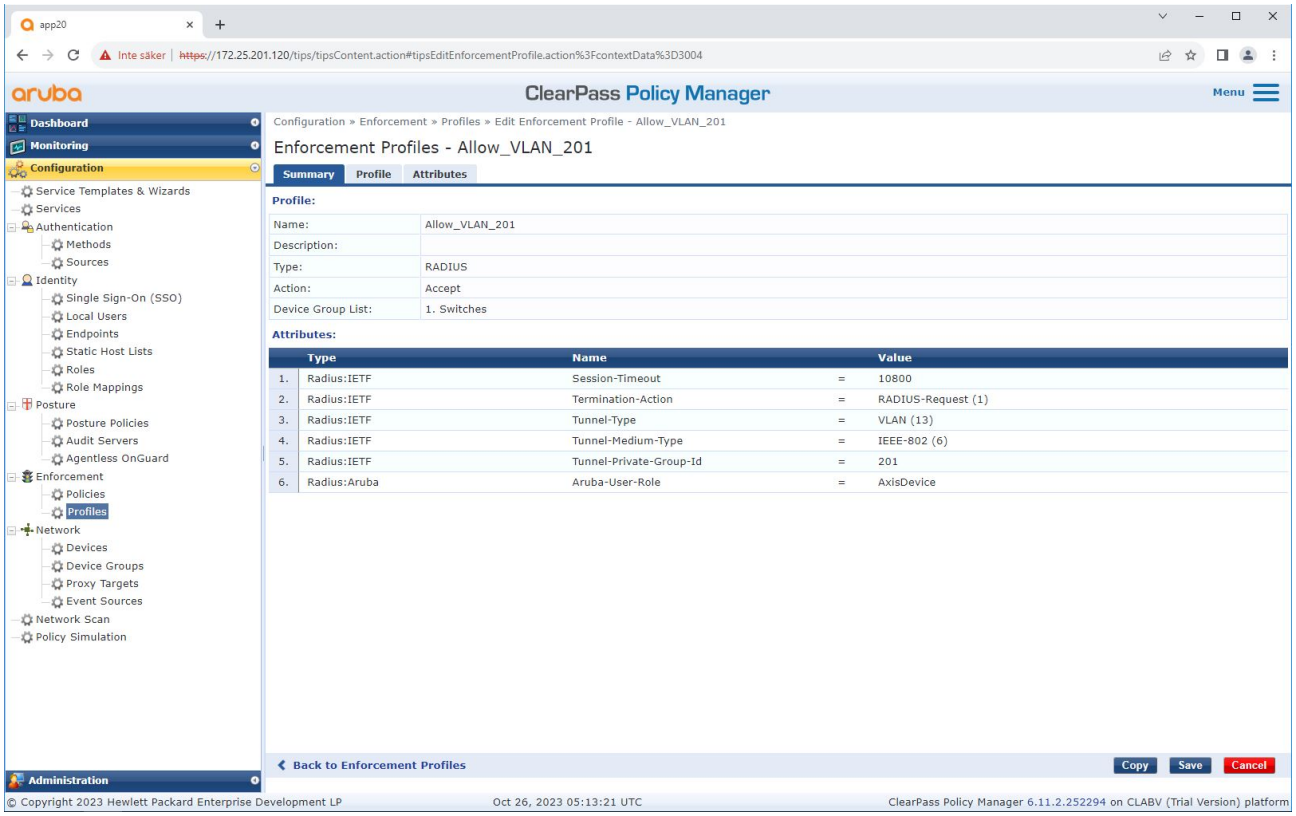


Hinzufügen der zuvor erstellten Axis Rollenzuordnungsrichtlinie zum Dienst, der IEEE 802.1X als Verbindungsmethode für die Einbindung von Axis Geräten definiert.



Hinzufügen des Axis Rollennamens als Bedingung zu den vorhandenen Richtliniendefinitionen.

Durchsetzungsprofil



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

HPE Aruba Networking Zugangsschalter

Zusätzlich zur sicheren Onboarding-Konfiguration, die in *HPE Aruba Networking Zugangsschalter auf Seite 16* beschrieben wird, finden Sie weitere Informationen in der folgenden Beispiel-Portkonfiguration für den zu konfigurierenden HPE Aruba Netzwerk-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
mkacak-length 16
enable
```

Legacy-Onboarding – MAC-Authentifizierung

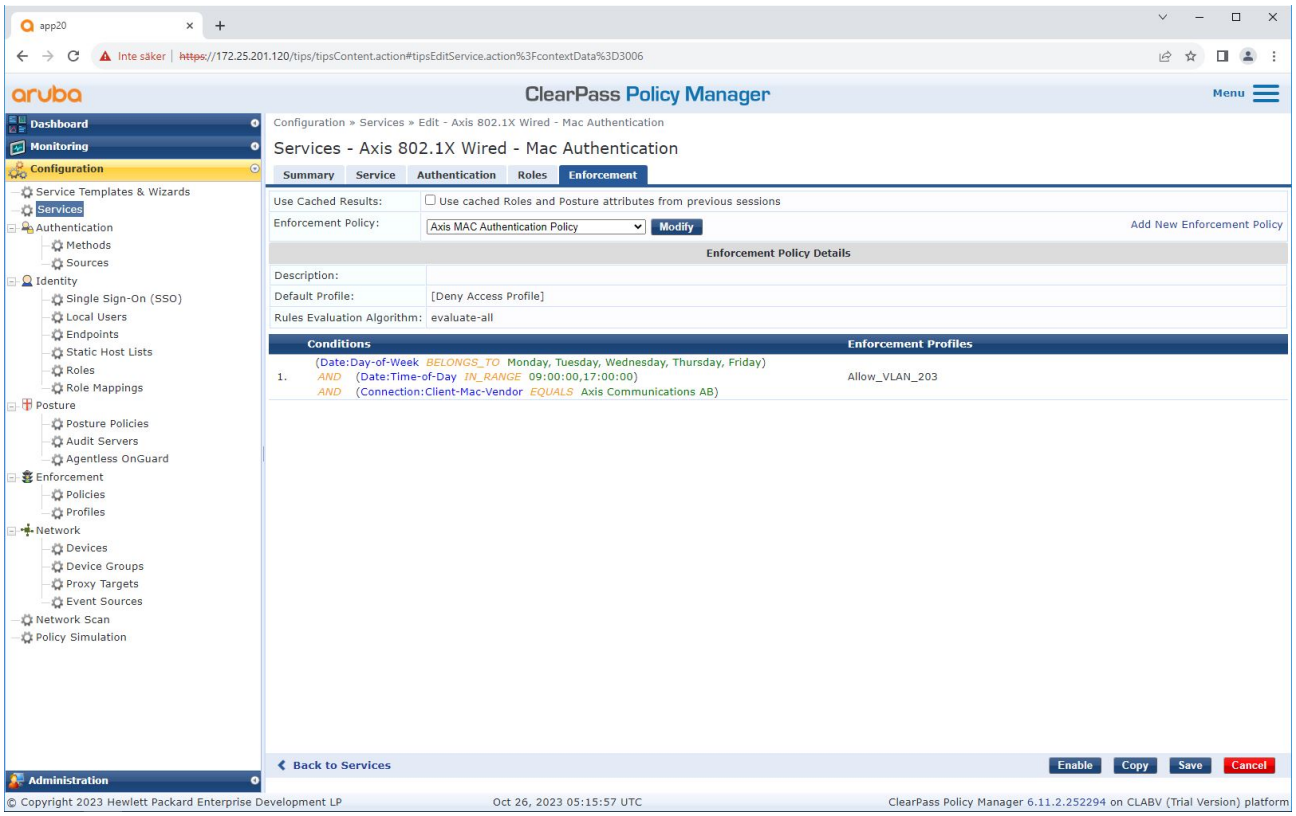
Sie können MAC Authentifizierungs-Bypass (MAB) verwenden, um Axis Geräte einzubinden, die IEEE 802.1AR Onboarding mit dem Axis Geräte-ID-Zertifikat und im Werkszustand aktiviertem IEEE 802.1X nicht unterstützen. Wenn die 802.1X-Einbindung fehlschlägt, validiert ClearPass Policy Manager die MAC Adresse 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. Auf dem Axis Gerät ist keine Konfiguration erforderlich, um MAB für die Einbindung zu ermöglichen.

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.



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:

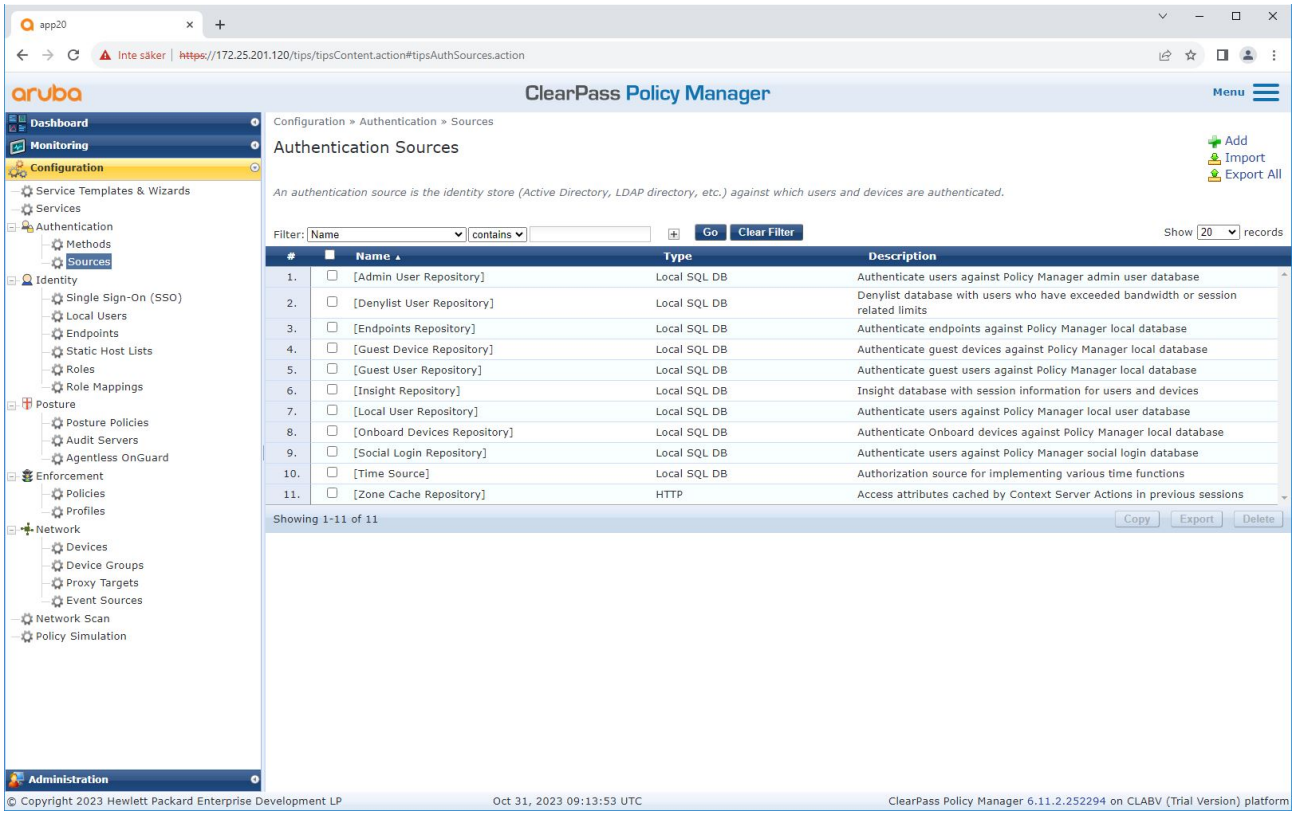
- Es ist ein Wochentag zwischen Montag und Freitag
- Es ist zwischen 09:00 und 17:00 Uhr

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

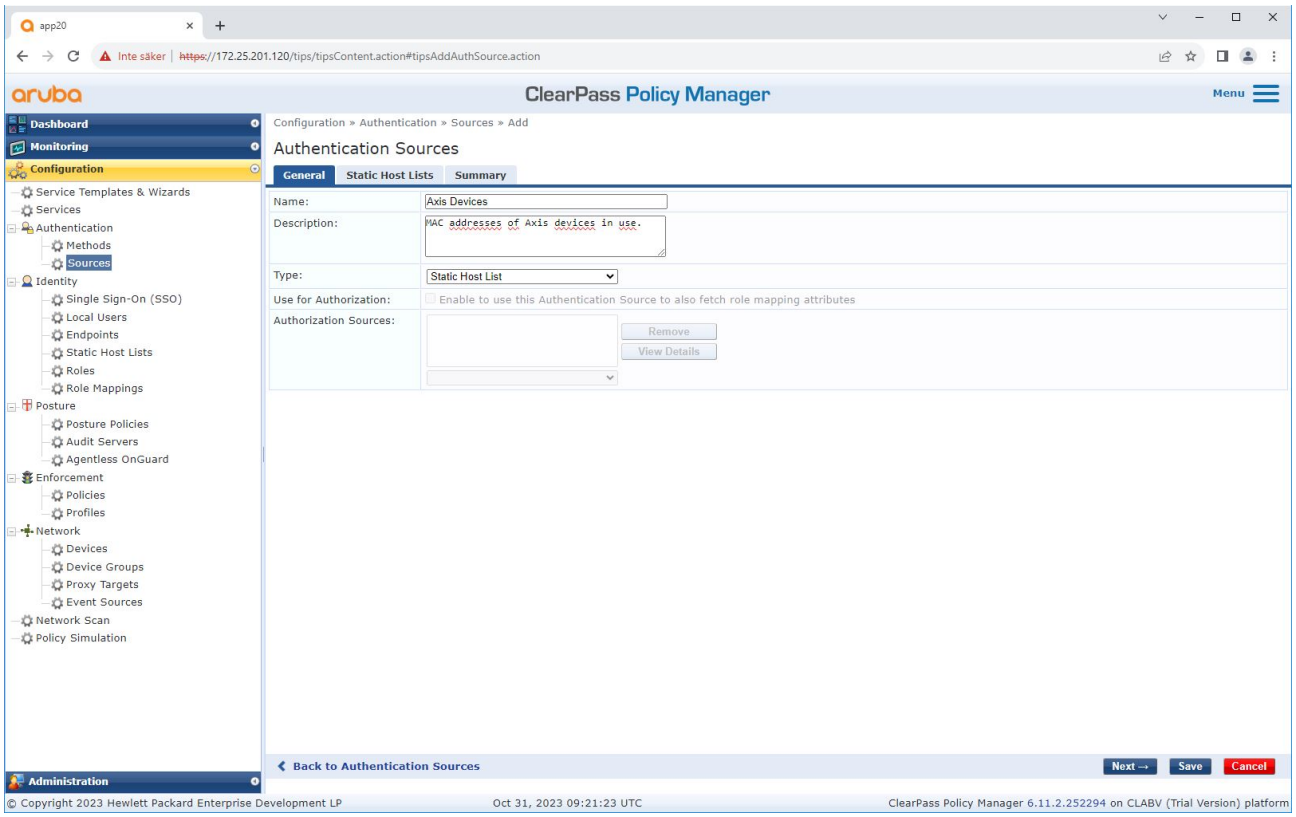
Da MAC Adressen gefälscht werden können, wird kein Zugriff auf das reguläre Bereitstellungsnetzwerk gewährt. Wir empfehlen, dass Sie MAB nur für das erste Onboarding und zur weiteren manuellen Überprüfung des Geräts verwenden.

Quellenkonfiguration

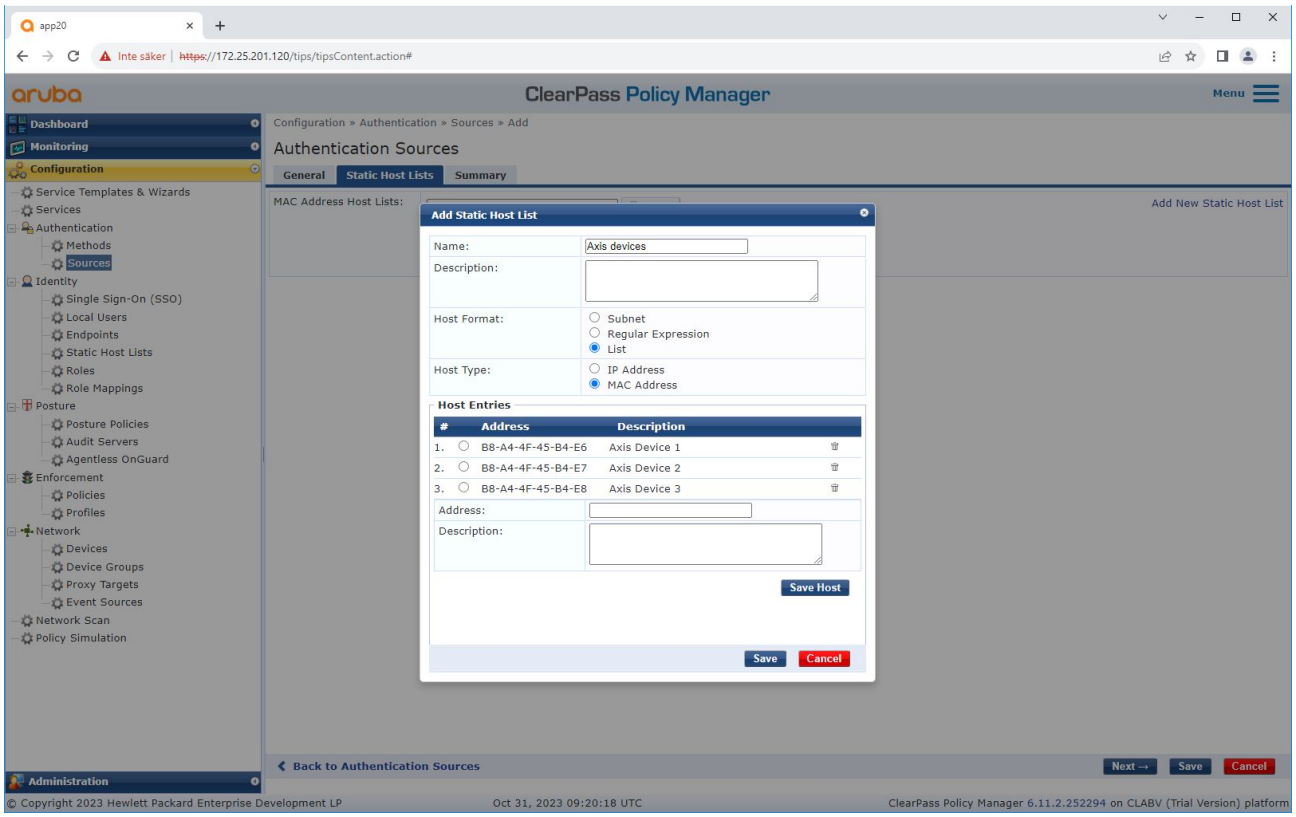
Auf der Seite **Sources (Quellen)** wird eine neue Authentifizierungsquelle erstellt, um nur manuell importierte MAC Adressen zuzulassen.



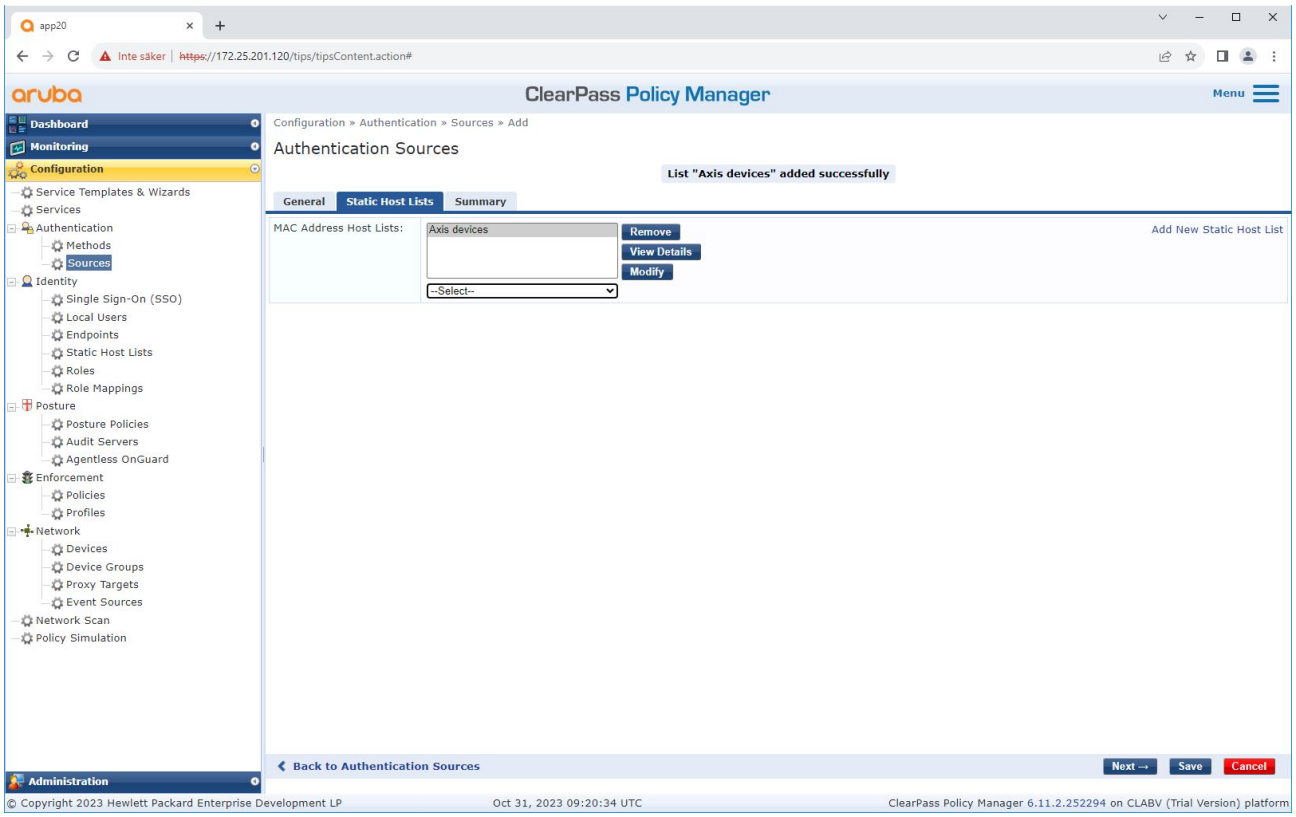
Legacy-Onboarding – MAC-Authentifizierung



Legacy-Onboarding – MAC-Authentifizierung



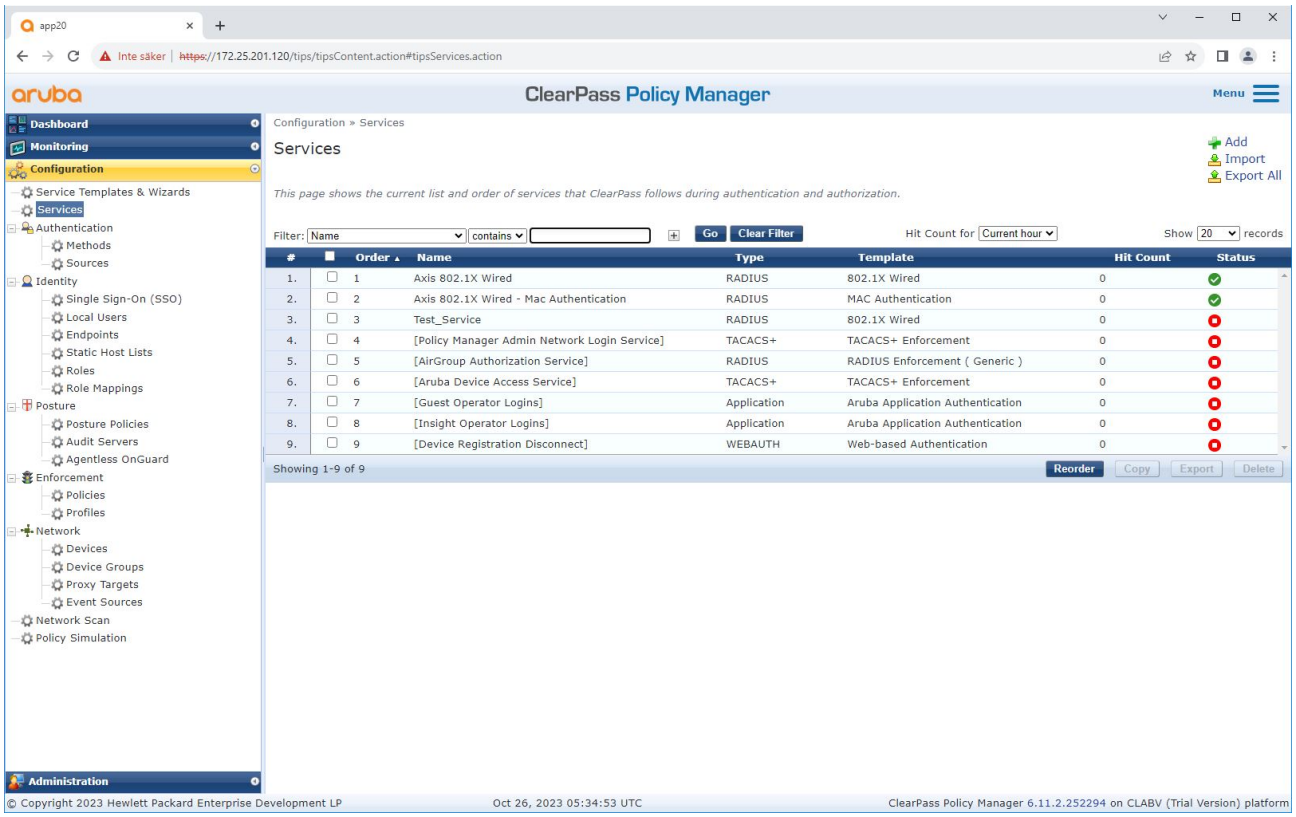
Es wird eine statische Hostliste erstellt, die Axis MAC Adressen enthält.



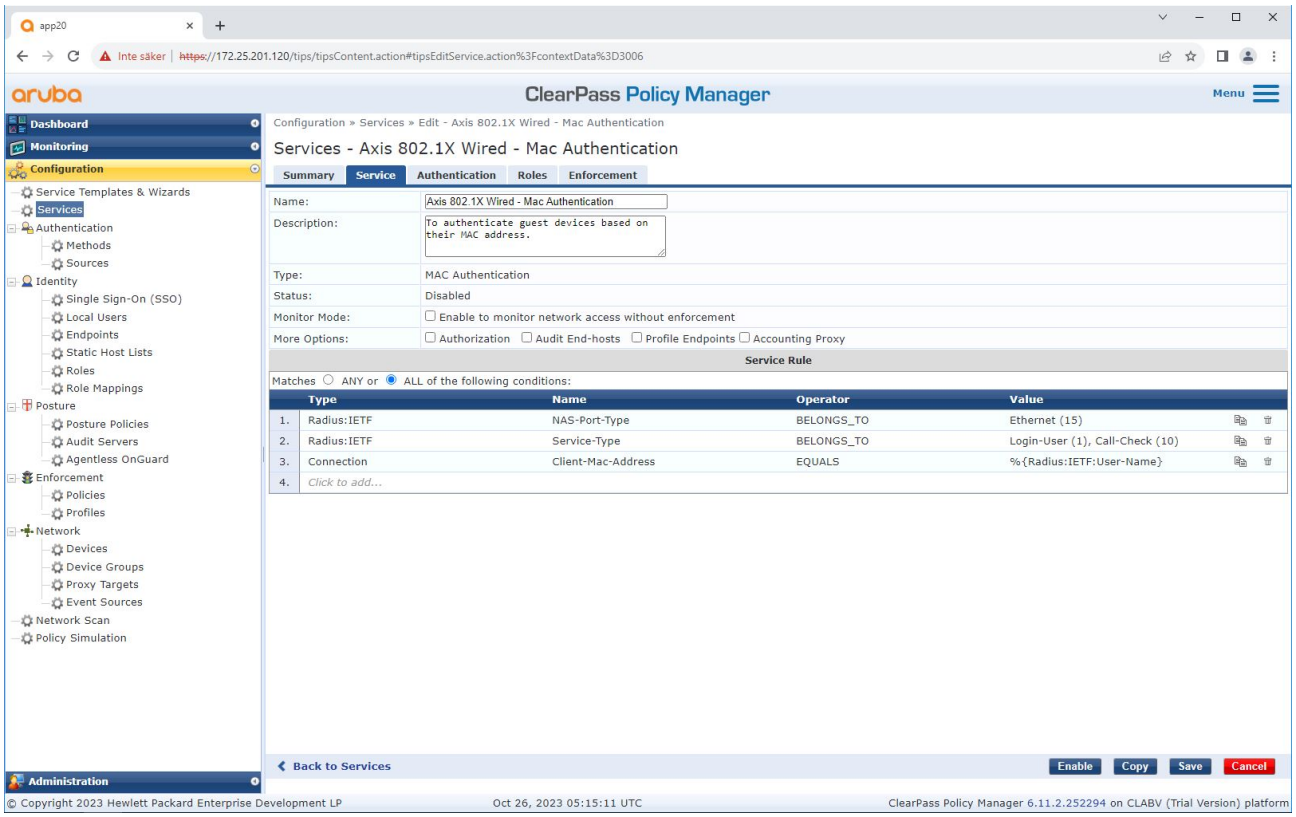
Servicekonfiguration

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

Legacy-Onboarding – MAC-Authentifizierung

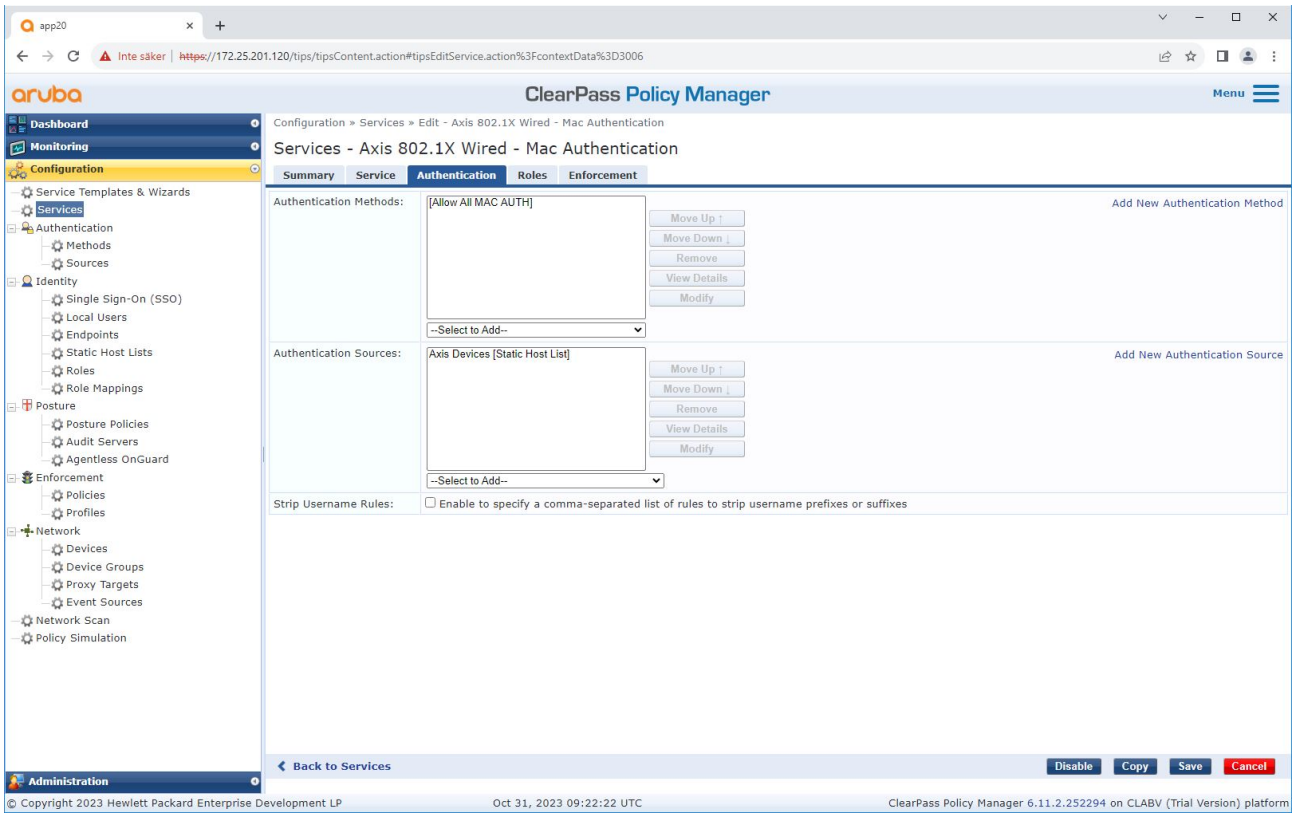


Legacy-Onboarding – MAC-Authentifizierung



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

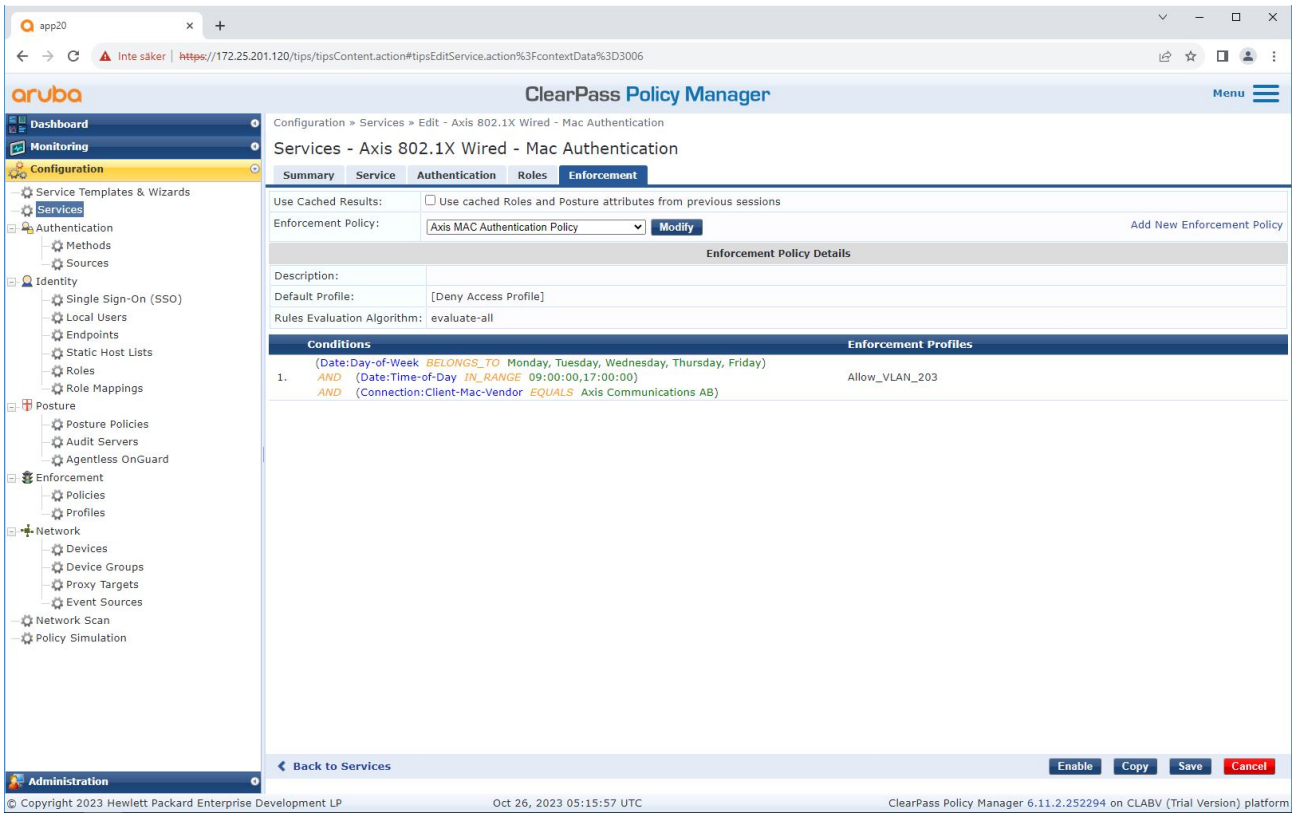
Legacy-Onboarding – MAC-Authentifizierung



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 verwendet die folgenden MAC Adressen-OUIs:

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



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

HPE Aruba Networking Zugangsschalter

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

Integrationsanleitung
HPE Aruba Networking

Vers. M6.2
Datum: Mai 2024
Teil-Nr. T10197992