HPE Aruba Networking

Benutzerhandbuch

Inhalt

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.

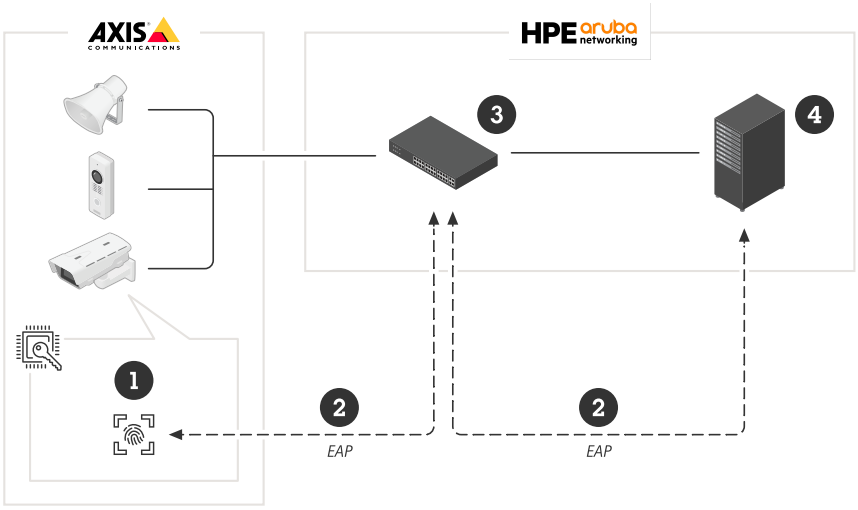
Sicheres Onboarding von Geräten in vertrauenswürdigen Netzwerken mit IEEE 802.1X/802.1AR

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.

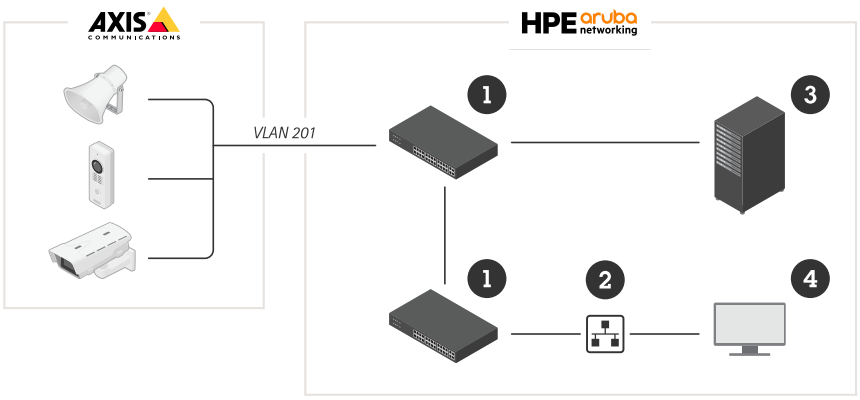


Das Axis Gerät authentifiziert sich im HPE Aruba Networking-Netzwerk mithilfe des IEEE 802.1AR-konformen Axis Geräte-ID-Zertifikats.

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.

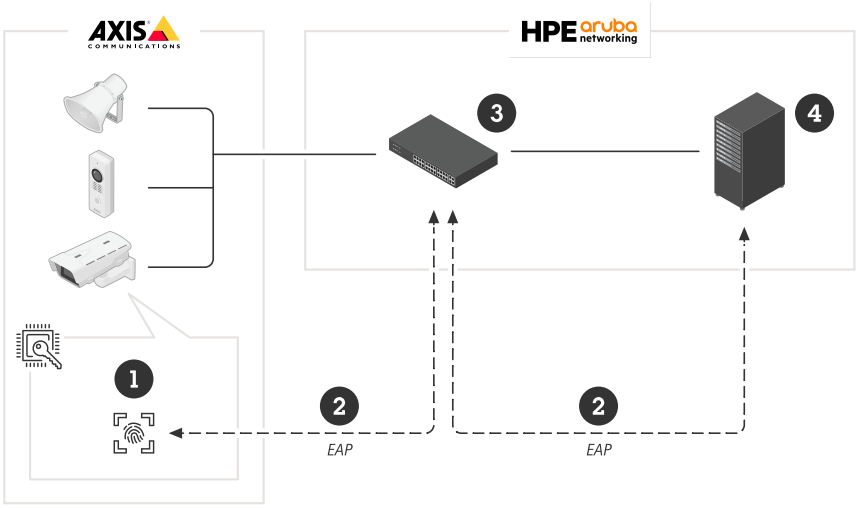


Nach erfolgreicher Authentifizierung wird das Axis Gerät zur Konfiguration in ein Bereitstellungsnetzwerk verschoben.

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

Produktionsnetzwerk

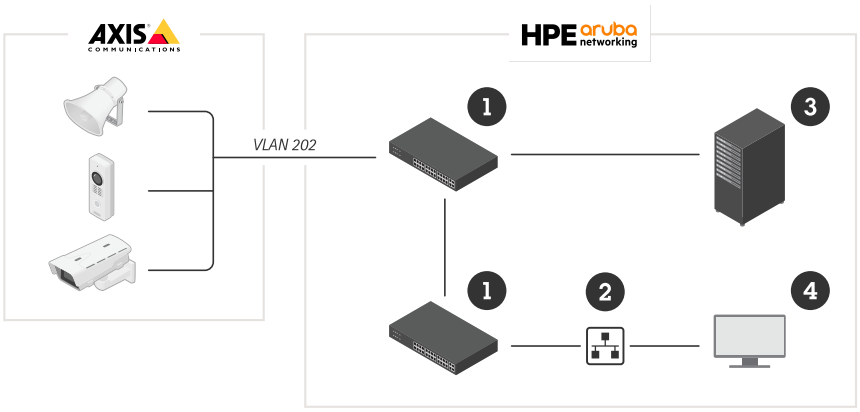
Die Bereitstellung des Axis Geräts mit neuen IEEE 802.1X-Zertifikaten löst einen neuen Authentifizierungsversuch aus. Der ClearPass Policy Manager überprüft die neuen Zertifikate und entscheidet, ob das Axis Gerät in das Produktionsnetzwerk verschoben wird oder nicht.



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*

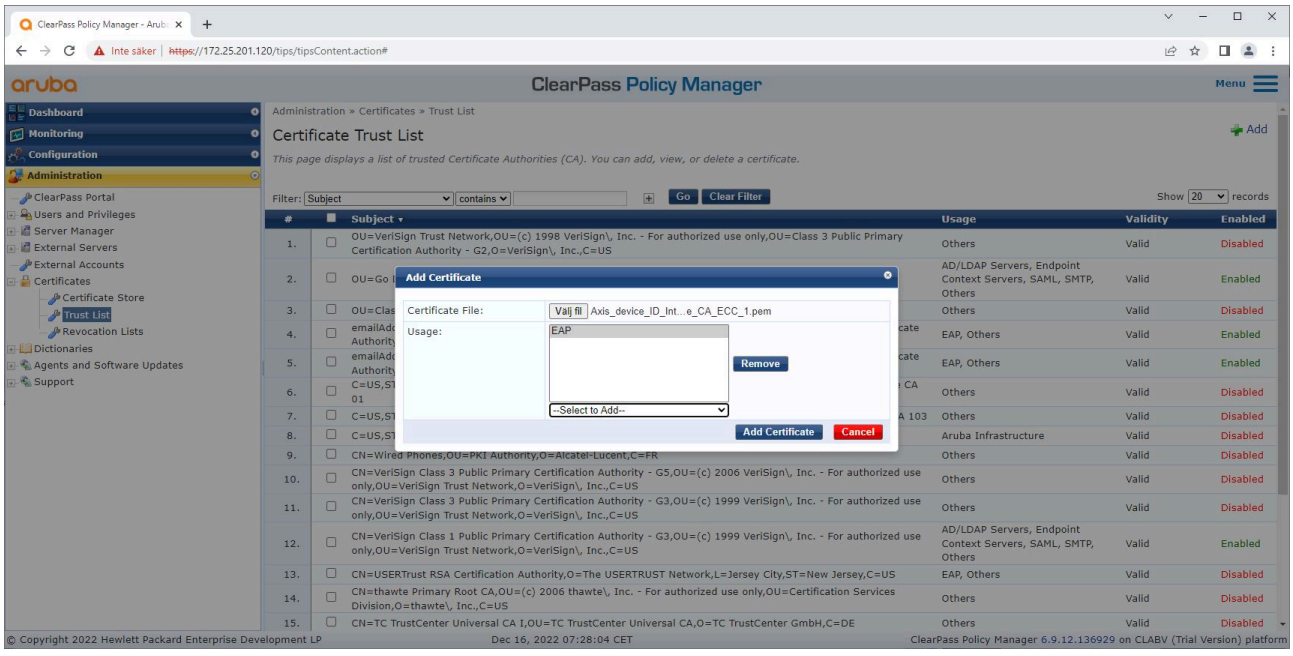
Konfiguration von HPE Aruba Networking

HPE Aruba Networking ClearPass Policy Manager

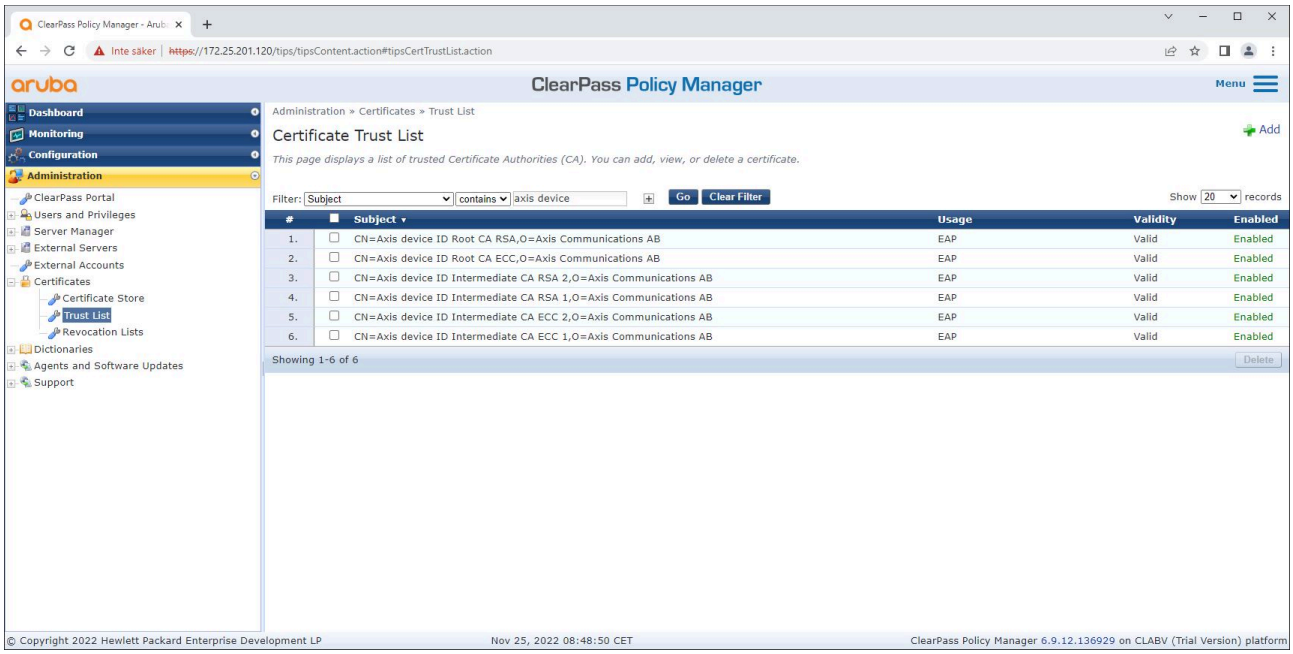
Der ClearPass Policy Manager bietet die rollen- und gerätebasierte sichere Netzwerkzugriffssteuerung für IoT, BYOD, Unternehmensgeräte, Beschäftigte, Auftragnehmer und Gäste in der kabelgebundenen, kabellosen und VPN-Infrastruktur mehrerer Anbieter.

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.



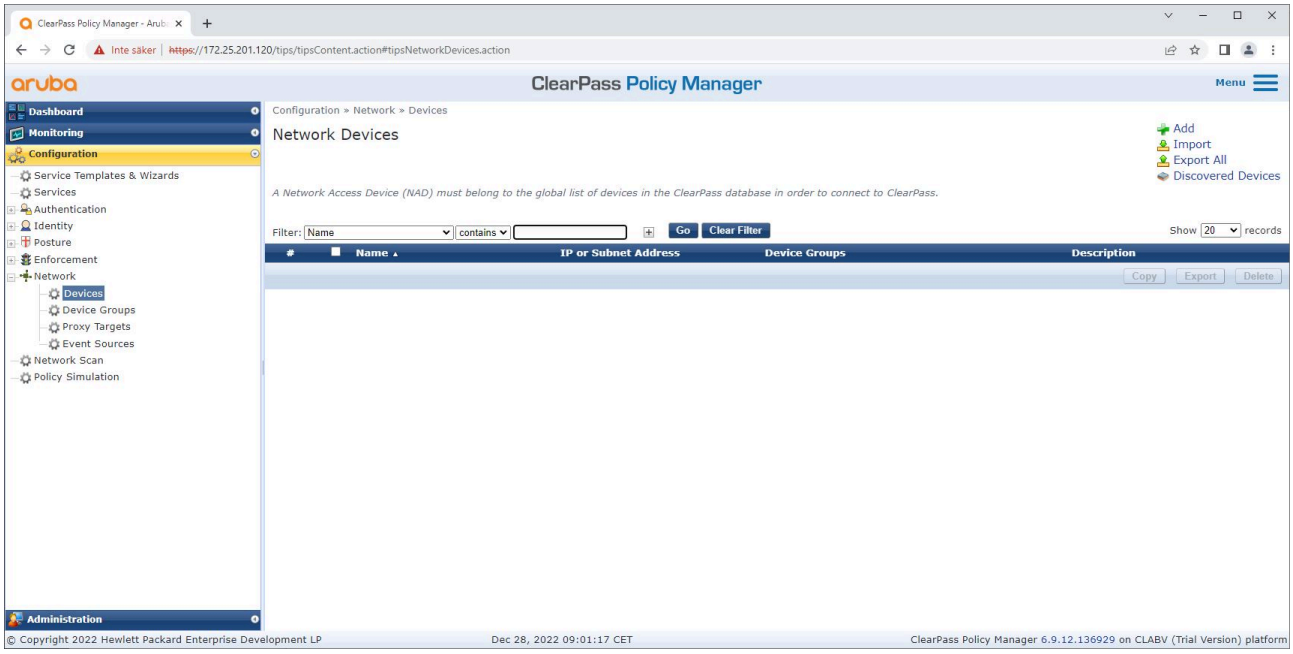
Hochladen der für Axis spezifischen IEEE 802.1AR-Zertifikate in den vertrauenswürdigen Zertifikatspeicher des ClearPass Policy Managers.



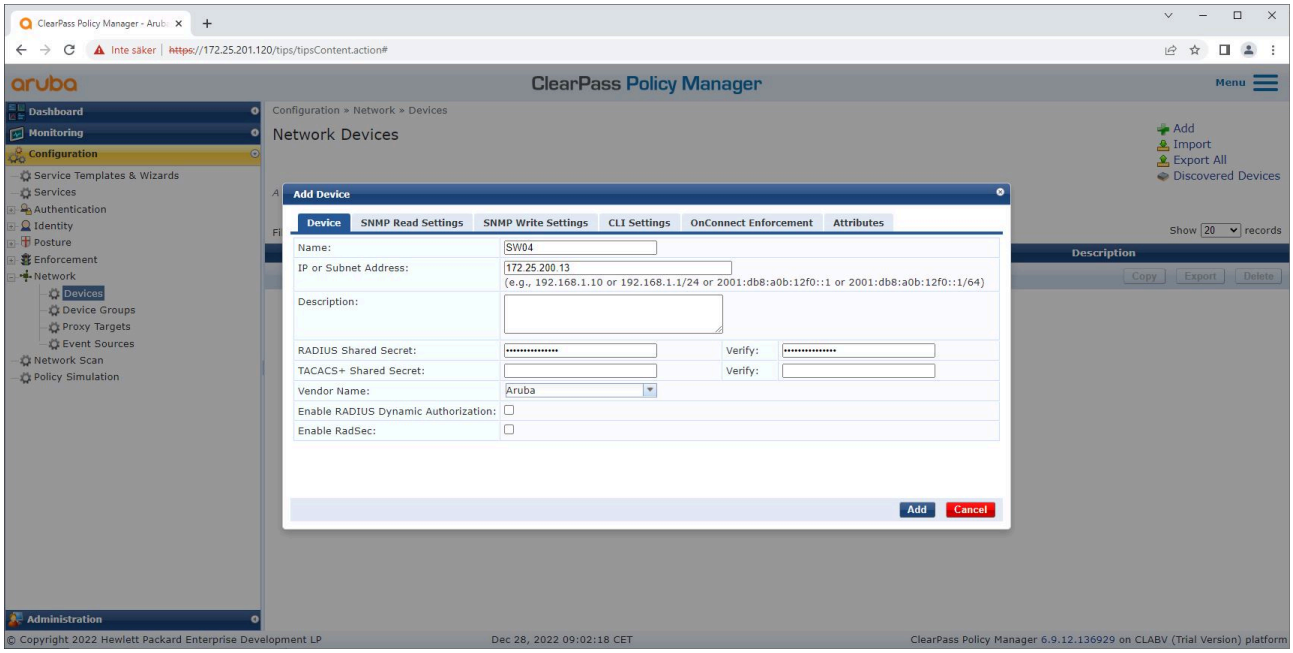
Der vertrauenswürdige Zertifikatsspeicher im ClearPass Policy Manager mit für Axis spezifischer IEEE 802.1AR-Zertifikatskette.

Netzwerkgeräte-/Gruppenkonfiguration

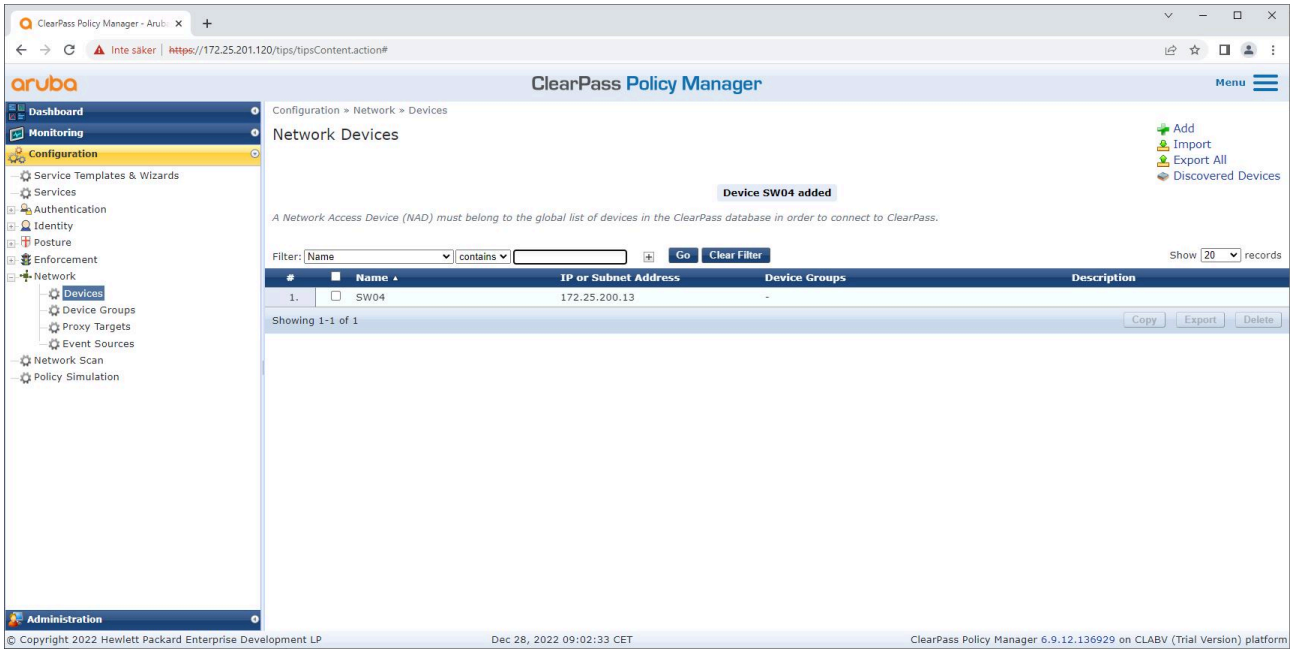
1. Fügen Sie dem ClearPass Policy Manager vertrauenswürdige Netzwerkzugriffsgeräte wie HPE Aruba Netzwerk Access Switches hinzu. Der ClearPass Policy Manager muss wissen, welche Access Switches im Netzwerk für die IEEE 802.1X-Kommunikation verwendet werden. Zusätzlich muss das gemeinsame RADIUS-Geheimnis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



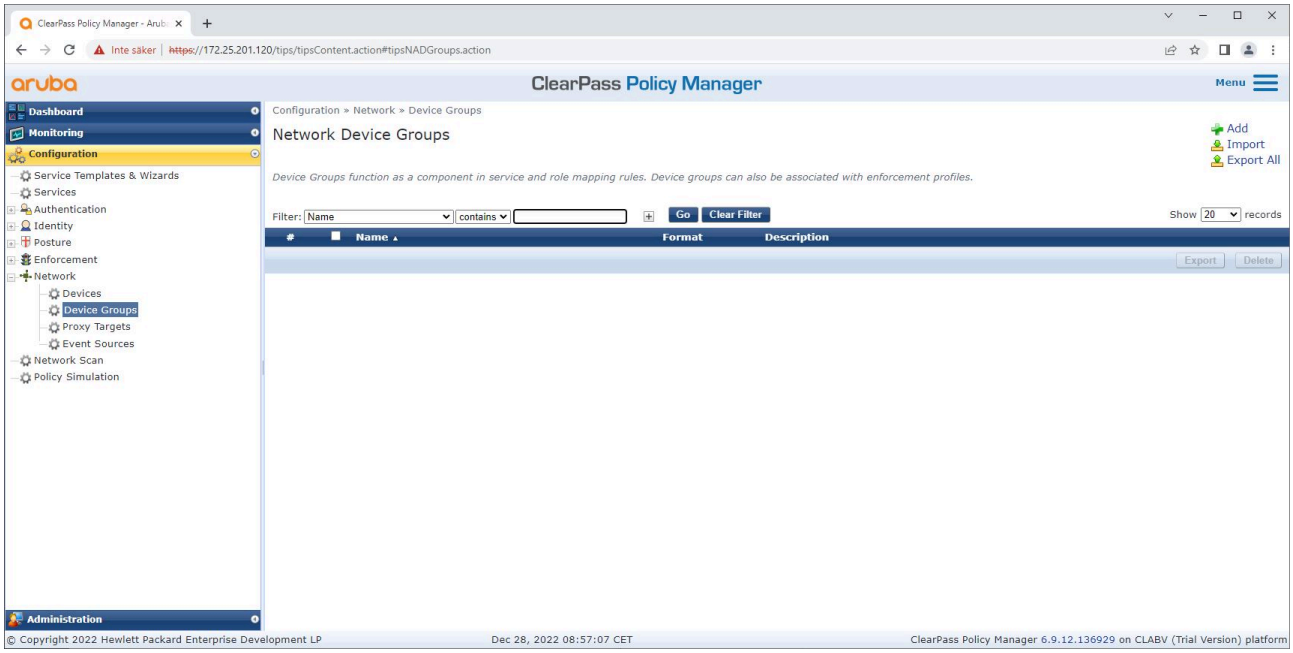
Die Schnittstelle für vertrauenswürdige Netzwerkgeräte im ClearPass Policy Manager.



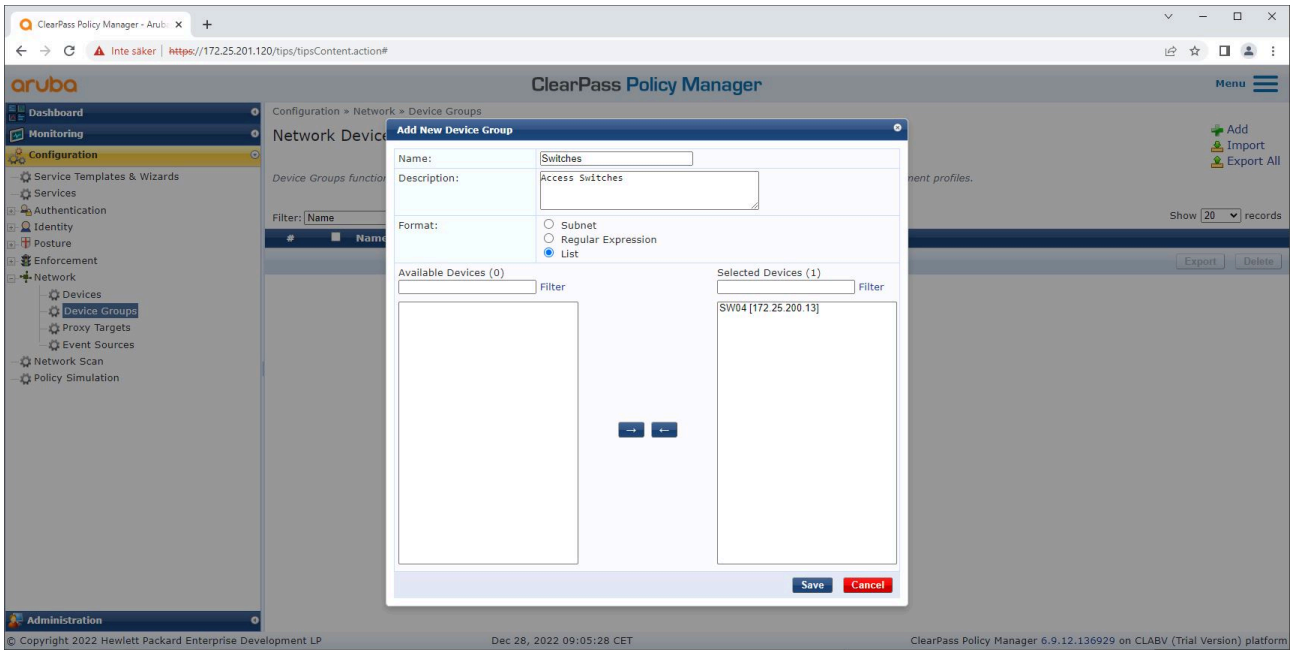
Hinzufügen des HPE Aruba Networking-Zugangsschalters als vertrauenswürdiges Gerät im ClearPass Policy Manager. Bitte beachten Sie, dass das gemeinsame RADIUS-Geheimnis mit der spezifischen IEEE 802.1X-Konfiguration des Switches übereinstimmen muss.



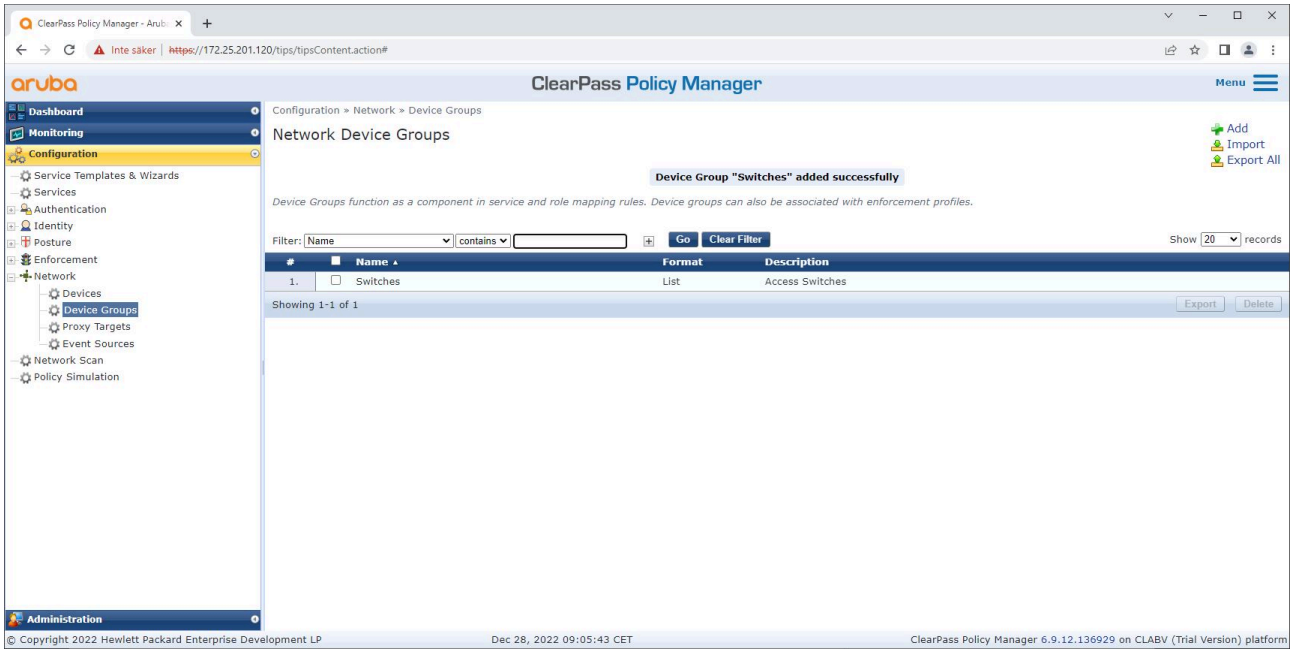
Der ClearPass Policy Manager mit einem konfigurierten vertrauenswürdigen Netzwerkgerät.



Die Schnittstelle für vertrauenswürdige Netzwerkgerätegruppen im ClearPass Policy Manager.



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

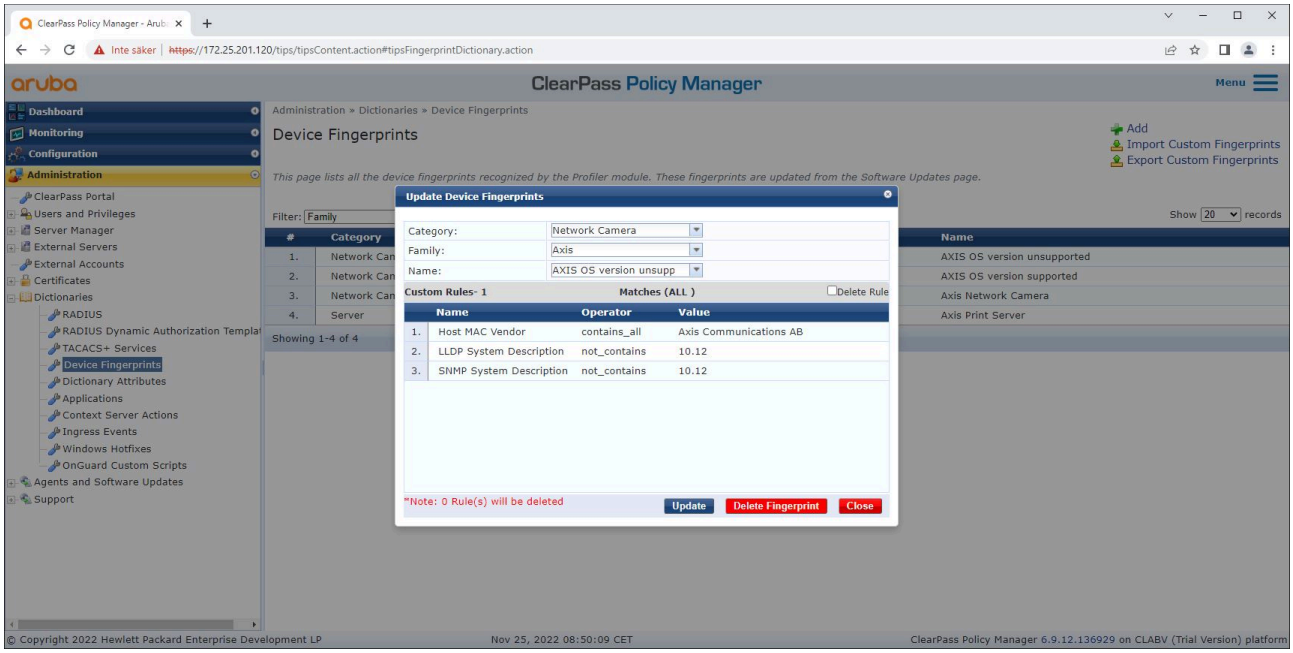


ClearPass Policy Manager mit konfigurierter Netzwerkgerätegruppe, die ein oder mehrere vertrauenswürdige Netzwerkgeräte umfasst.

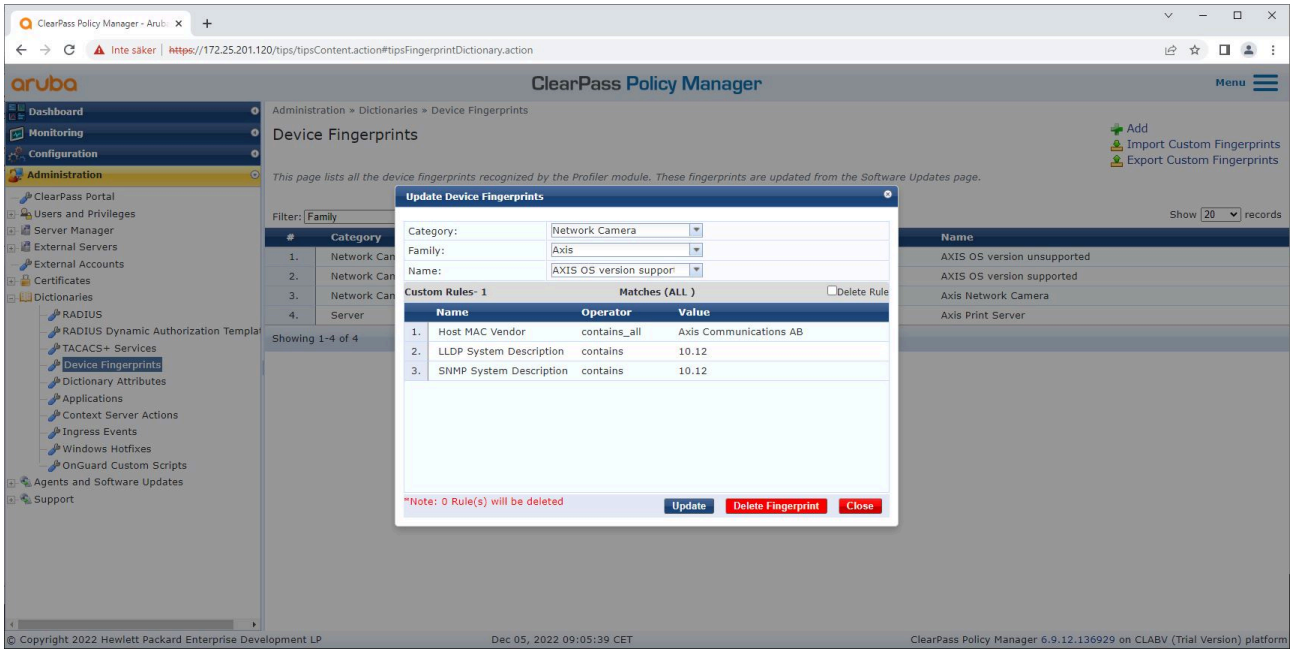
Konfiguration des Gerätefingerabdrucks

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.



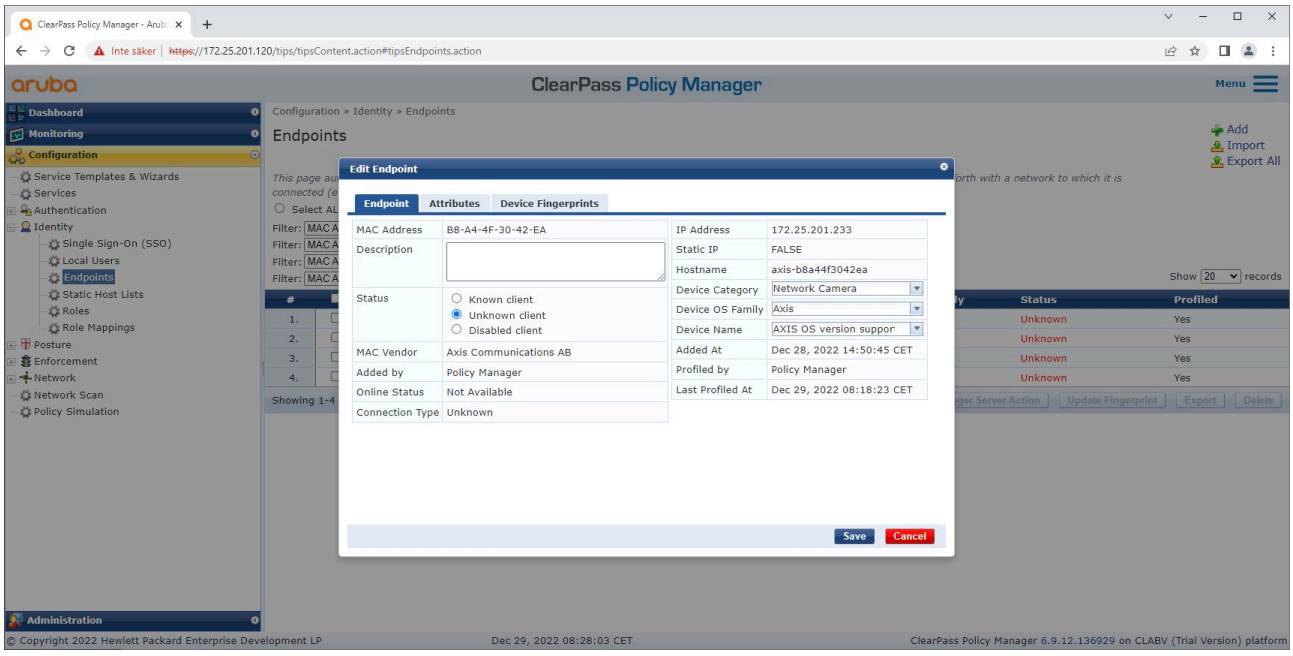
Die Konfiguration des Gerätefingerabdrucks im ClearPass Policy Manager. Axis Geräte, die andere AXIS OS-Versionen als 10.12 verwenden, werden in diesem Beispiel unterstützt.

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

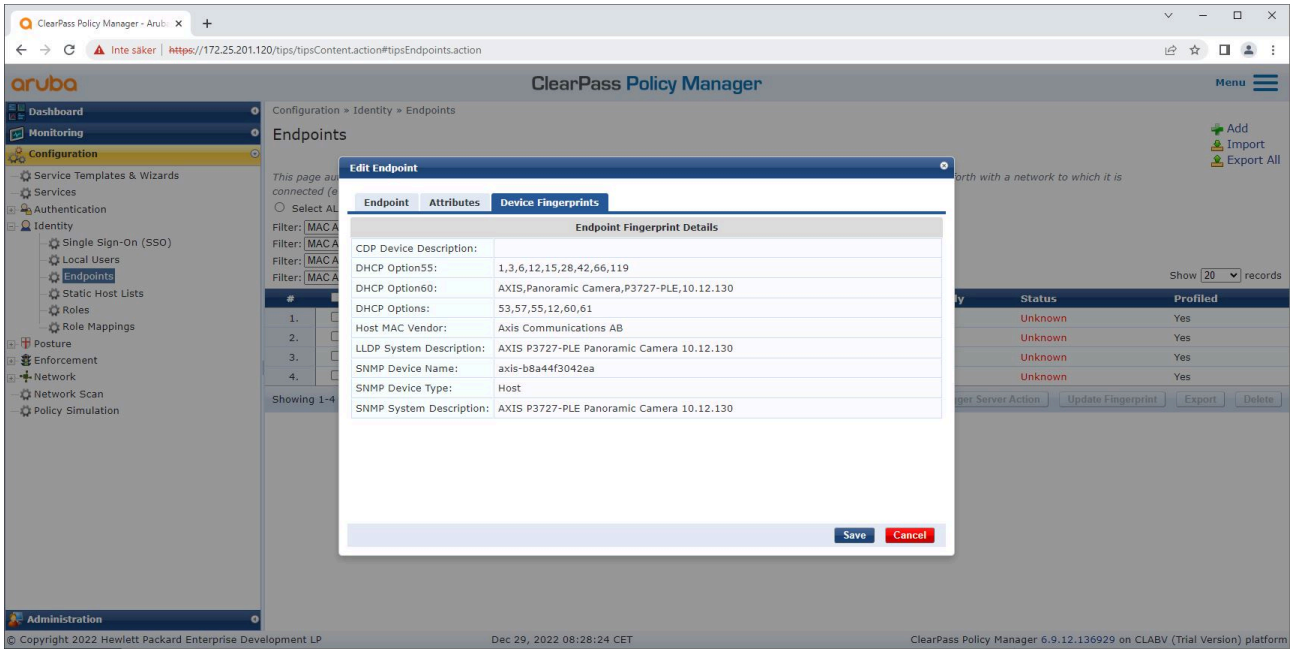
1. Gehen Sie zu **Configuration > Identity > Endpoints (Konfiguration > Identität > Endpunkte)**.
2. Wählen Sie das Gerät, das Sie ansehen möchten.
3. Klicken Sie auf die Registerkarte **Device Fingerprints (Gerätefingerabdrücke)**.

Hinweis

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



Ein von ClearPass Policy Manager profiliertes Axis Gerät.

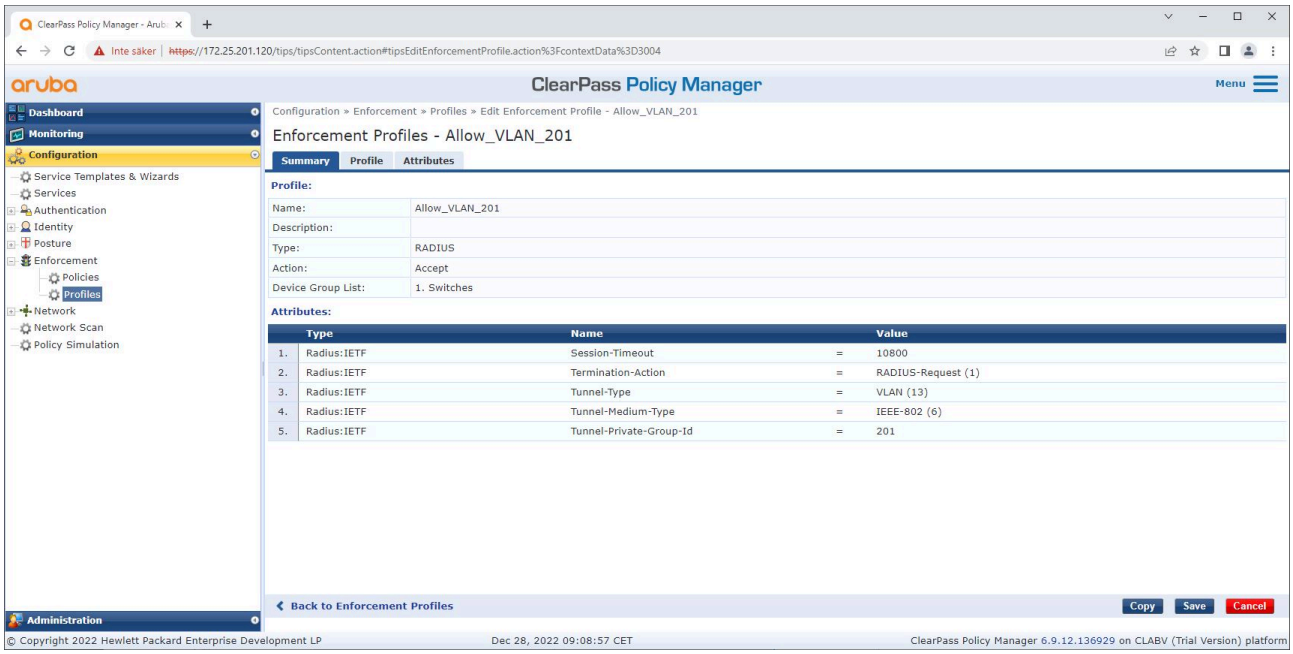


Die detaillierten Gerätefingerabdrücke eines profilierten Axis Geräts. Bitte beachten Sie, dass SNMP in Axis Geräten standardmäßig deaktiviert ist. LLDP-, CDP- und DHCP-spezifische Erkennungsinformationen werden vom Axis Gerät in der werksseitigen Standardeinstellung weitergegeben und vom HPE Aruba Networking-Zugangsschalter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

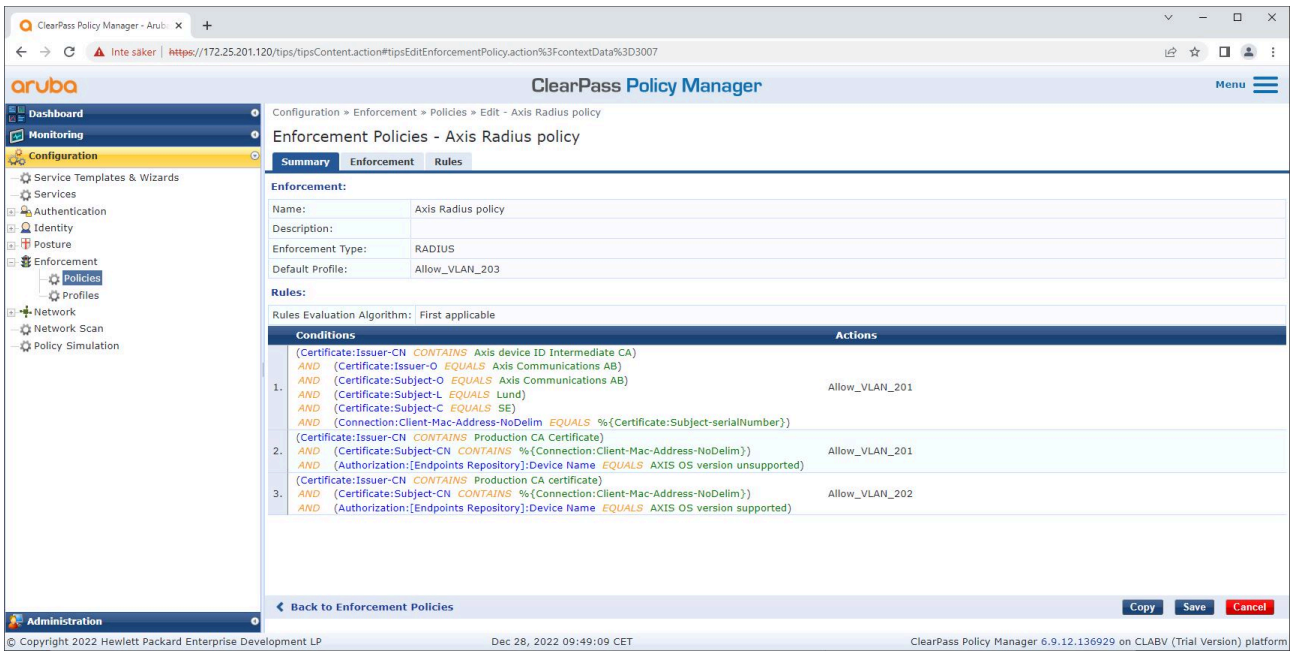
Konfiguration des Durchsetzungsprofils

Das Durchsetzungsprofil gestattet es dem ClearPass Policy Manager, einem Zugriffsport 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.

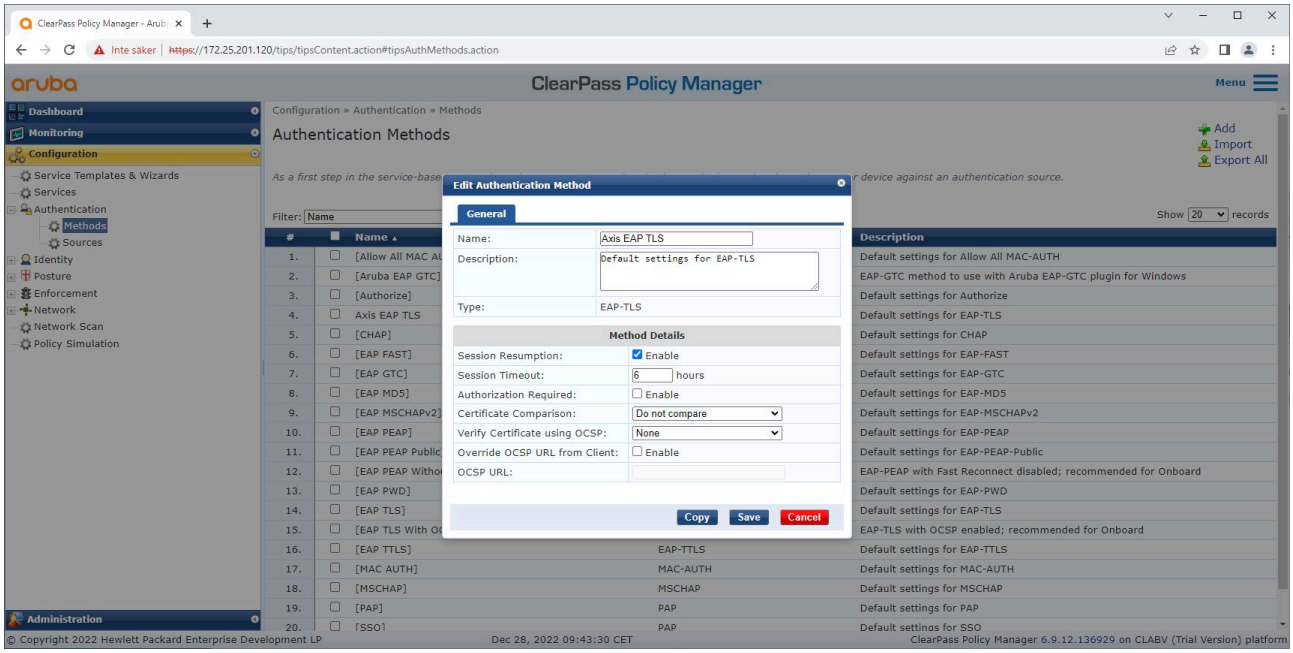
Produktionsnetzwerk (VLAN 202)

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

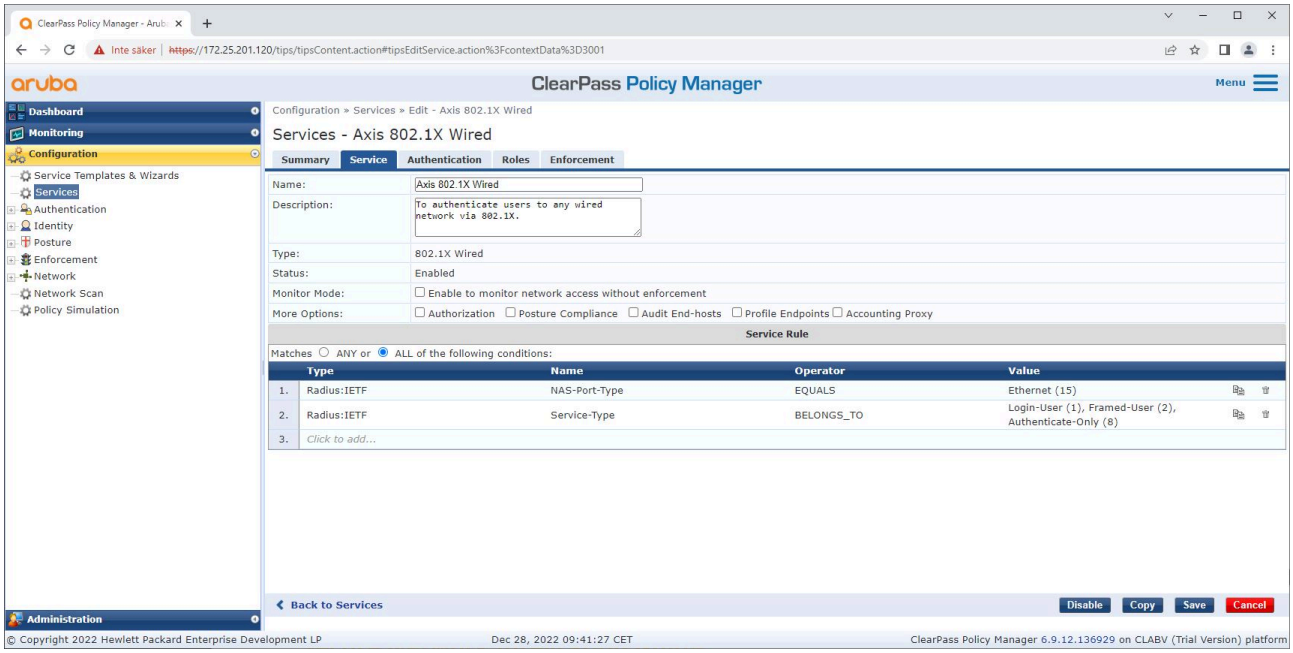
Die Authentifizierungsmethode gibt vor, wie ein Axis Gerät versucht, sich im Netzwerk zu authentifizieren. Die bevorzugte Methode ist IEEE 802.1X EAP-TLS, da bei Axis Geräten mit Axis Edge Vault standardmäßig IEEE 802.1X EAP-TLS aktiviert ist.



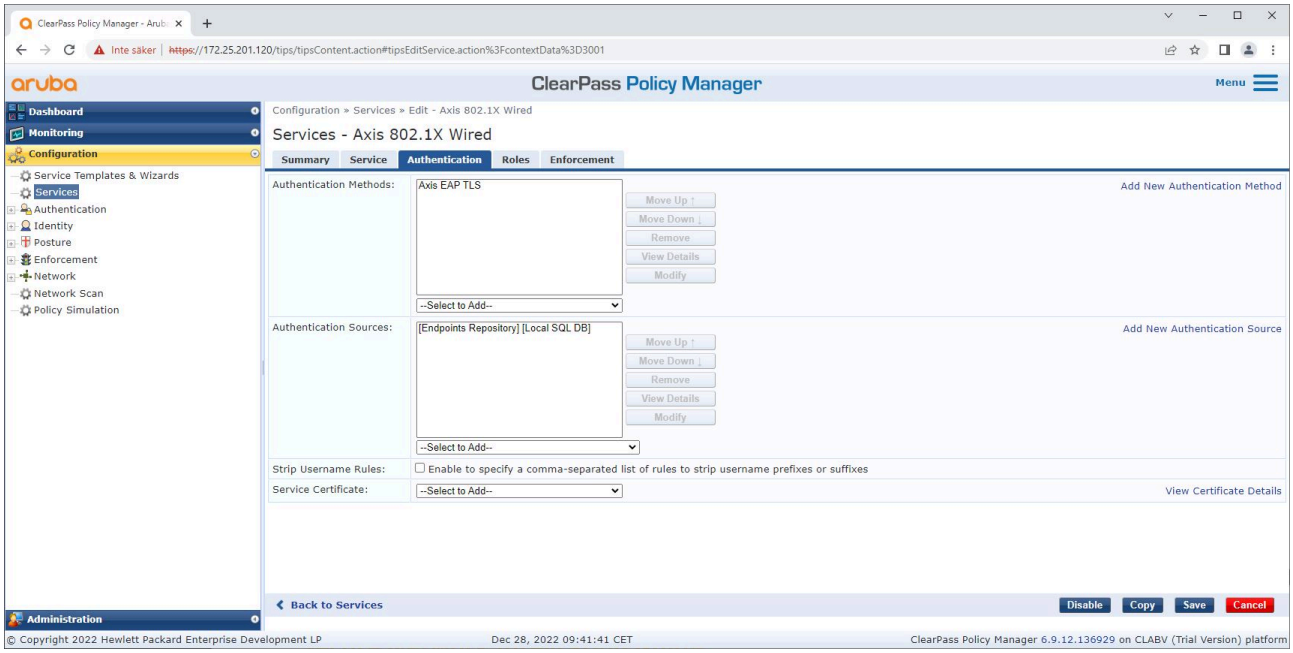
Benutzeroberfläche für Authentifizierungsmethoden im ClearPass Policy Manager, in der die EAP-TLS-Authentifizierungsmethode für Axis Geräte definiert wird.

Servicekonfiguration

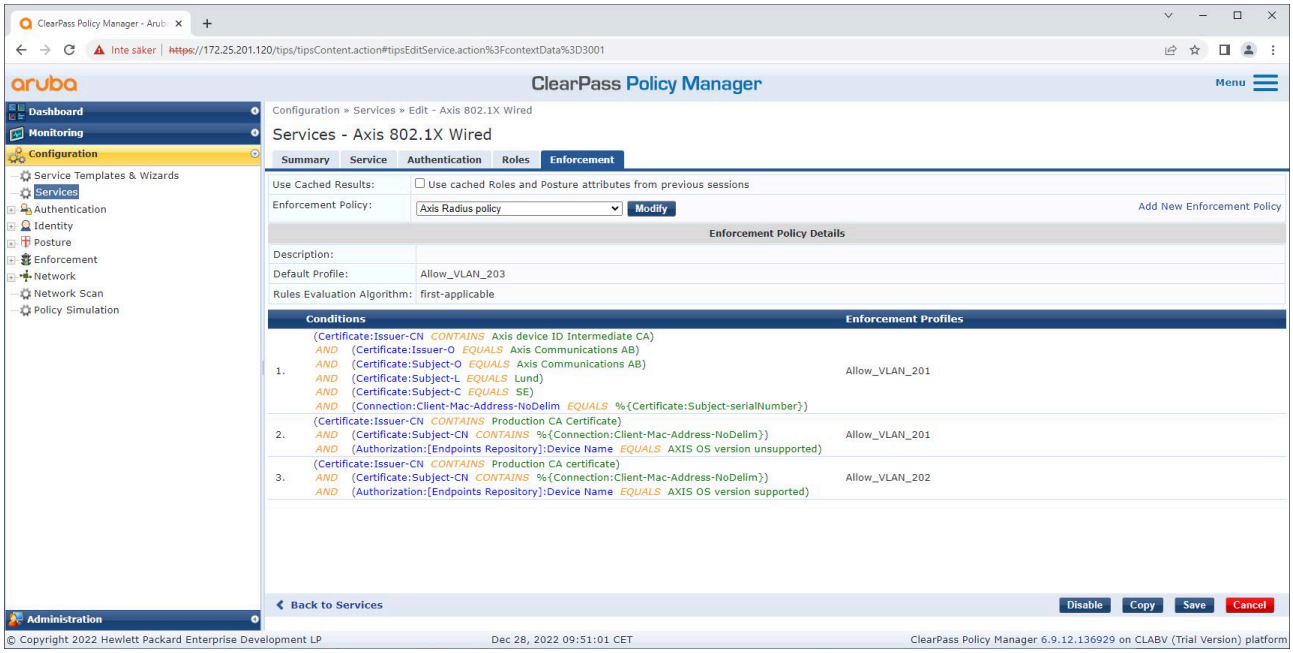
Auf der Seite **Services** werden die Konfigurationsschritte in einem Dienst zusammengefasst, der die Authentifizierung und Autorisierung von Axis Geräten in HPE Aruba Networking-Netzwerken übernimmt.



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.

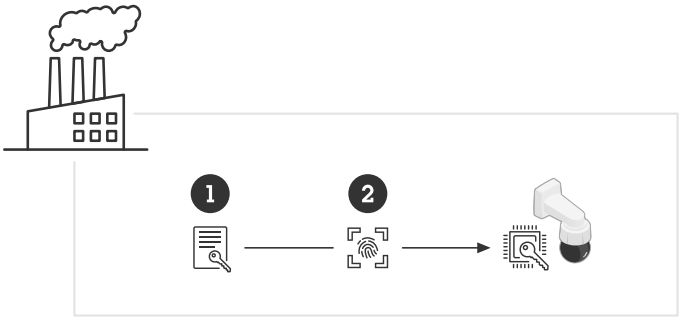
```
radius-server host MyRADIUSIPAddress key "MyRADIUSKey"
```

```
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 Gerätekennung 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.



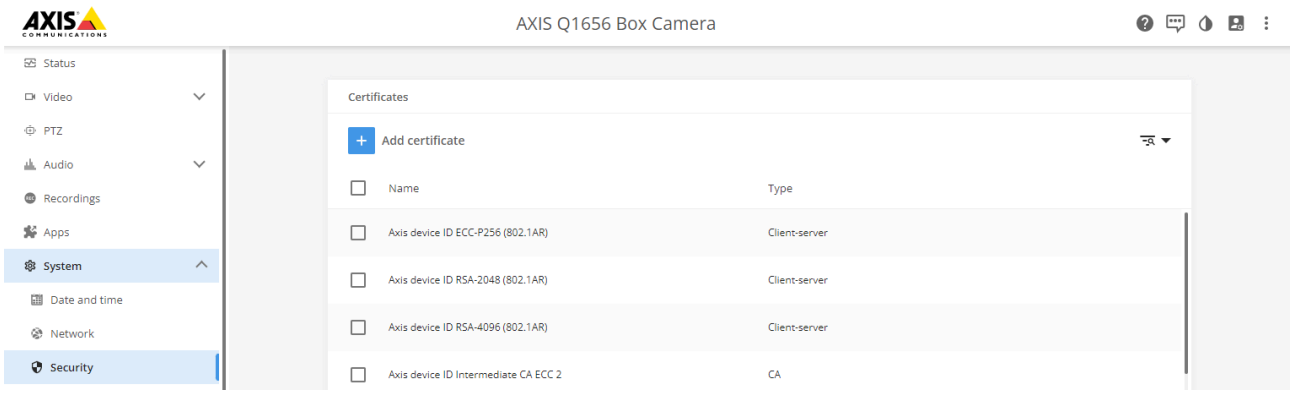
Axis Geräte werden mit dem IEEE 802.1AR-konformen Axis Geräte-ID-Zertifikat für vertrauenswürdige Geräteidentitätsdienste hergestellt

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.

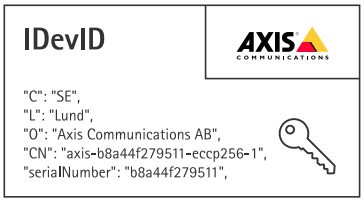
Hinweis

Die Seriennummer eines Axis Geräts ist seine MAC Adresse.



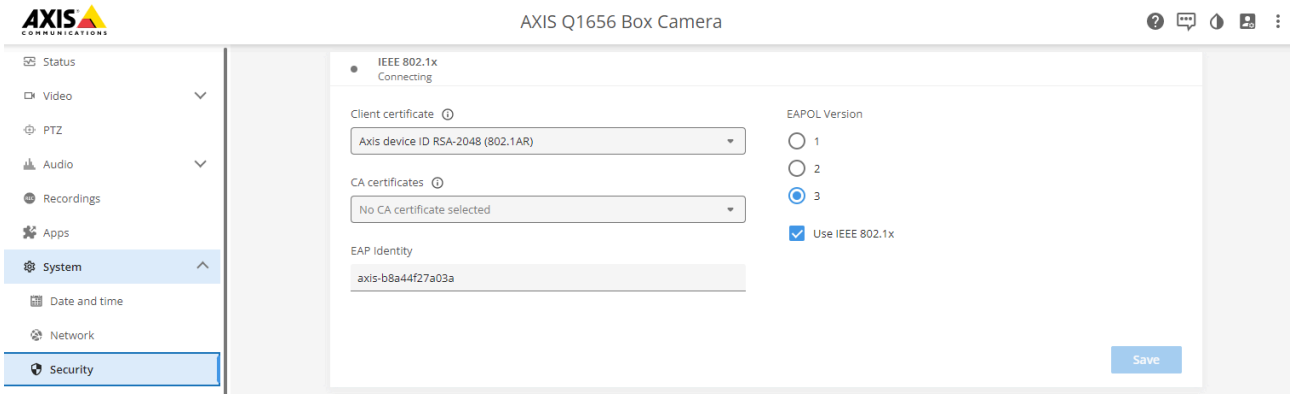
Der Zertifikatspeicher des Axis Geräts in der werkseitigen Standardeinstellung mit der Axis Geräte-ID.

Das IEEE 802.1AR-konforme Axis Geräte-ID-Zertifikat enthält Informationen zur Seriennummer und andere herstellerspezifische 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 Netzwerkbetrieb – IEEE 802.1AE MACsec

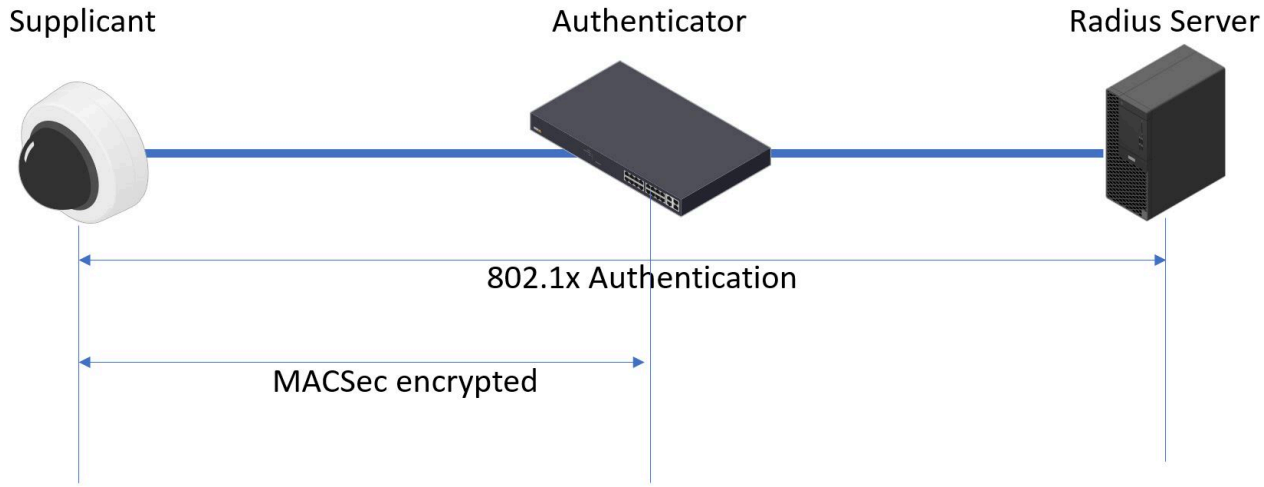
Rufen Sie zur Wiedergabe dieses Videos die Webversion dieses Dokuments auf.

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

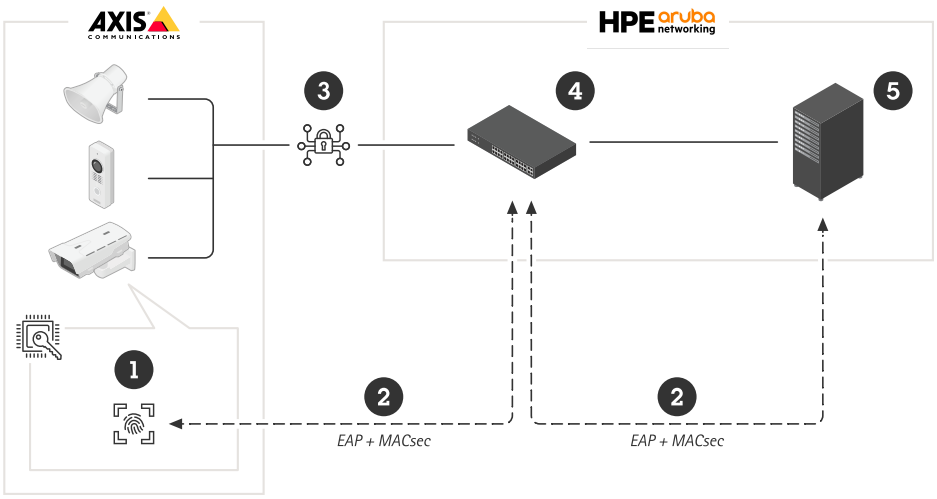
IEEE 802.1AE MACsec (Media Access Control Security) ist ein genau definiertes Netzwerkprotokoll, das Punkt-zu-Punkt-Ethernet-Verbindungen auf Netzwerkschicht 2 kryptografisch sichert. Es gewährleistet die Vertraulichkeit und Integrität der Datenübertragungen zwischen zwei Hosts.

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



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.



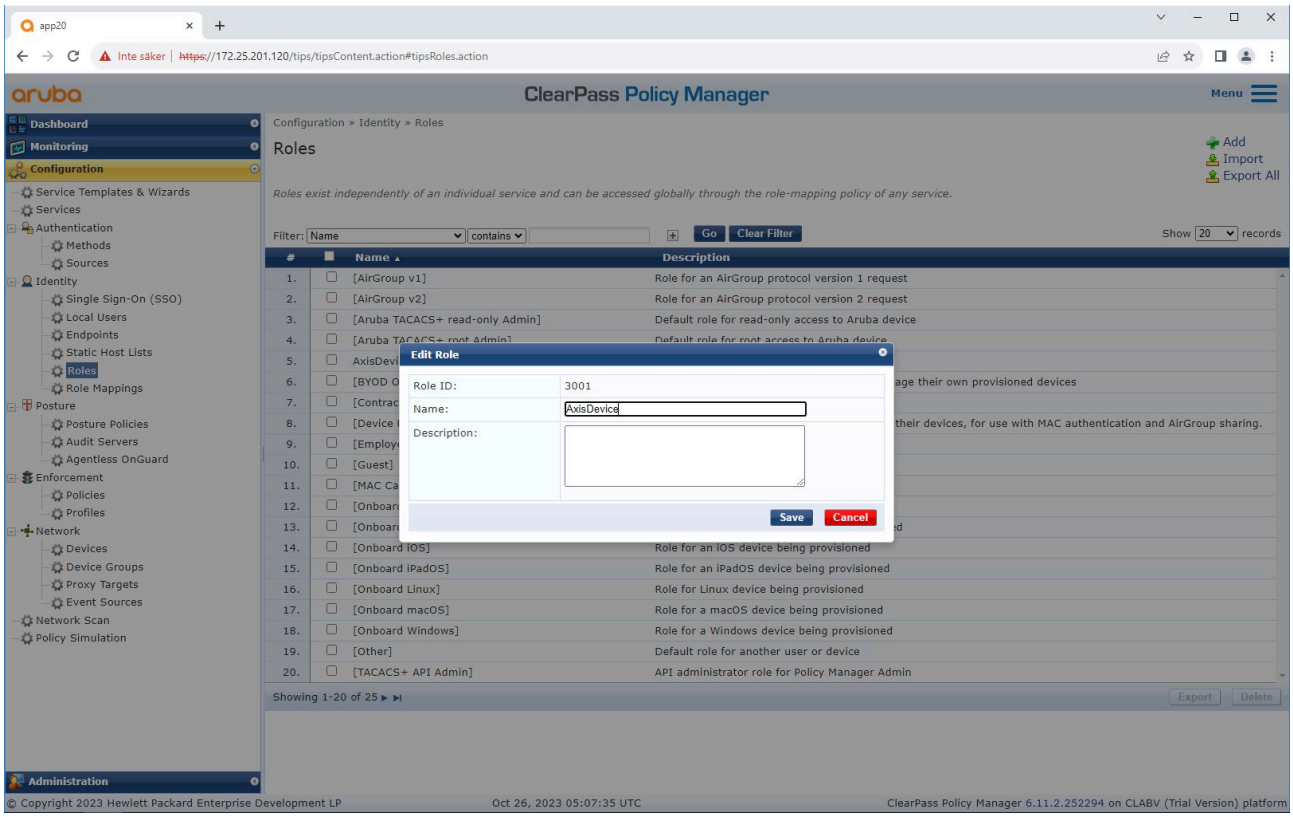
Die sicher gespeicherte Axis Geräte-ID (1), eine IEEE 802.1AR-konforme sichere Gerätekennung, dient zur Authentifizierung im Netzwerk (4, 5) durch die portbasierte IEEE 802.1X-EAP-TLS-Netzwerkzugriffskontrolle (2). Über die EAP-TLS-Sitzung werden MACsec-Schlüssel automatisch ausgetauscht, um eine sichere 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.

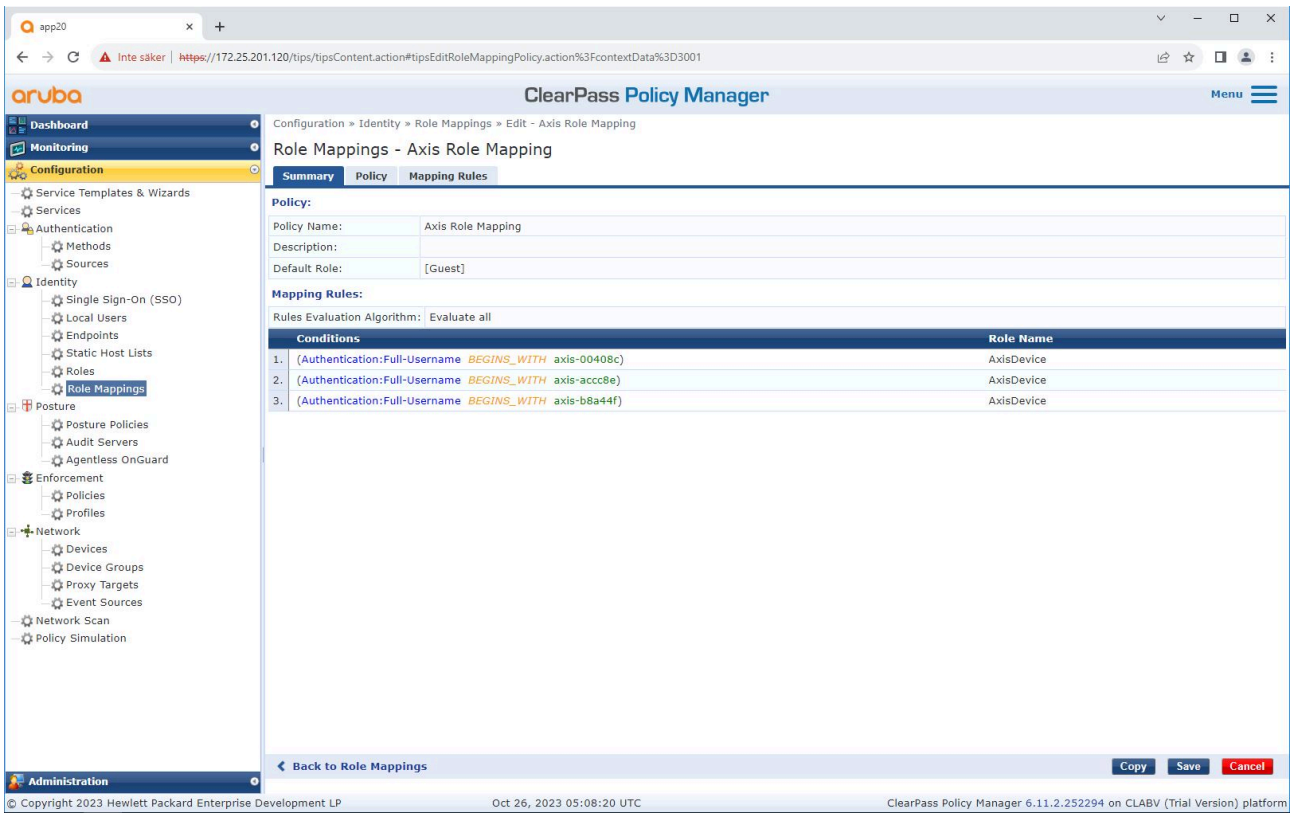
Wenn der HPE Aruba Netzwerk-Zugangsschalter MACsec mit EAP-TLS nicht unterstützt, kann der Pre-Shared Key-Modus verwendet und manuell konfiguriert werden.

HPE Aruba Networking ClearPass Policy Manager

Rollen- und Rollenzuordnungsrichtlinie



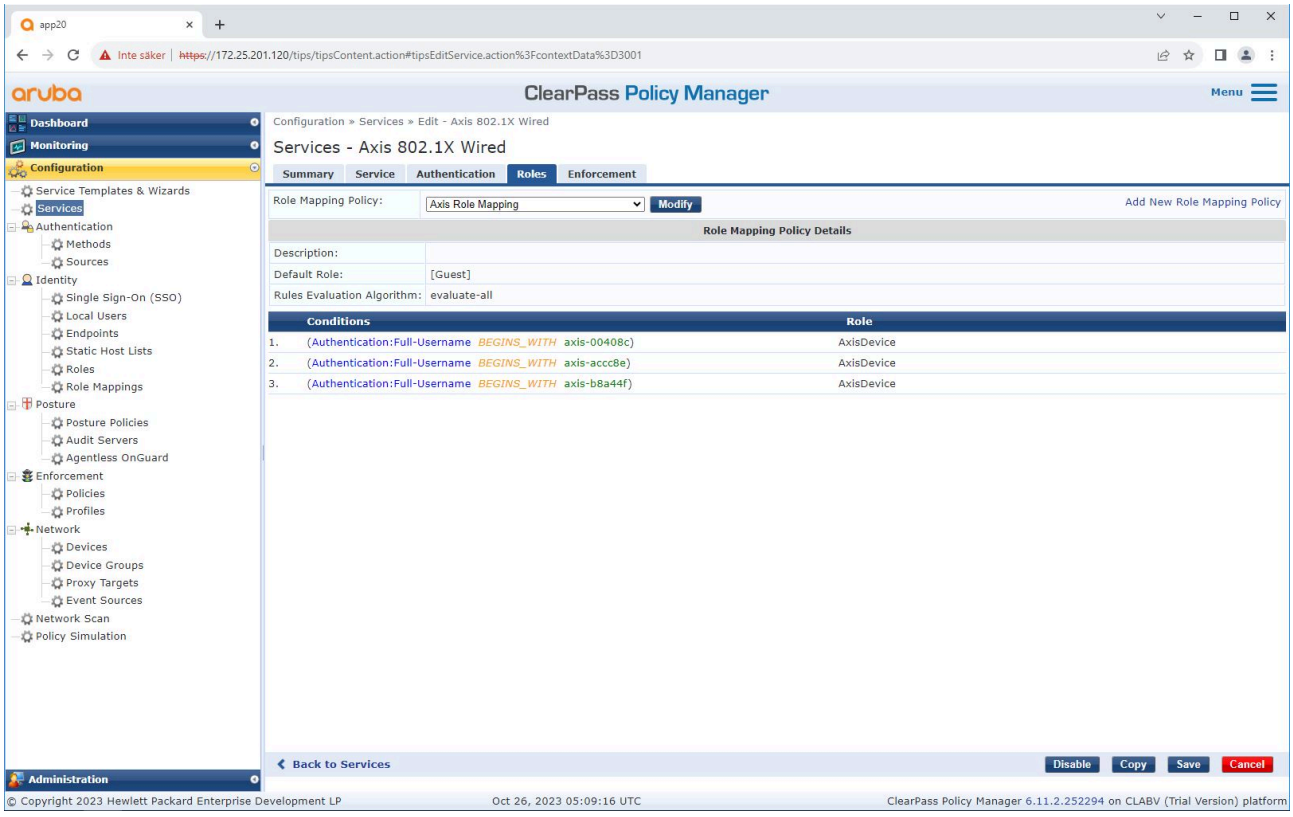
Hinzufügen eines Rollennamens für Axis Geräte. Der Name ist der Name der Port-Zugriffsrolle in der Zugangsschalter-Konfiguration.



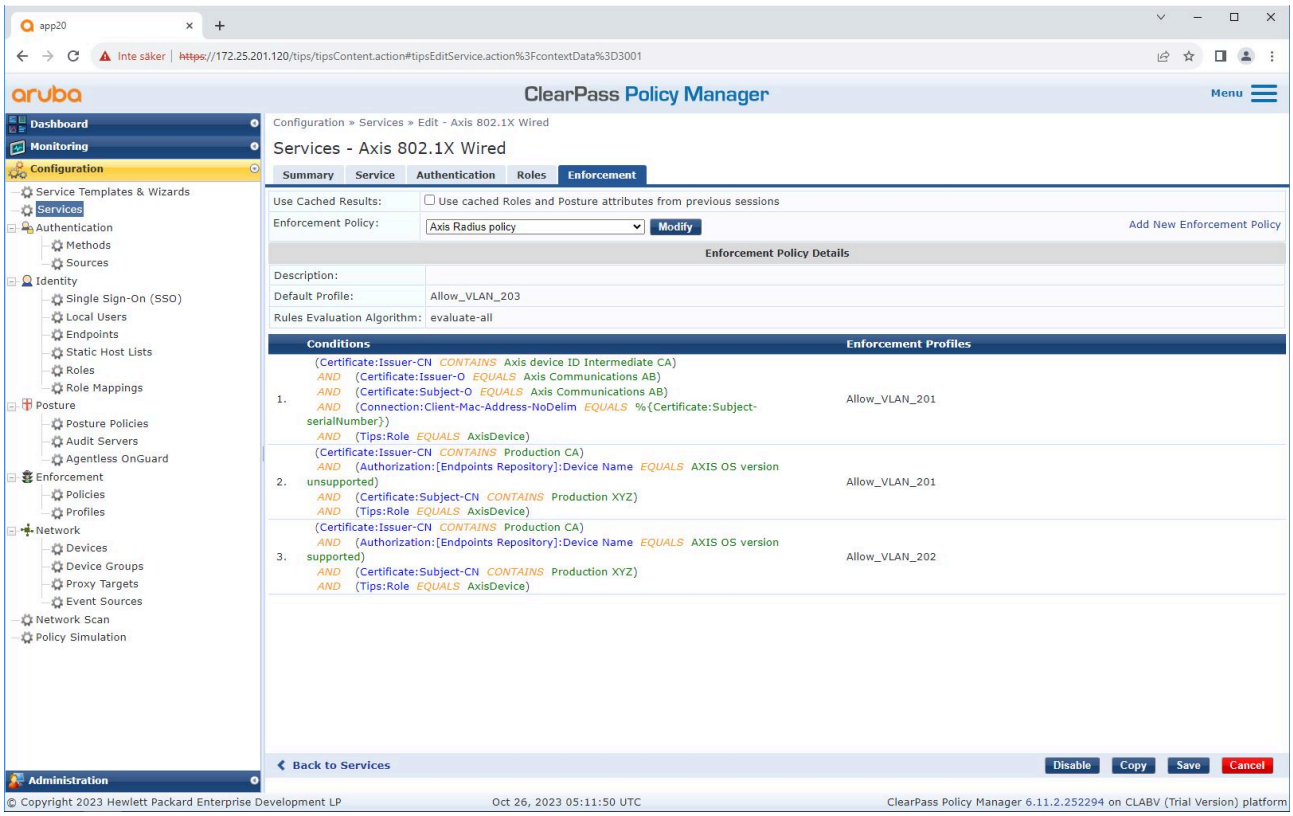
Hinzufügen einer Axis Rollenzuordnungsrichtlinie für die zuvor erstellte Axis Geräterolle. Die definierten Bedingungen sind erforderlich, damit ein Gerät der Axis Geräterolle zugeordnet werden kann. Wenn die Bedingungen nicht erfüllt sind, wird dem Geräte eine Gastrolle [Guest] zugewiesen.

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

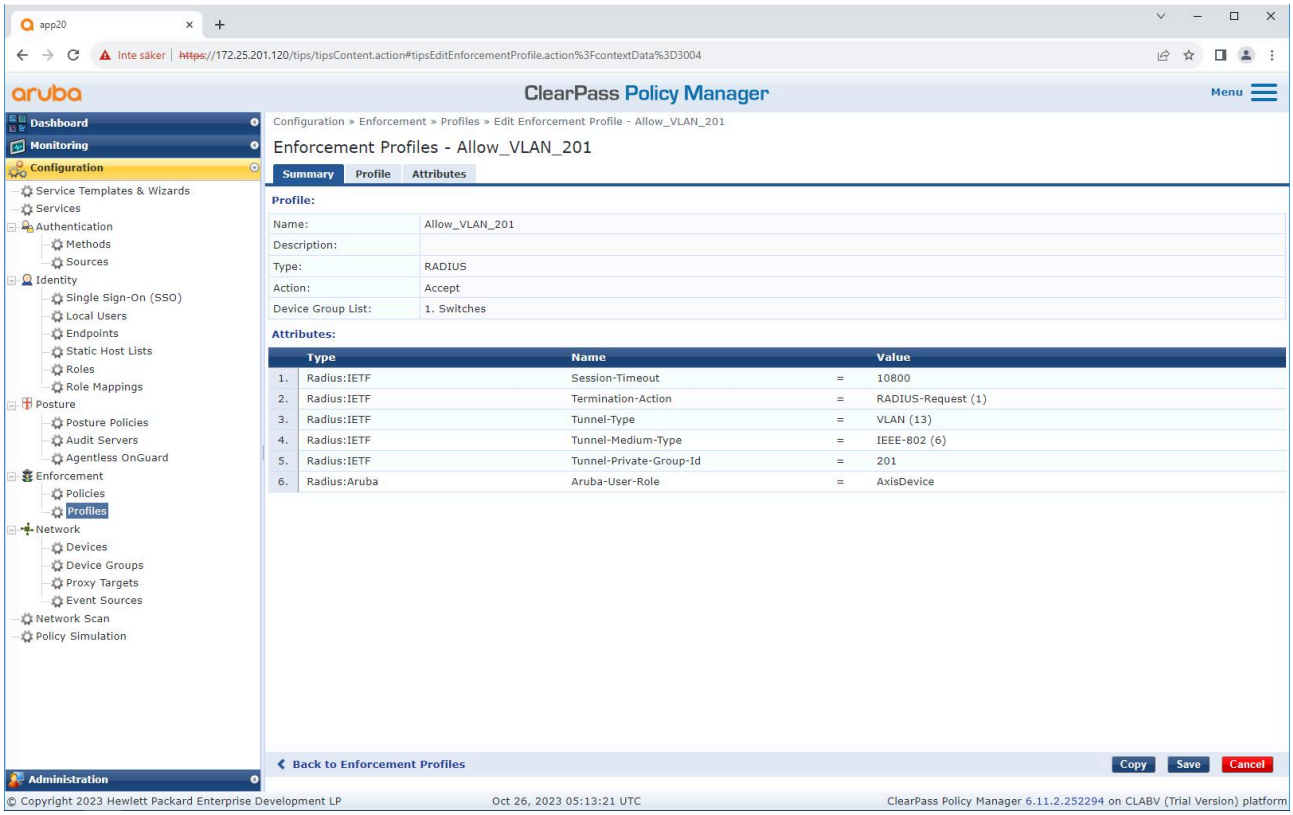


Hinzufügen der zuvor erstellten Axis Rollenzuordnungsrichtlinie zum Dienst, der IEEE 802.1X als Verbindungsmethode für das Onboarding von Axis Geräten definiert.



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 zugewiesen 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 authenticatormacsecmkacak-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

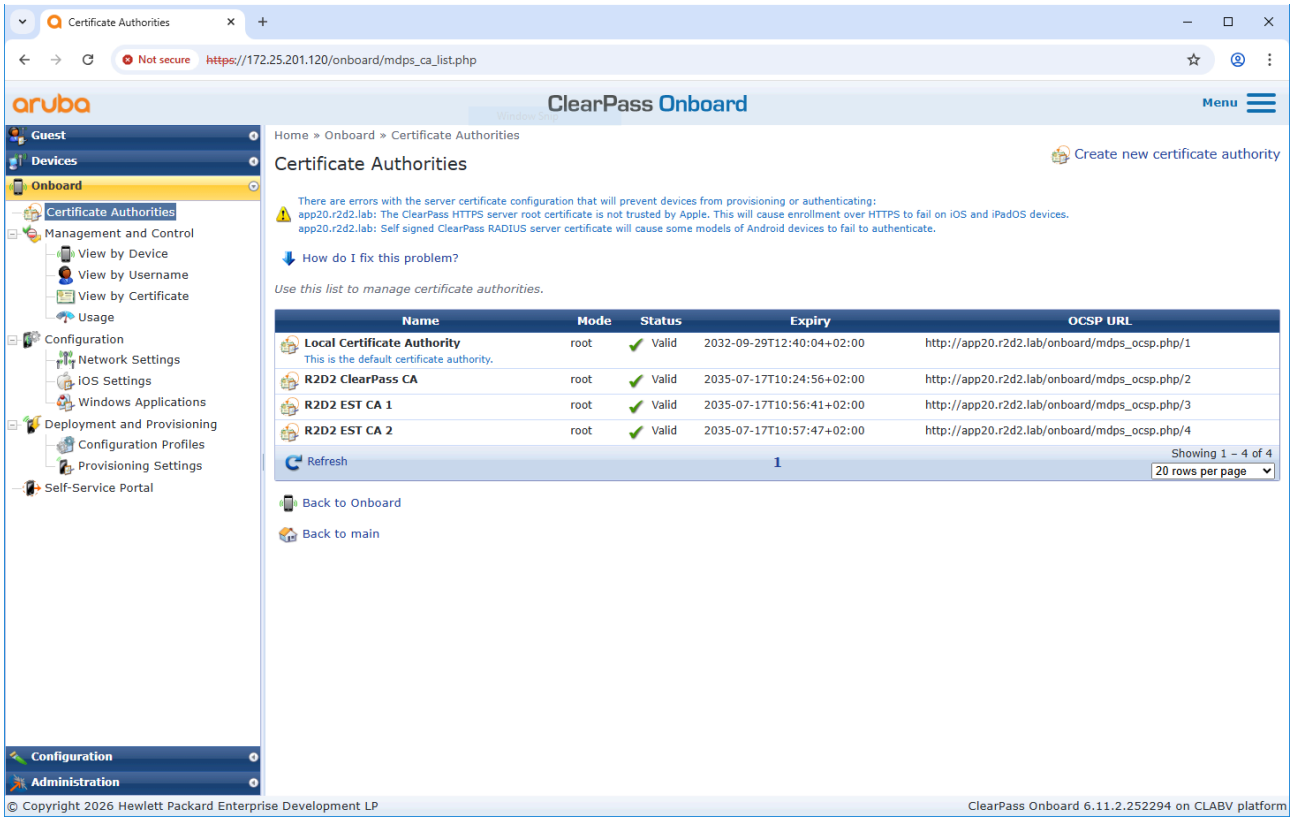
- Die automatisierte Registrierung, Erneuerung und Neuregistrierung von Zertifikaten auf der Grundlage von IT-Richtlinien, wodurch die zeitaufwändige manuelle Konfiguration vollständig entfällt.
- Hochmoderne, sichere Kommunikation ausschließlich über HTTPS TLS 1.2/1.3.
- Zentralisierte Sichtbarkeit/Überwachung 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*.

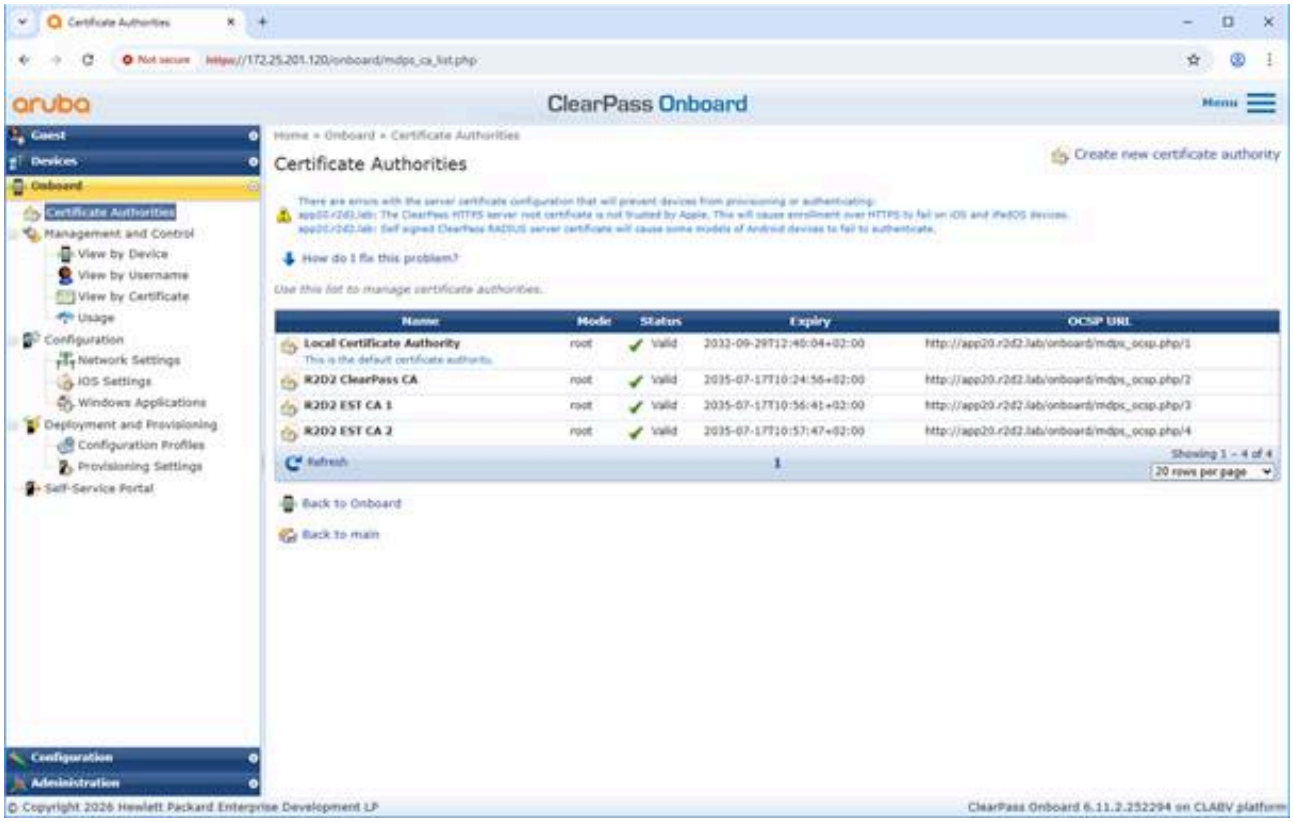
Konfiguration von HPE Aruba ClearPass Onboard

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.

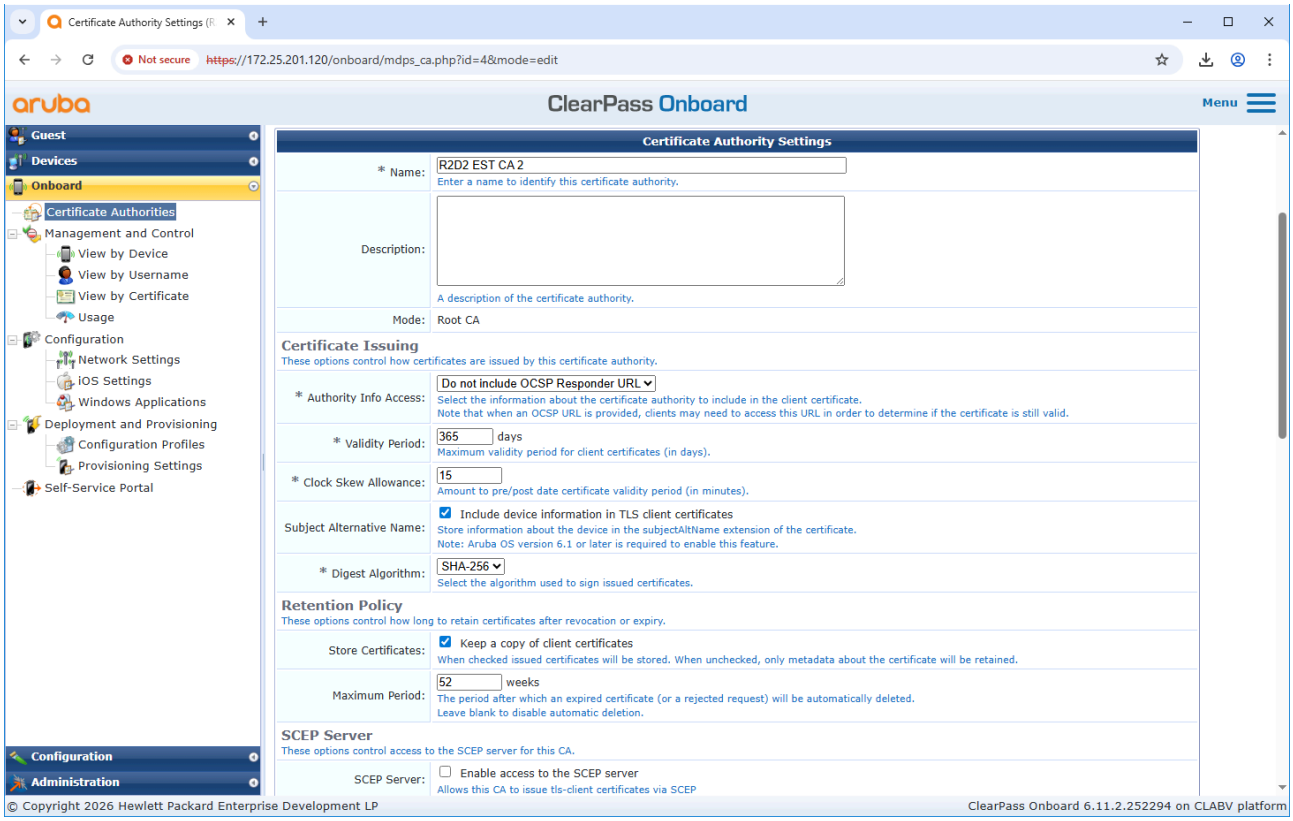
Konfiguration der Zertifizierungsstelle



Erstellen Sie eine neue Zertifizierungsstelle in ClearPass Onboard.



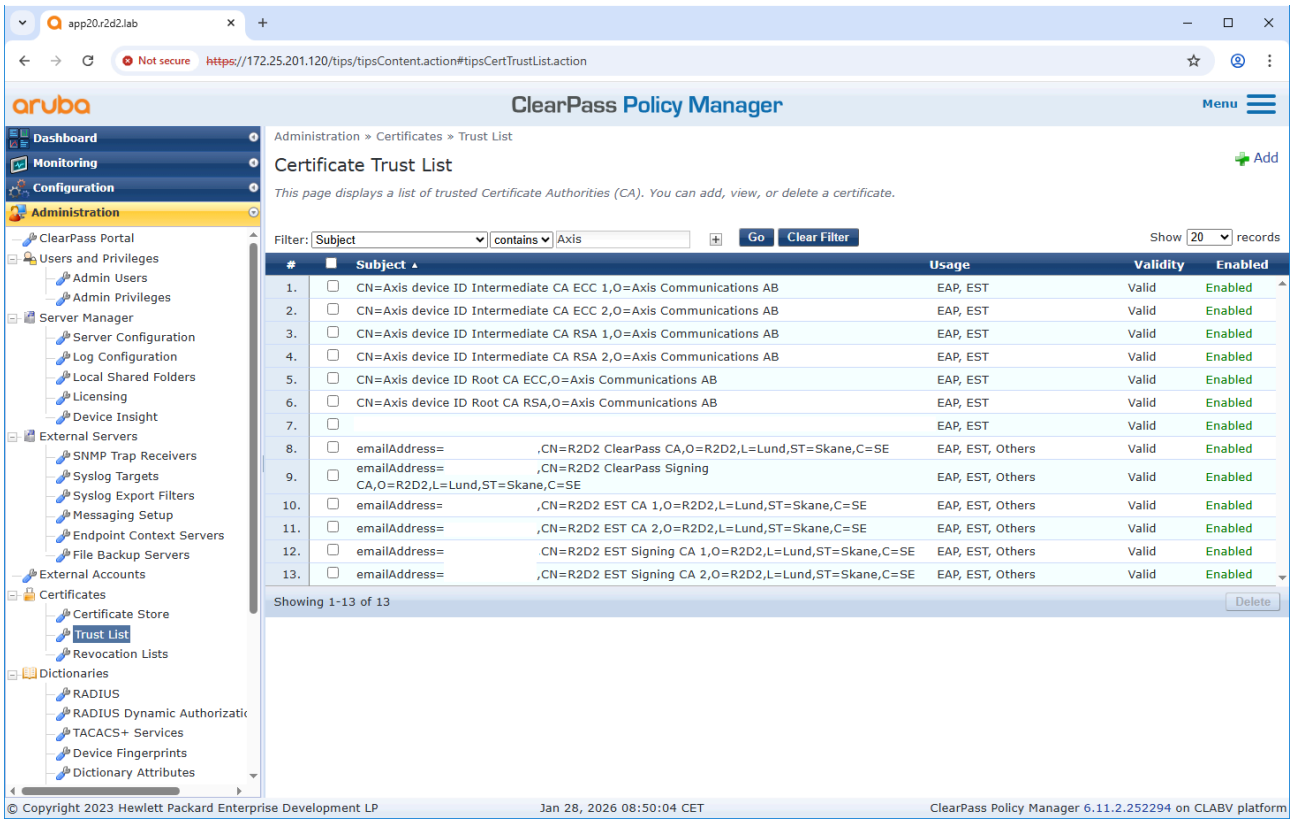
In der erstellten Zertifizierungsstelle werden der Schlüsseltyp, die Schlüsselgröße, die Gültigkeitsdauer und weitere Parameter definiert.



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

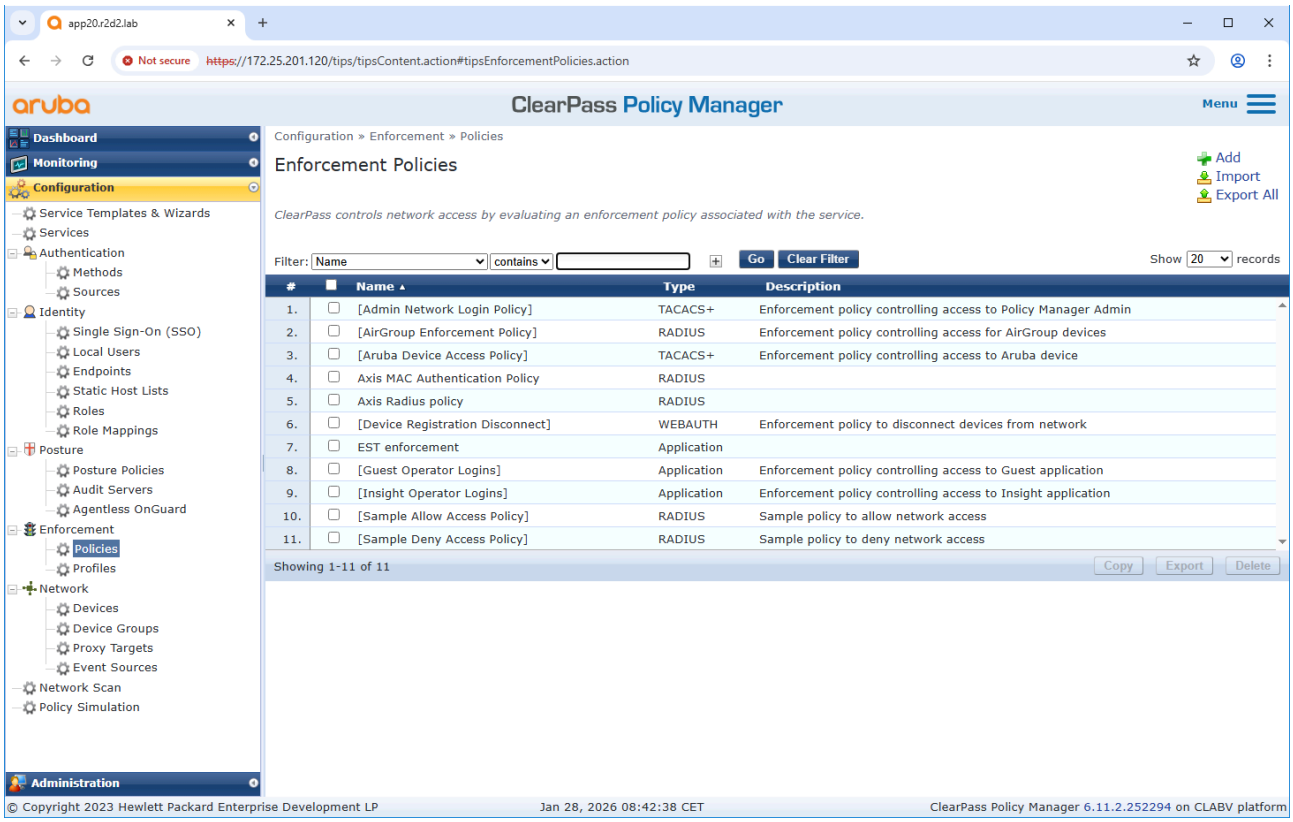
Konfiguration des vertrauenswürdigen Zertifikatspeichers



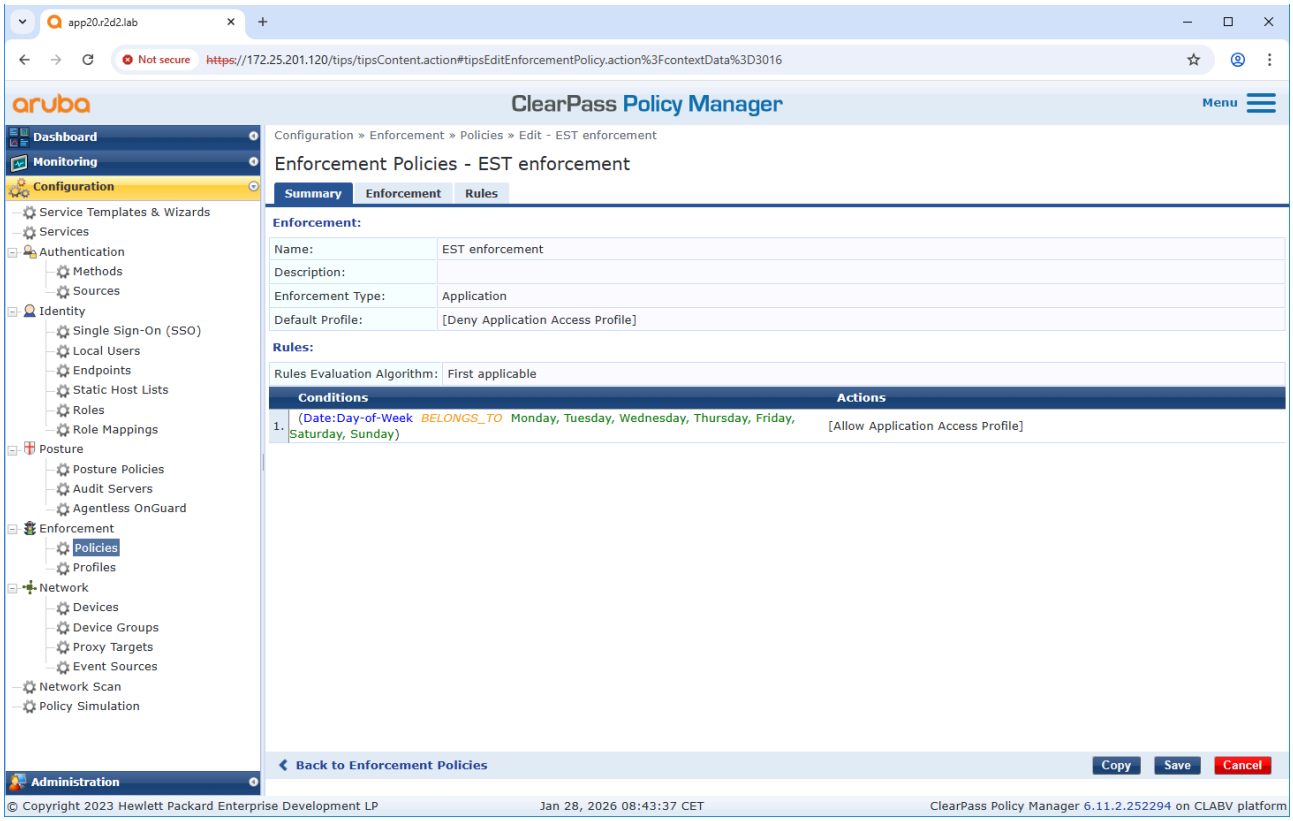
Falls nicht schon geschehen, laden Sie die *für Axis spezifischen IEEE 802.1AR-Zertifikate* in den Speicher für vertrauenswürdige Zertifikate des ClearPass Policy Managers. Achten Sie darauf, die EST-Nutzung hinzuzufügen. Überprüfen Sie dies auch für die zuvor erstellte Zertifizierungsstelle von ClearPass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

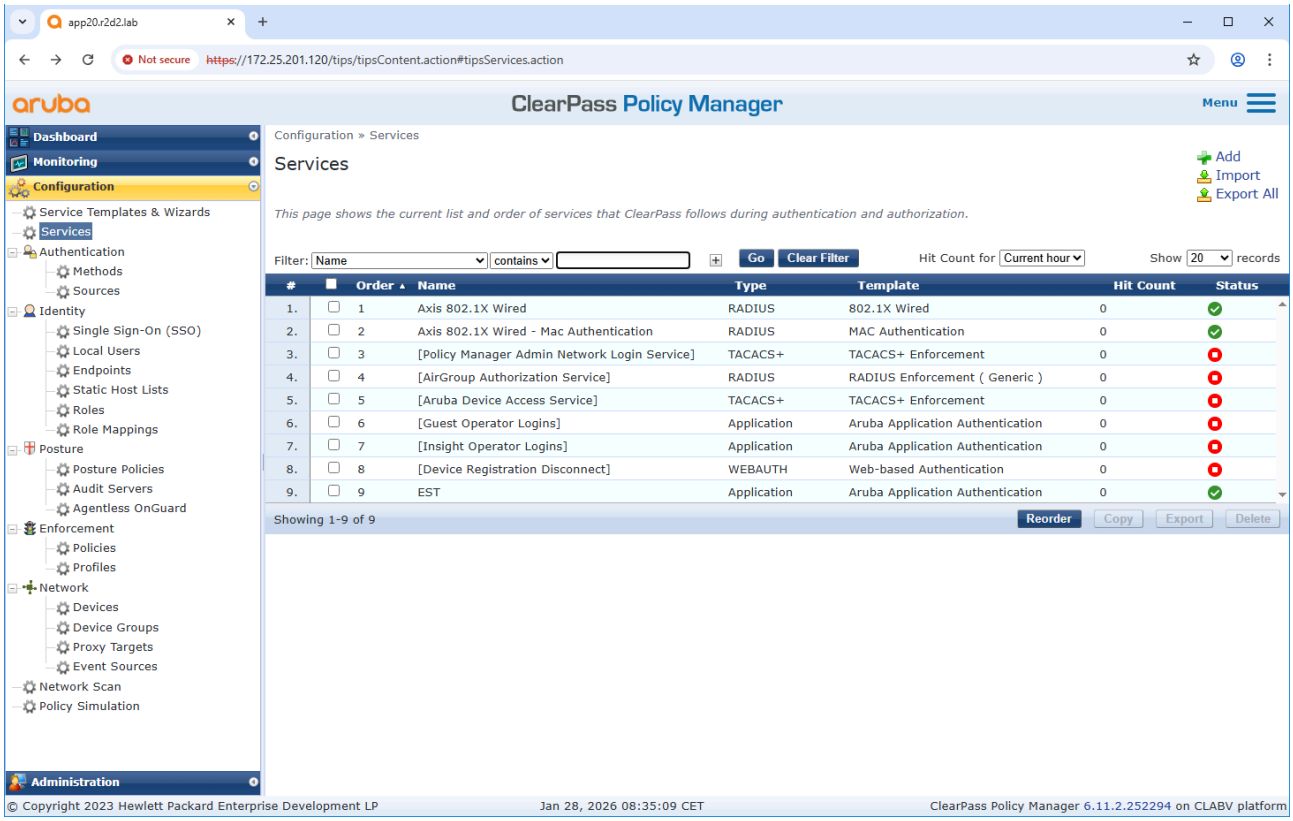


Übersicht über die Durchsetzungsrichtlinien im ClearPass Policy Manager.

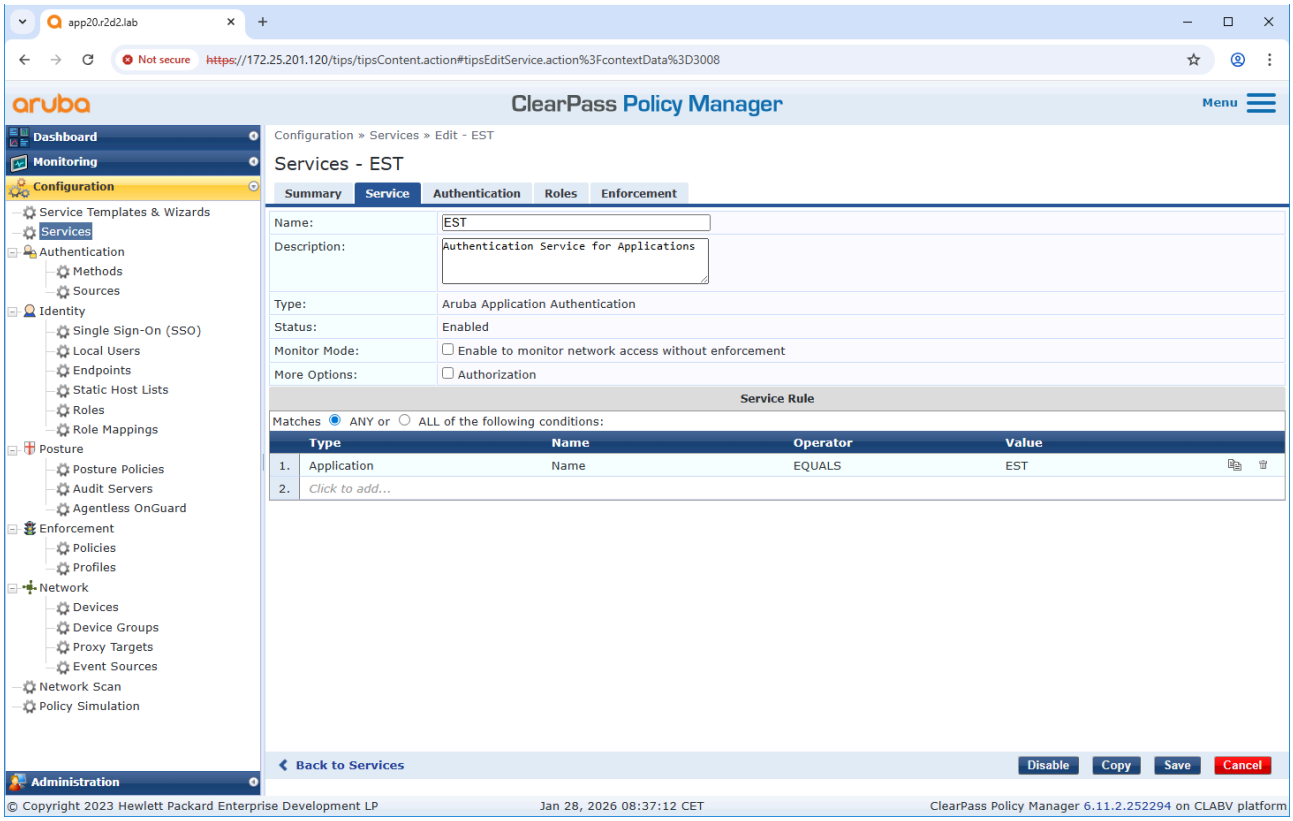


In dieser Beispielrichtlinie hat die EST-Anwendung eine Berechtigung für alle Tage der Woche.

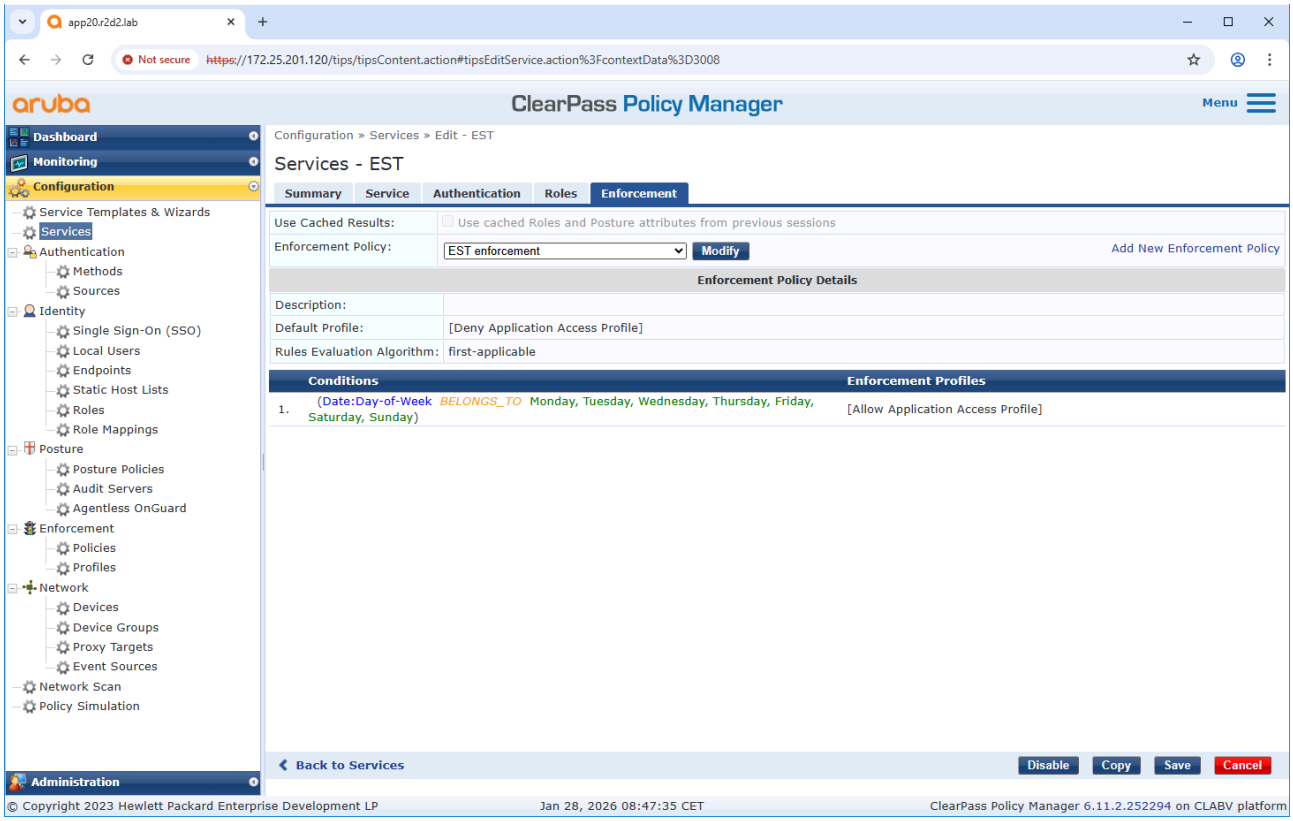
Servicekonfiguration



Ein spezieller EST-Dienst muss erstellt werden.



Der Dienst muss für die EST-Anwendung konfiguriert werden.



Wählen Sie die zuvor erstellte EST-Durchsetzungsrichtlinie aus.

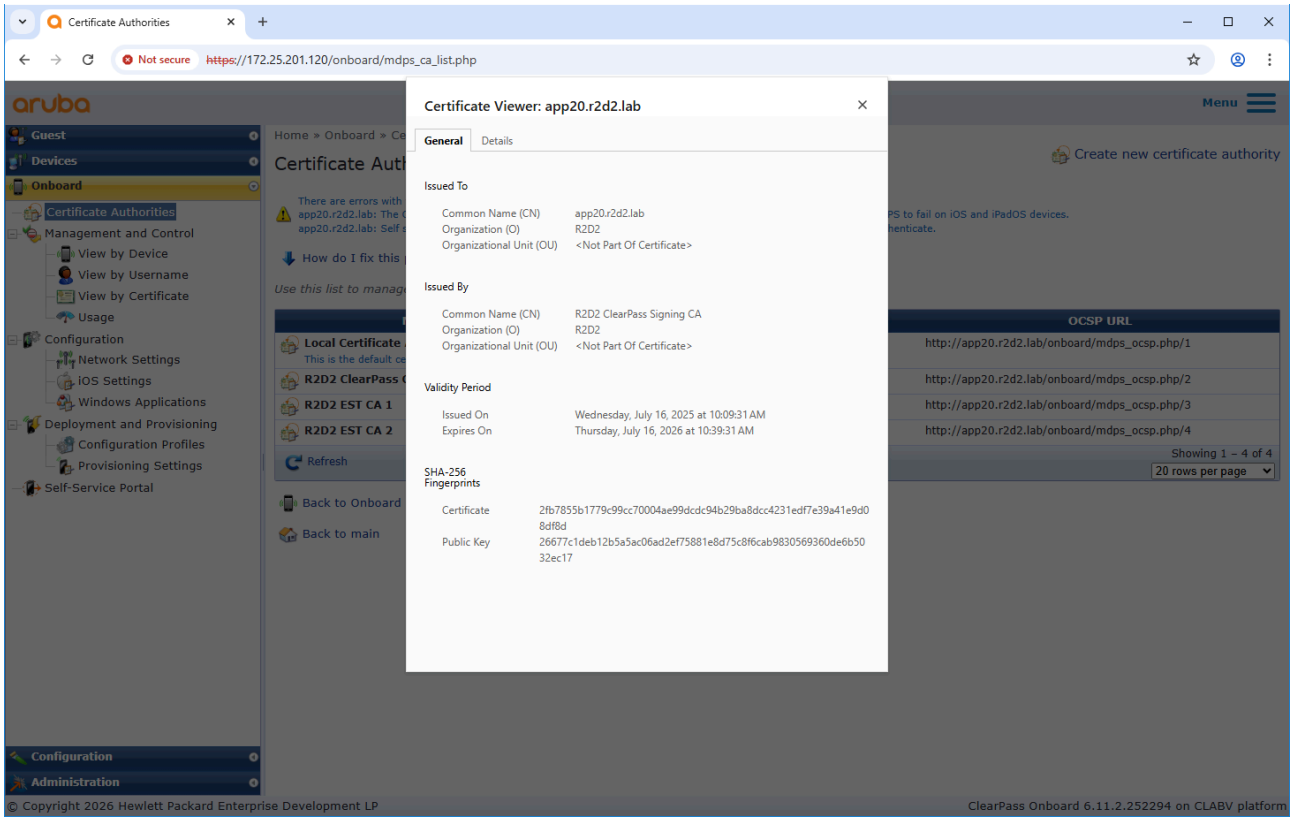
Konfiguration Axis

Die Konfiguration auf dem Axis Gerät erfolgt in zwei Schritten.

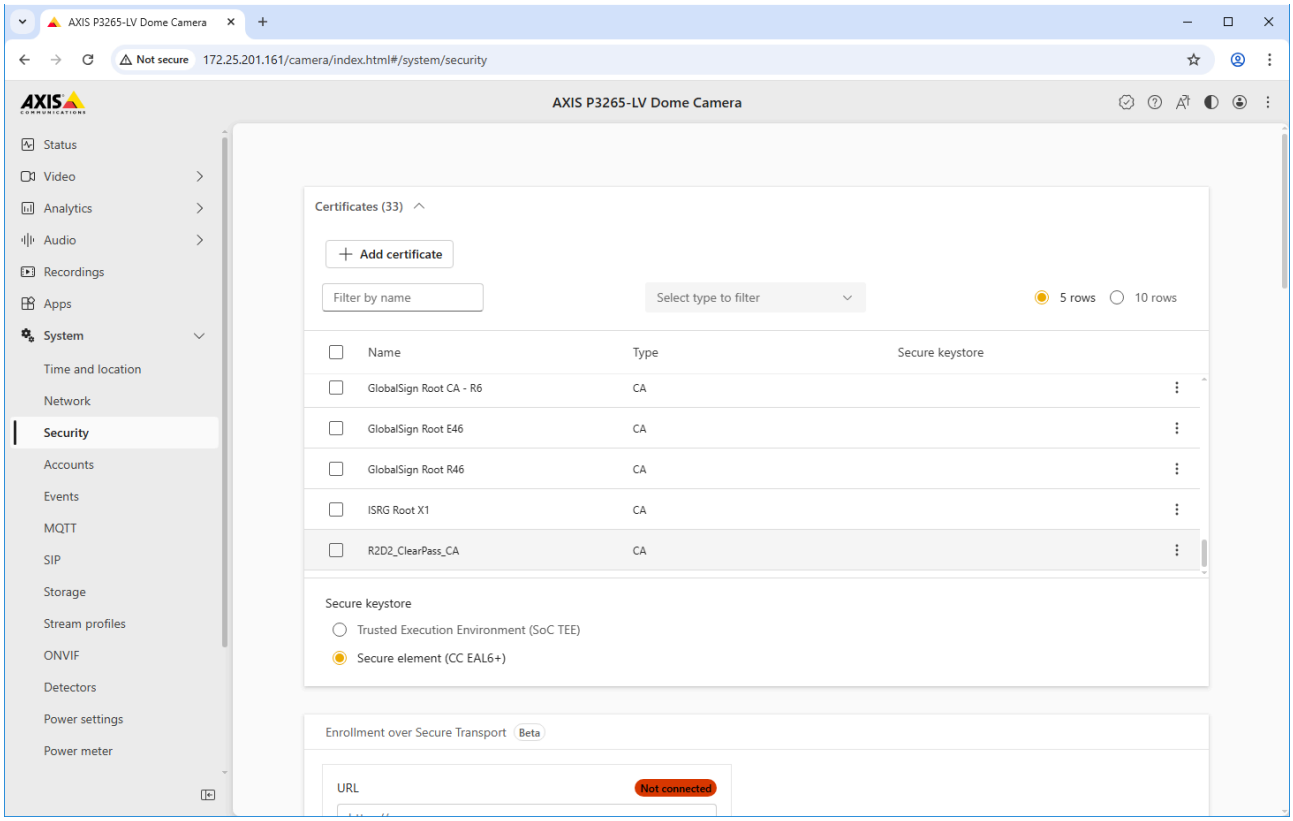
1. Stellen Sie eine vertrauenswürdige Verbindung mit dem ClearPass Onboard HTTPS-Endpunkt her.

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

Konfiguration des vertrauenswürdigen Zertifikats

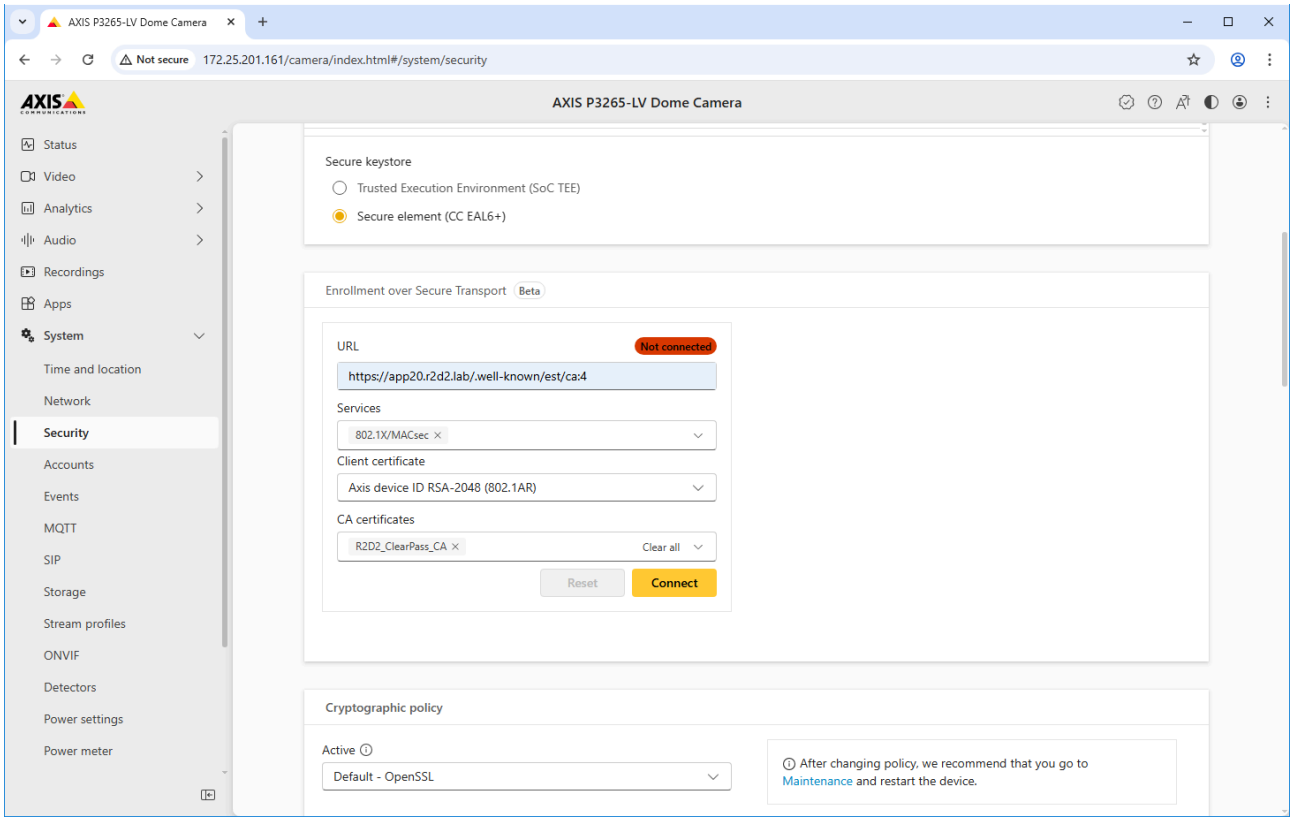


Überprüfen Sie die Zertifikatskette vom ClearPass Onboard HTTPS-Endpunkt.

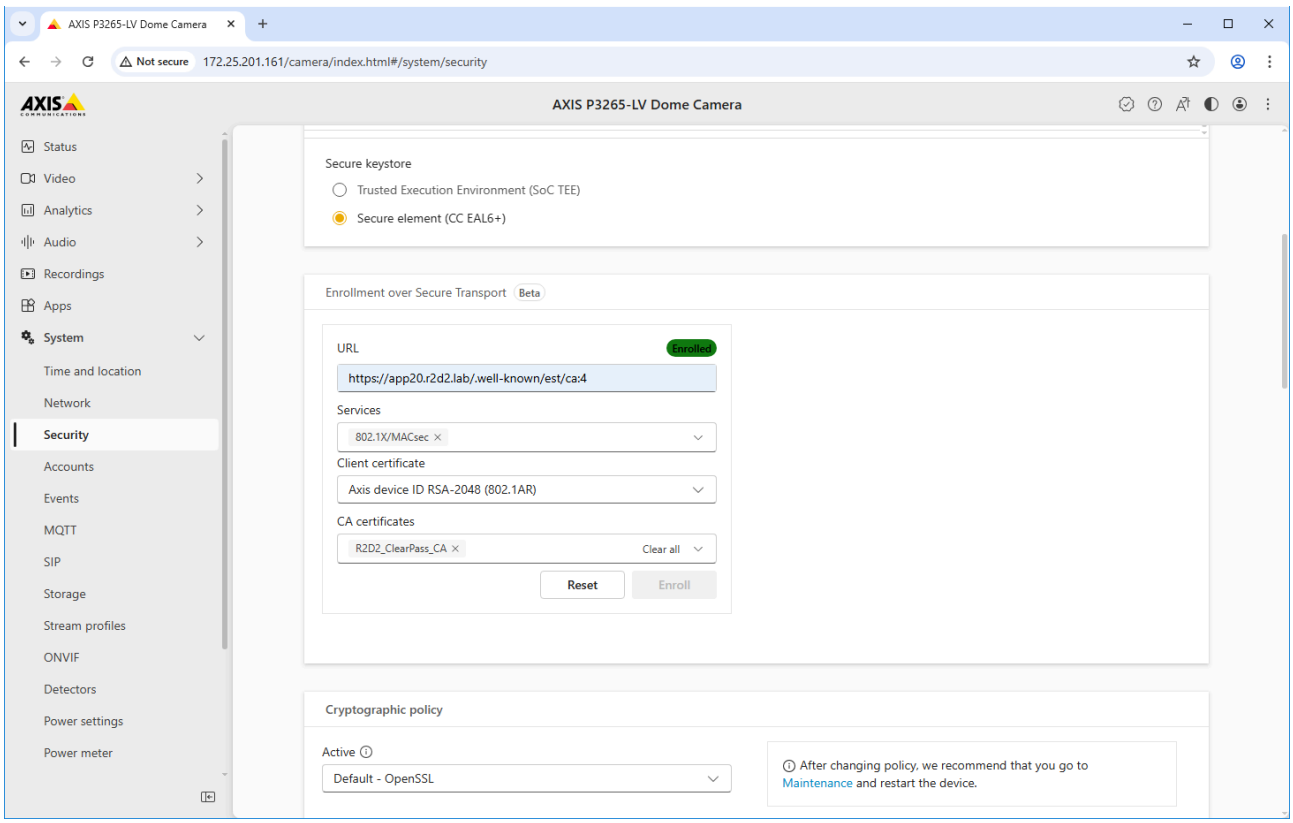


Laden Sie die Zertifizierungsstelle vom ClearPass Onboard HTTPS-Endpunkt auf das Axis Gerät hoch.

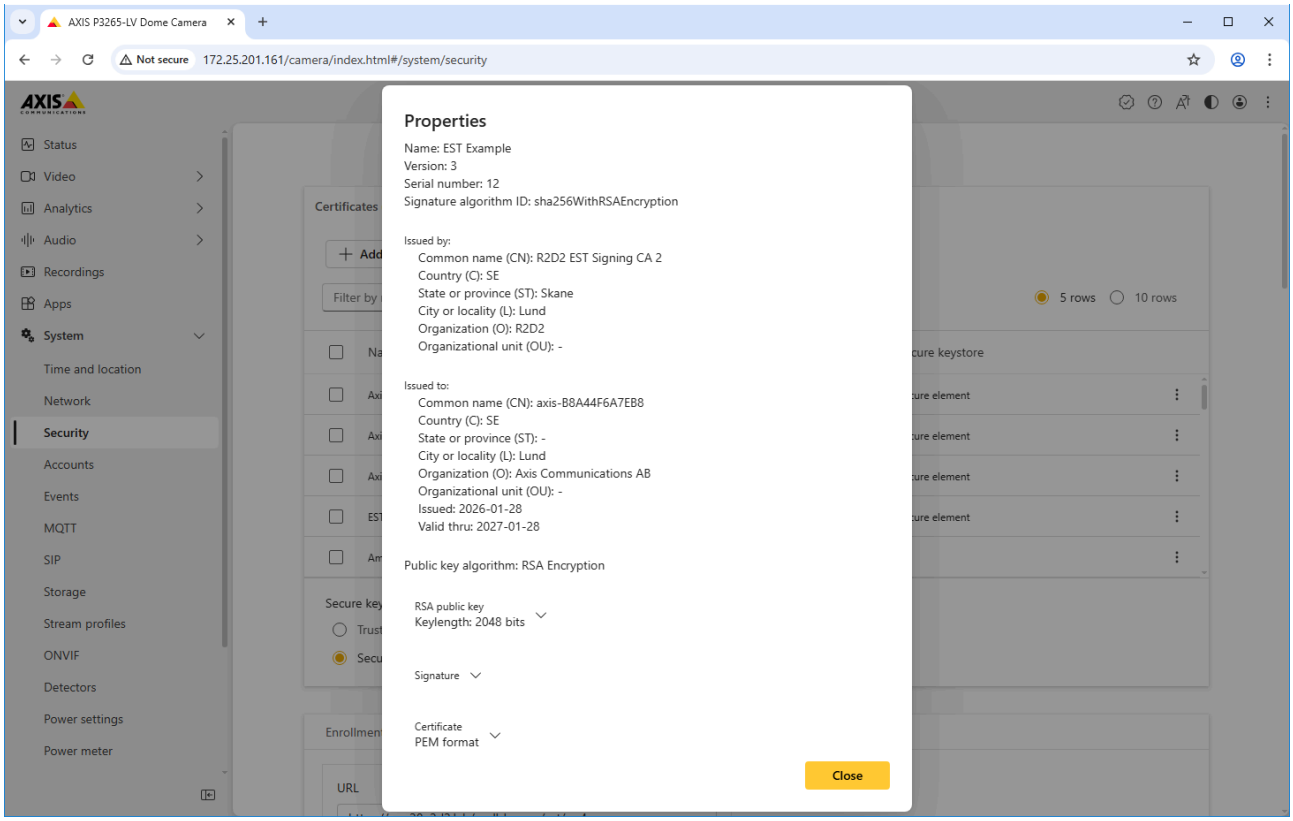
Konfiguration des EST-Clients



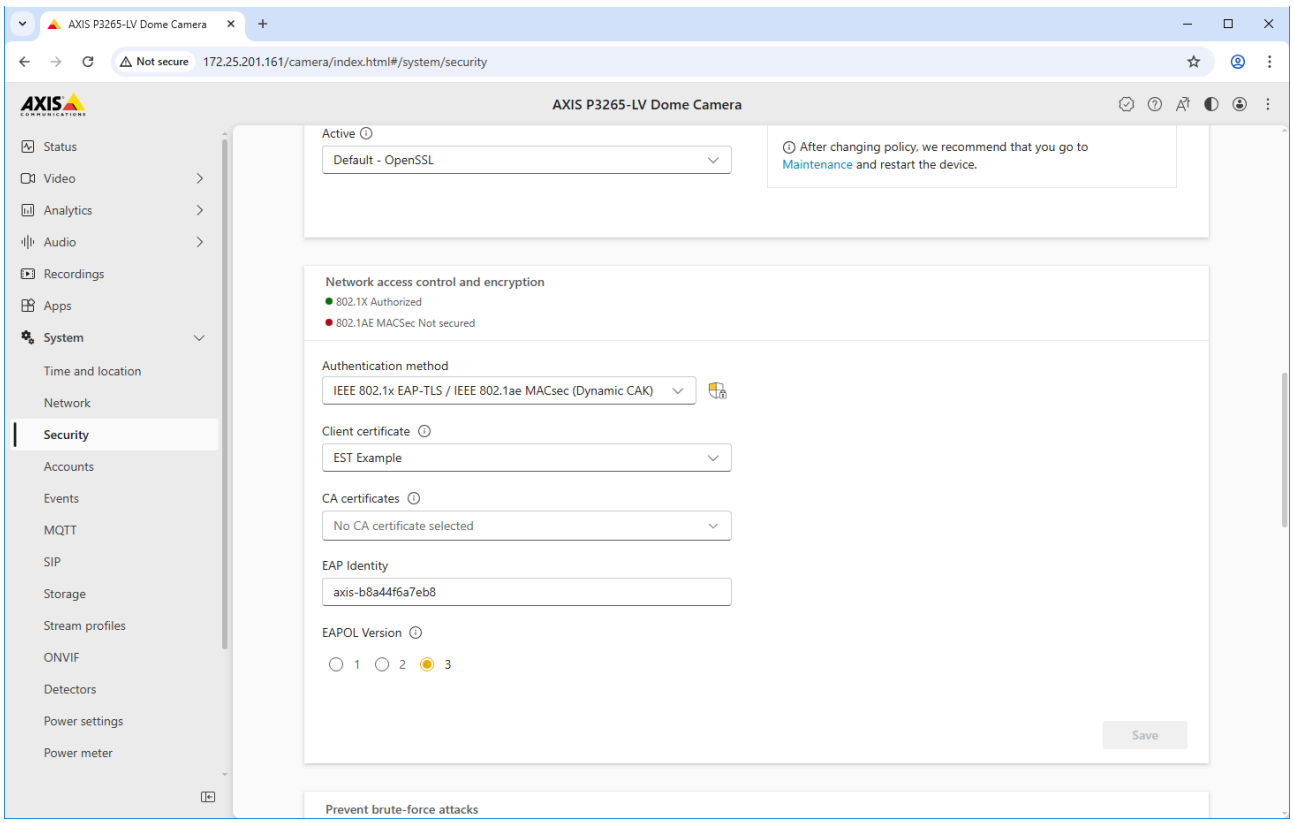
Parameter	Wert
URL	Die EST-URL finden Sie in der erstellten Zertifizierungsstelle für EST in ClearPass Onboard.
Services	Wählen Sie die Dienste aus, die automatisch mit dem registrierten Zertifikat konfiguriert werden sollen.
Client certificate (Clientzertifikat)	Wählen Sie ein Client-Zertifikat für 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.



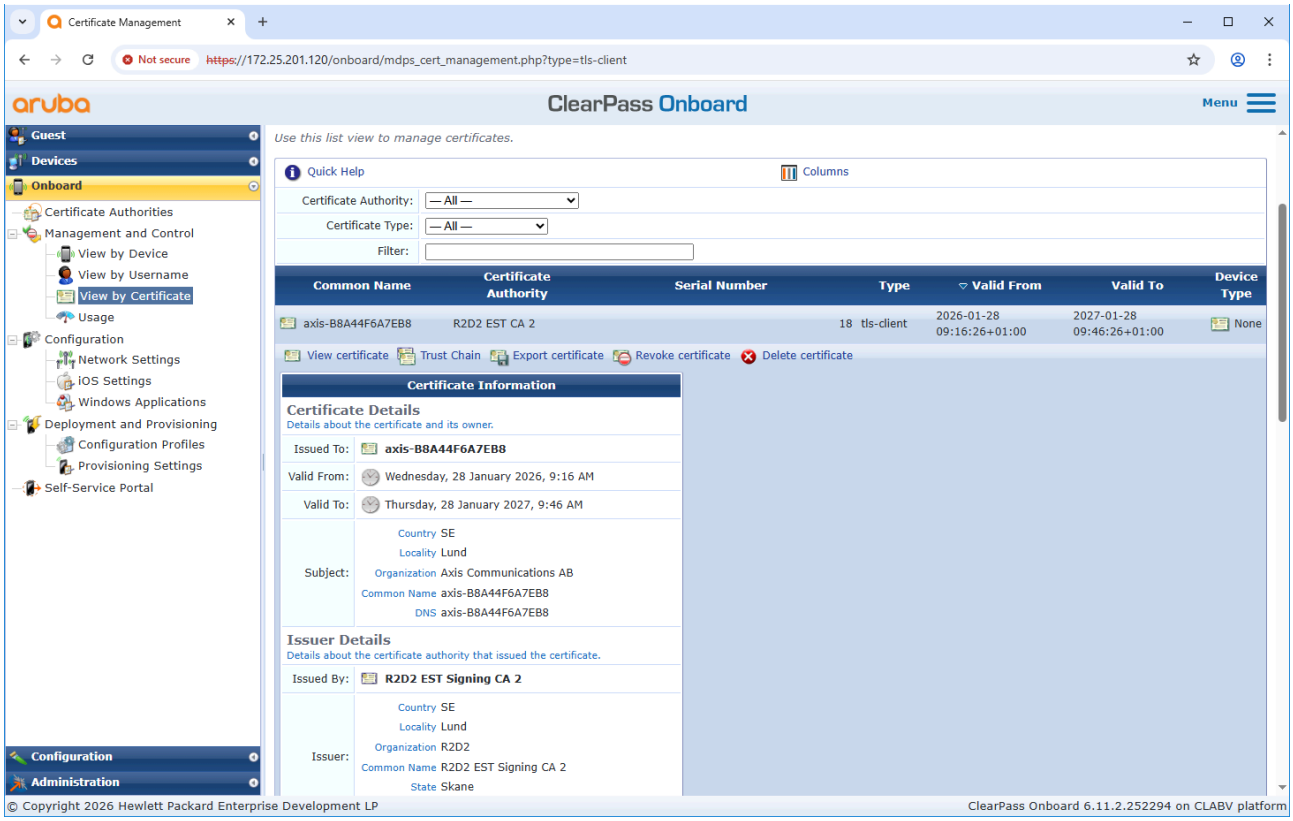
Die Registrierung wurde erfolgreich abgeschlossen.



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

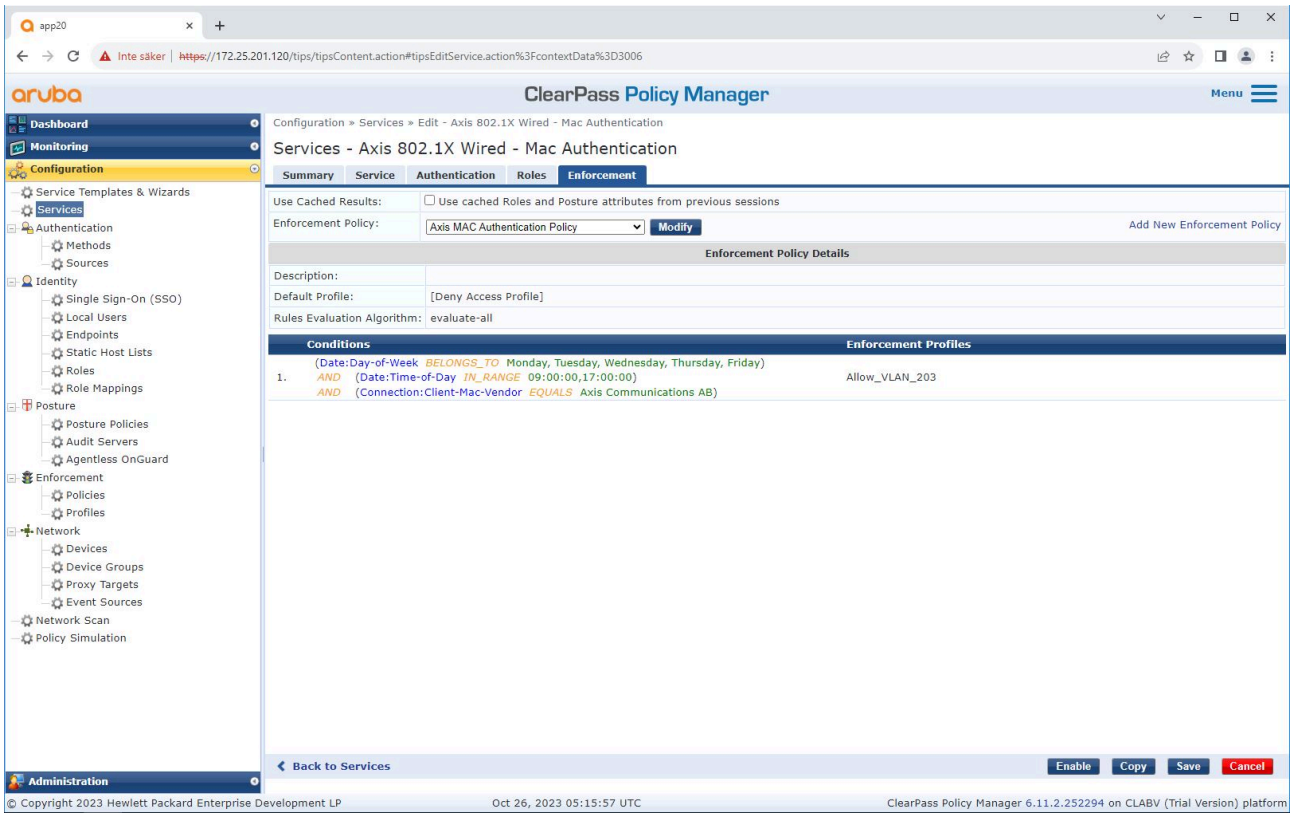
Sie können den MAC-Authentifizierungsbypass (MAB) nutzen, um Axis Geräte einzubinden, die das IEEE 802.1AR-Onboarding mit dem Axis Geräte-ID-Zertifikat und in der werksseitigen Standardeinstellung aktiviertem IEEE 802.1X nicht unterstützen. Wenn die 802.1X-Einbindung fehlschlägt, validiert ClearPass 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.



Netzwerkzugriff verweigert

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

Gastnetzwerk (VLAN 203)

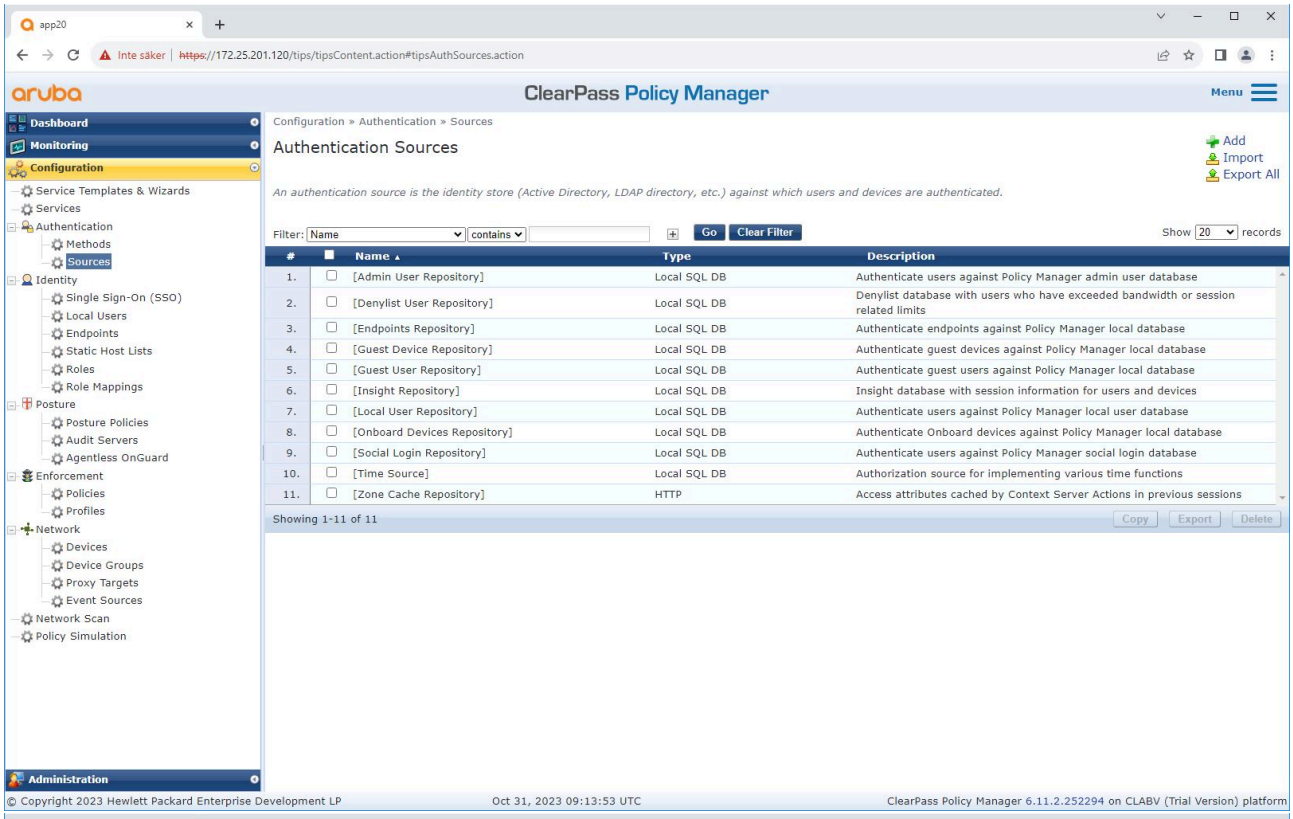
Dem Axis Gerät wird Zugriff auf ein begrenztes, isoliertes Netzwerk gewährt, wenn die folgenden Bedingungen erfüllt sind:

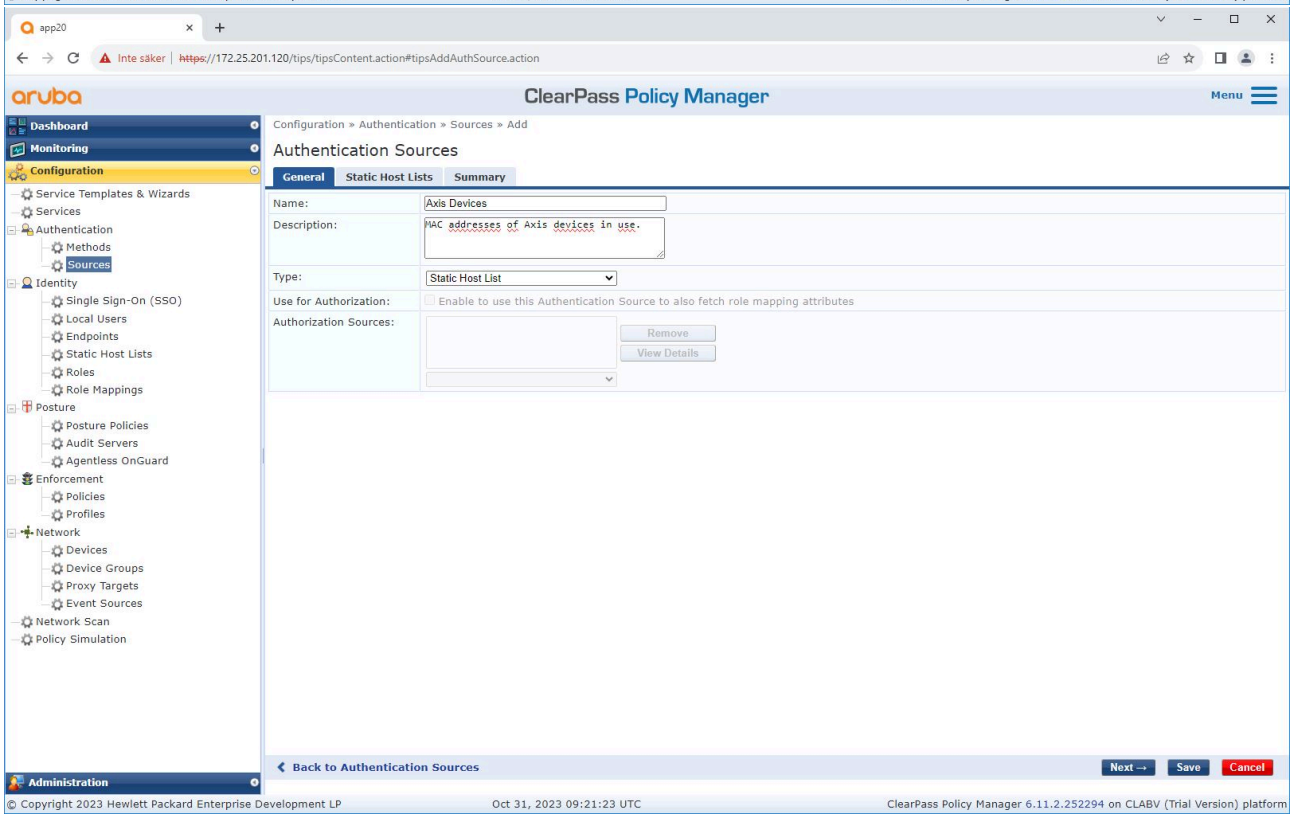
- Der Zugriff erfolgt an einem Wochentag von Montag bis Freitag.
- Der Zugriff erfolgt in einer Zeit zwischen 9:00 und 17:00 Uhr.
- Der mit der MAC-Adresse Hersteller ist Axis Communications.

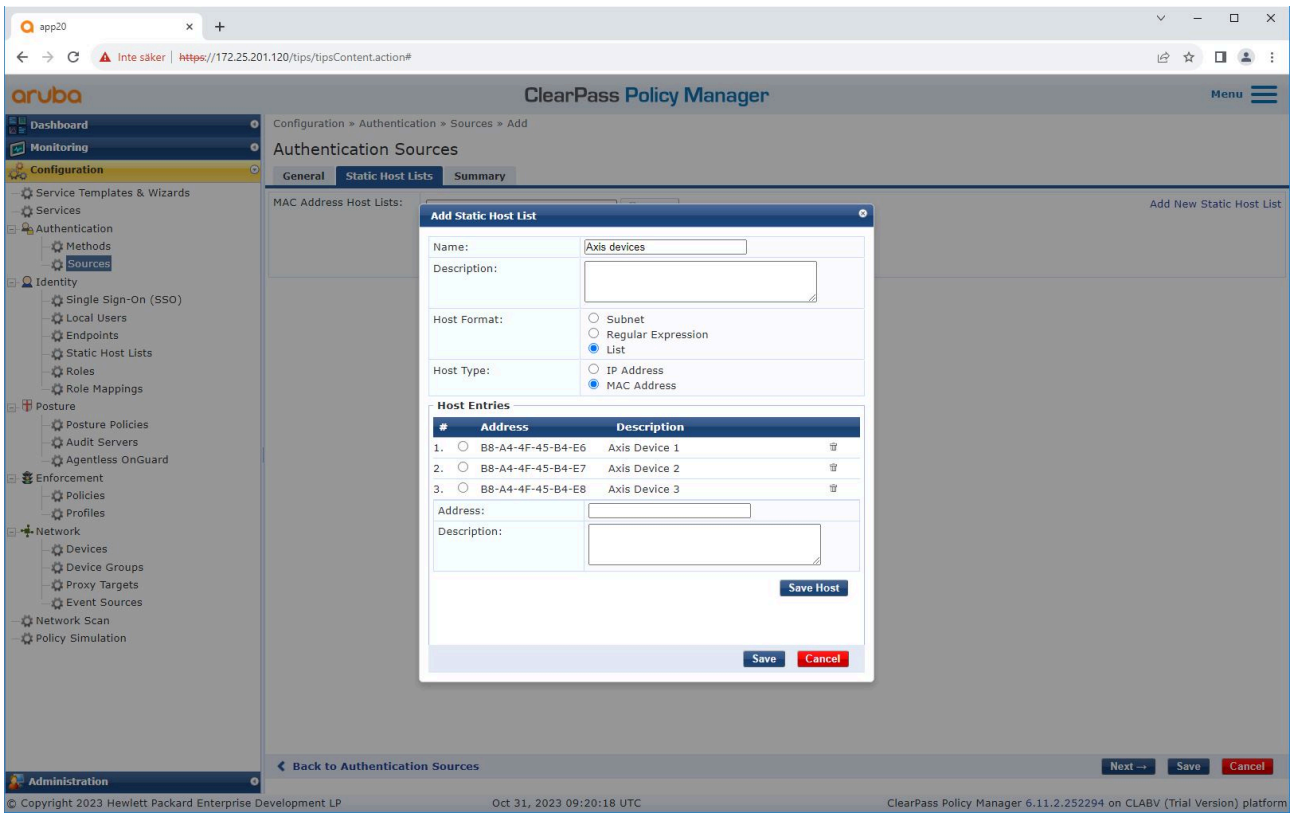
Da es möglich ist, MAC-Adressen zu fälschen, wird der Zugriff auf das reguläre Bereitstellungsnetzwerk nicht gewährt. Wir empfehlen, dass Sie MAB nur für das erste Onboarding verwenden und das Gerät im Weiteren manuell überprüfen.

Quellenkonfiguration

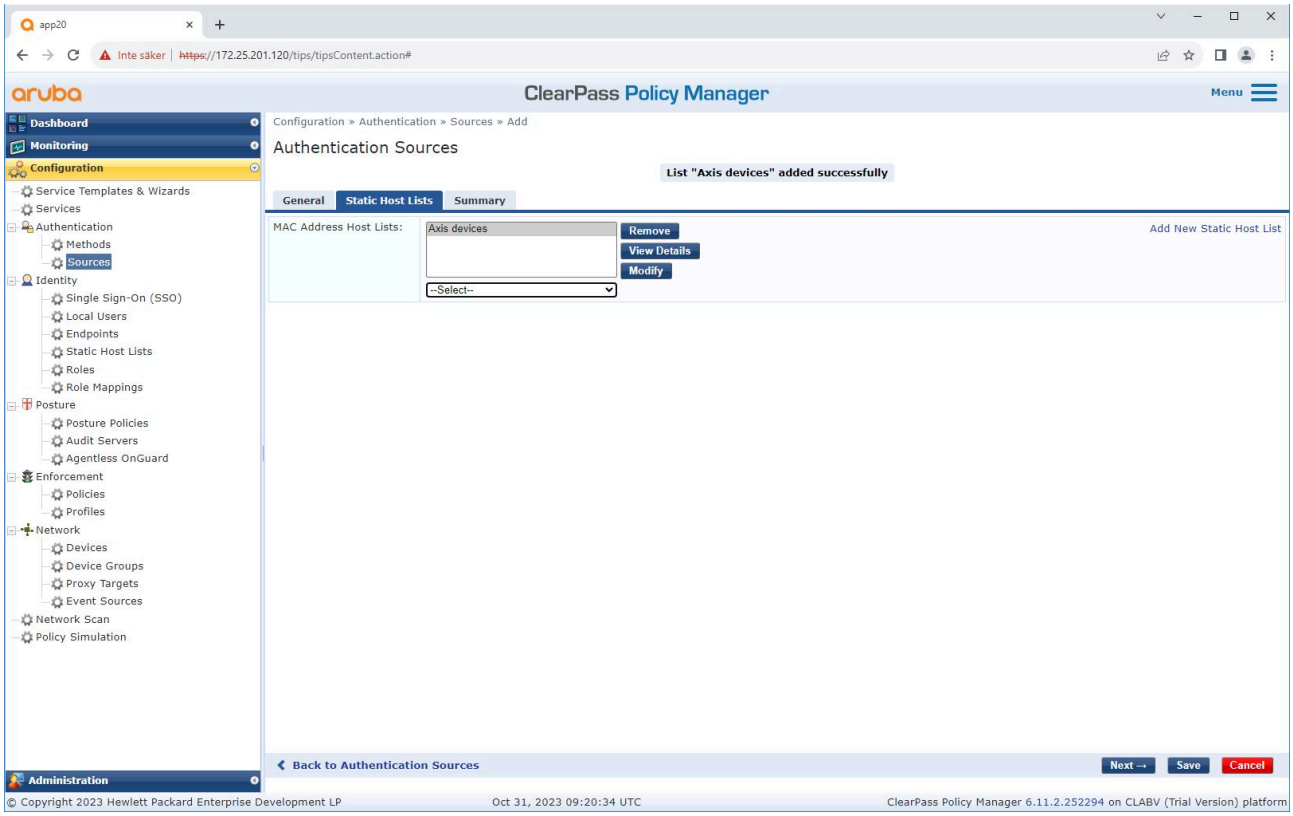
Auf der Seite **Sources (Quellen)** wird eine neue Authentifizierungsquelle erstellt, um nur manuell importierte MAC Adressen zuzulassen.





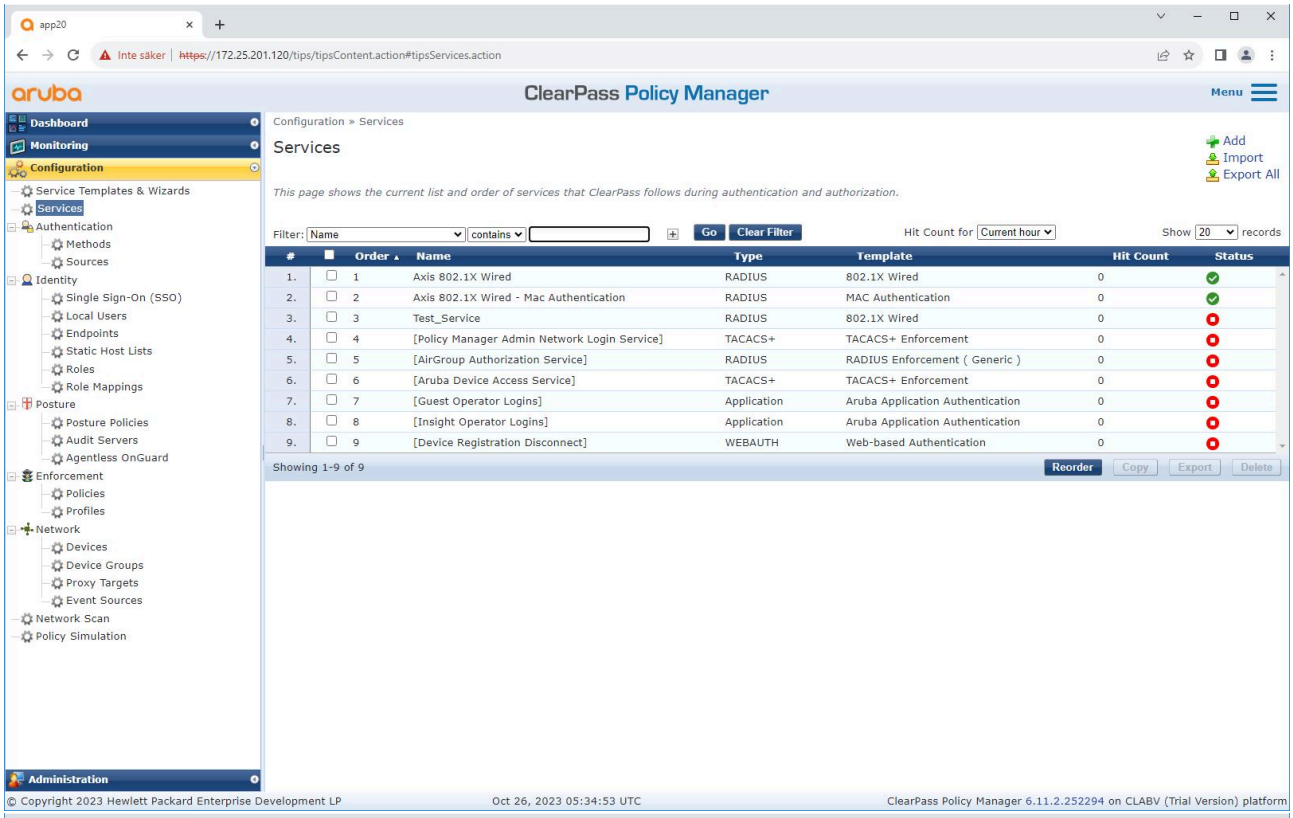


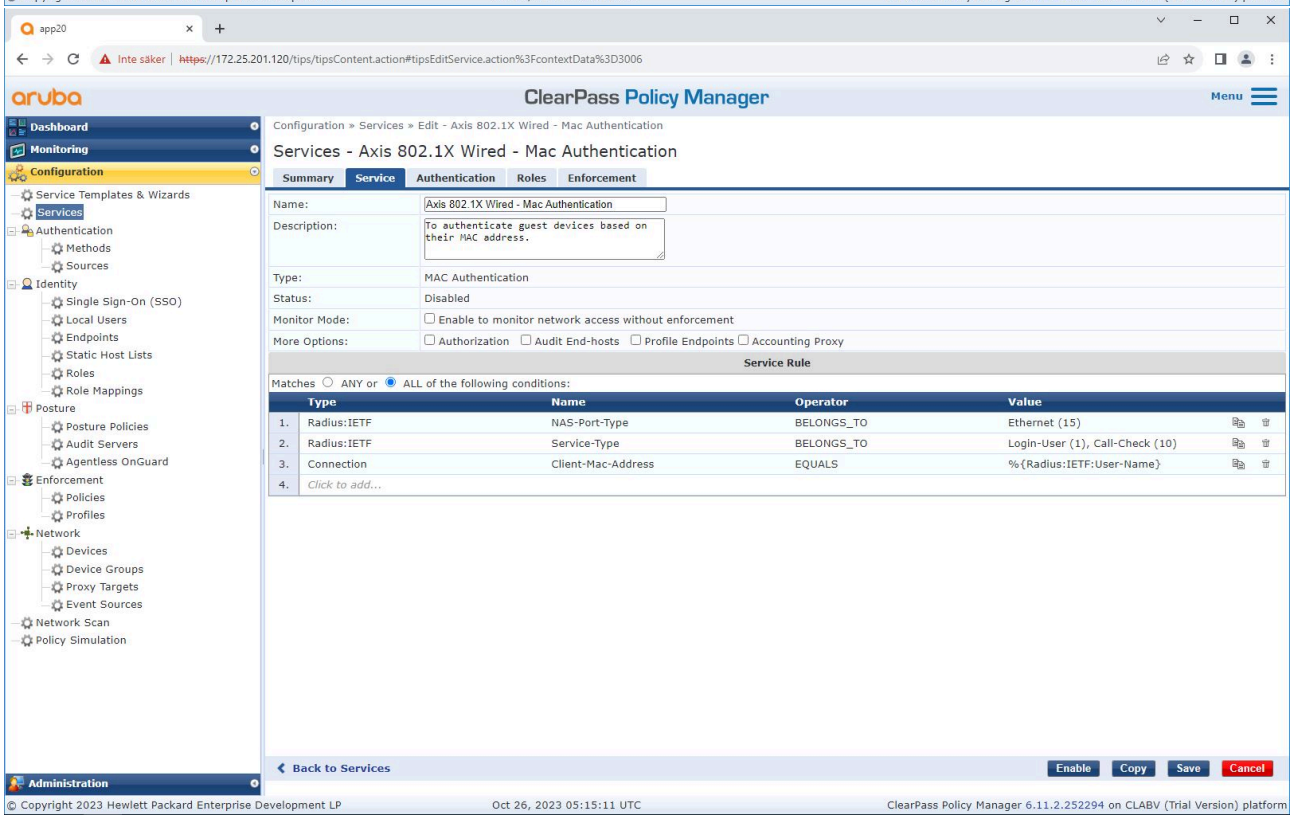
Eine statische Hostliste mit dem Axis MAC-Adressen wird erstellt.



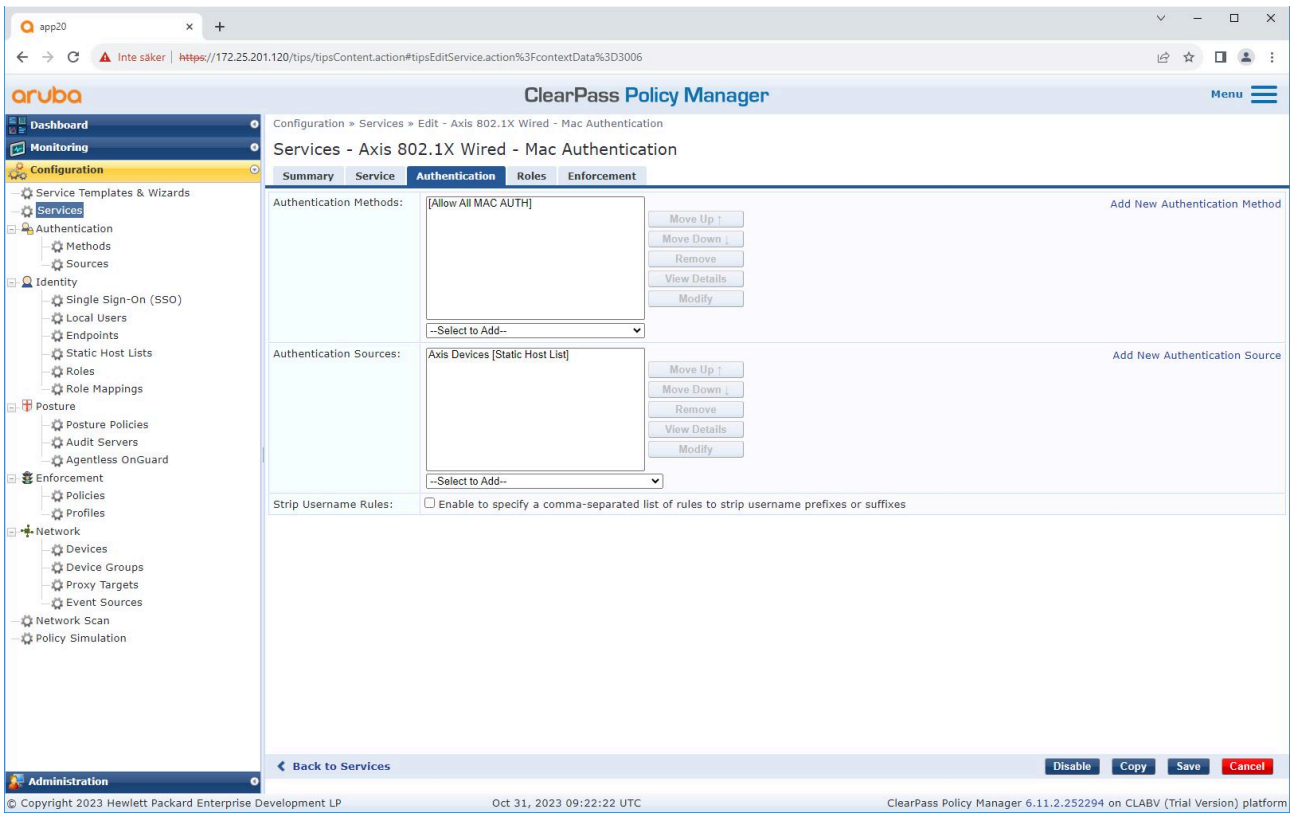
Servicekonfiguration

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.





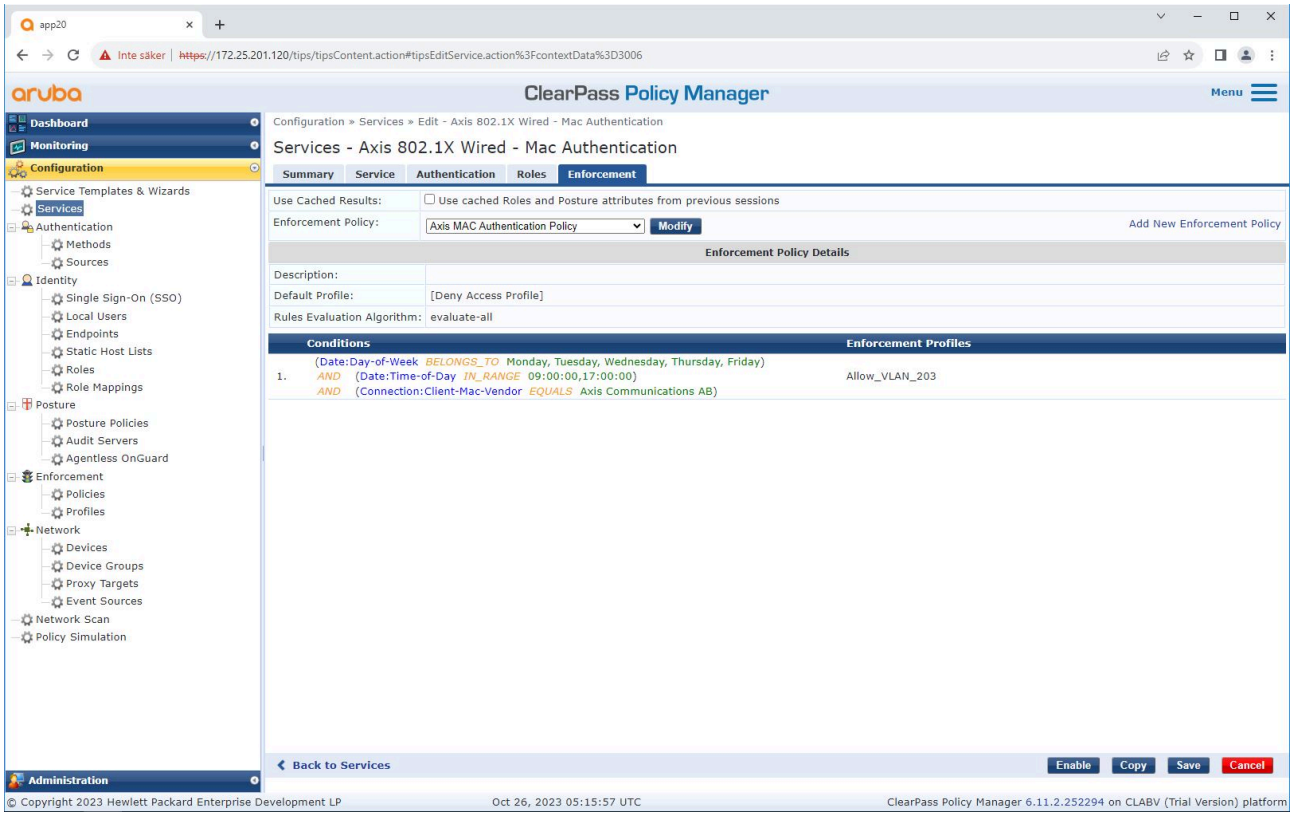
Es wird ein dedizierter Axis Dienst erstellt, der MAB als Verbindungsmethode definiert.



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



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)