HPE Aruba Networking

Manuale dell'utente

Indice

Introduzione....3
Onboarding sicuro: IEEE 802.1AR/802.1X....4
- Autenticazione iniziale....4
- Provisioning....4
- Rete di produzione....5
- Configurazione HPE Aruba Networking....6
  - HPE Aruba Networking ClearPass Policy Manager....6
  - Switch di accesso HPE Aruba Networking....15
- Axis configurazione....16
  - Dispositivo con tecnologia di rete Axis....16
  - AXIS Device Manager....17

Funzionamento sicuro della rete: IEEE 802.1AE MACsec....18
- HPE Aruba Networking ClearPass Policy Manager....19
  - Ruolo e policy di mappatura del ruolo....19
  - Configurazione del servizio....20
  - Profilo esecutivo....21
- Switch di accesso HPE Aruba Networking....22

Gestione certificati – Registrazione tramite trasporto sicuro (EST)....23
- Vantaggi principali di EST....23
- Configurazione HPE Aruba ClearPass integrata....23
- Configurazione HPE Aruba ClearPass Policy Manager....25
- Axis configurazione....28

Onboarding legacy: autenticazione MAC....33
- HPE Aruba Networking ClearPass Policy Manager....33
  - Politica di applicazione....33
  - Configurazione di origine....34
  - Configurazione del servizio....35
- Switch di accesso HPE Aruba Networking....38

Introduzione

La presente guida all'integrazione descrive la configurazione ottimale per l'integrazione e l'operazione dei dispositivi Axis nelle reti HPE Aruba Networking. La configurazione utilizza protocolli e standard di sicurezza moderni come IEEE 802.1X, IEEE 802.1AR, IEEE 802.1AE e HTTPS.

Stabilire un'automazione adeguata per l'integrazione della rete può far risparmiare tempo e denaro. Rimuove inutili complessità di sistema quando si utilizzano applicazioni di gestione dei dispositivi Axis con infrastrutture e applicazioni HPE Aruba Networking. Combinando i dispositivi e il software Axis con un'infrastruttura HPE Aruba Networking, è possibile ottenere i seguenti vantaggi:

- Rimozione di reti di staging dei dispositivi per ridurre al minimo la complessità del sistema.
- Aggiunta di processi di onboarding integrati e la gestione dei dispositivi contribuiscono a ridurre i costi.
- I dispositivi Axis offrono controlli di protezione della rete zero-touch.
- Maggiore protezione complessiva della rete grazie all'esperienza di HPE e Axis.

Per garantire una transizione fluida e definita dal software tra reti logiche durante tutto il processo di onboarding, l'infrastruttura di rete deve essere predisposta per verificare in modo sicuro l'integrità dei dispositivi Axis prima di avviare la configurazione. Prima di procedere con la configurazione, è necessario disporre di quanto segue:

- Esperienza di infrastruttura IT di gestione rete aziendale di HPE Aruba Networking, inclusi switch di accesso HPE Aruba Networking e HPE Aruba Networking ClearPass Policy Manager.
- Competenza nelle moderne tecniche di controllo dell'accesso alla rete e nelle politiche di sicurezza della rete.
- È auspicabile una conoscenza di base precedente dei dispositivi Axis, tuttavia nella guida vengono fornite tutte le indicazioni necessarie.

Onboarding sicuro: IEEE 802.1AR/802.1X



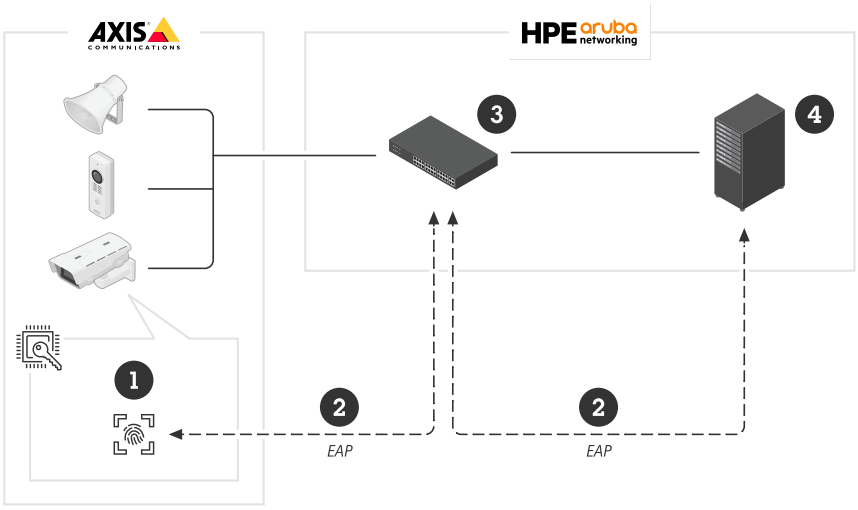
Onboarding sicuro dei dispositivi su reti non attendibili con IEEE 802.1X/802.1AR

Autenticazione iniziale

Quando il dispositivo Axis supportato da Axis Edge Vault è connesso alla rete, utilizza il certificato ID dispositivo Axis IEEE 802.1AR attraverso il (sistema) di controllo degli accessi alla rete IEEE 802.1X per l'autenticazione.

Per garantire l'accesso alla rete, ClearPass Policy Manager verifica l'ID del dispositivo Axis insieme ad altre impronte digitali specifiche del dispositivo. Queste informazioni, quali il MAC address e la versione del sistema operativo AXIS OS del dispositivo, vengono utilizzate per prendere decisioni basate su criteri prestabiliti.

Il dispositivo Axis esegue l'autenticazione sulla rete utilizzando il certificato ID dispositivo Axis conforme a IEEE 802.1AR.

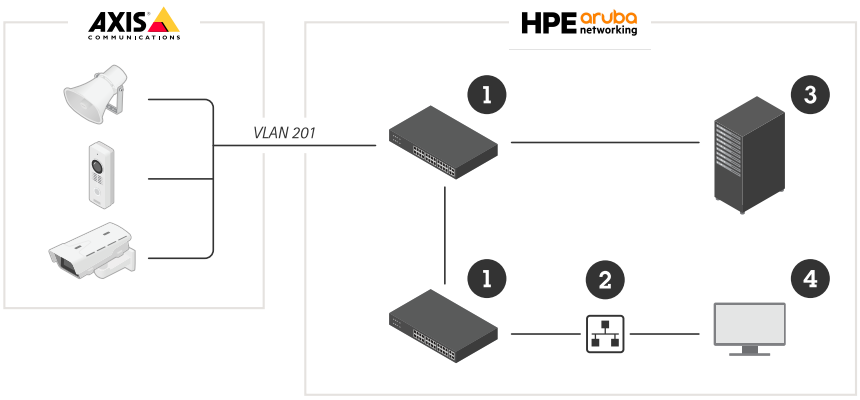


Il dispositivo Axis esegue l'autenticazione sulla rete di HPE Aruba Networking utilizzando il certificato ID dispositivo Axis conforme a IEEE 802.1AR.

1. *ID dispositivo Axis*
2. *Autenticazione di rete IEEE 802.1x EAP-TLS*
3. *Switch di accesso (autenticatore)*
4. *ClearPass Policy Manager*

Provisioning

Dopo l'autenticazione, il dispositivo Axis passa alla rete di provisioning (VLAN201). Questa rete include AXIS Device Manager, che esegue la configurazione dei dispositivi, il rafforzamento della sicurezza e gli aggiornamenti del sistema operativo AXIS OS. Per completare il provisioning, sul dispositivo vengono caricati nuovi certificati di livello produttivo specifici del cliente per IEEE 802.1X e HTTPS.

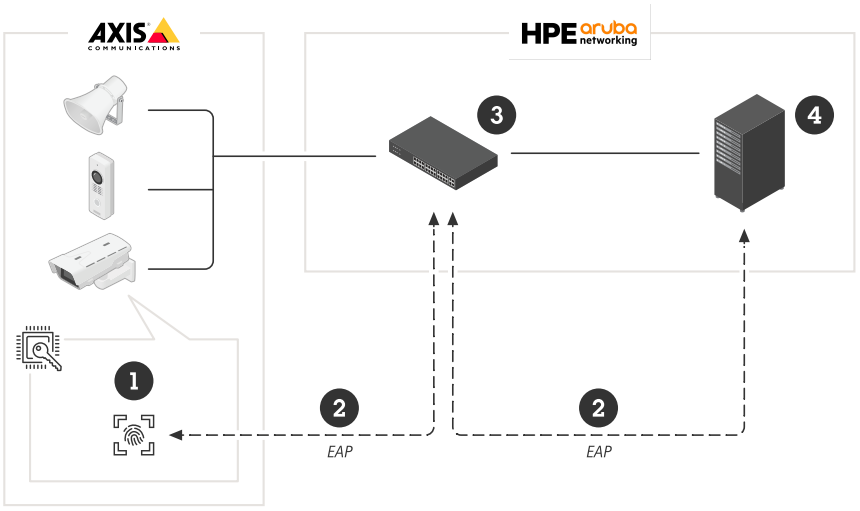


Dopo l'autenticazione, il dispositivo Axis passa a una rete di provisioning per la configurazione.

1 *Interruttore di accesso*
2 *Rete di provisioning*
3 *ClearPass Policy Manager*
4 *Applicazione di gestione del dispositivo*

Rete di produzione

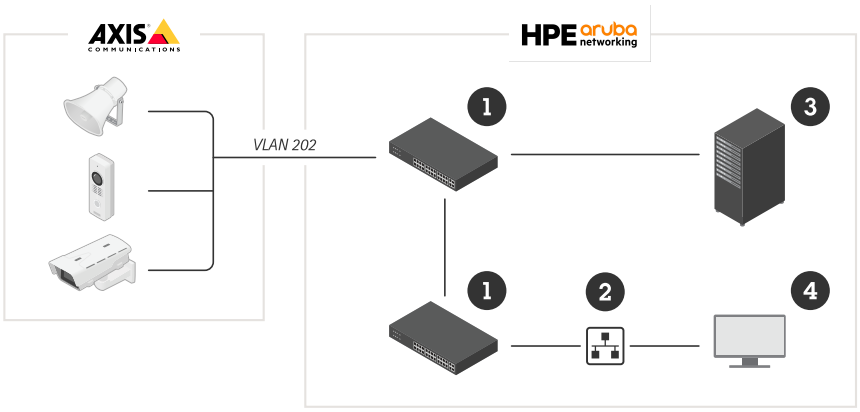
Il provisioning del dispositivo Axis con nuovi certificati IEEE 802.1X attiva un nuovo tentativo di autenticazione. ClearPass Policy Manager verifica i nuovi certificati e decide se spostare o meno il dispositivo Axis nella rete di produzione.



Dopo la configurazione, il dispositivo Axis esce dalla rete di provisioning e tenta di eseguire nuovamente l'autenticazione sulla rete.

1 *ID dispositivo Axis*
2 *Autenticazione di rete IEEE 802.1x EAP-TLS*
3 *Switch di accesso (autenticatore)*
4 *ClearPass Policy Manager*

Dopo la ripetizione dell'autenticazione, il dispositivo Axis passa alla rete di produzione (VLAN 202), dove il Video Management System (VMS) si connette al dispositivo e avvia l'operazione.



Al dispositivo Axis viene concesso l'accesso alla rete di produzione.

1 *Interruttore di accesso*
2 *Rete di produzione*
3 *ClearPass Policy Manager*
4 *Sistema di gestione video*

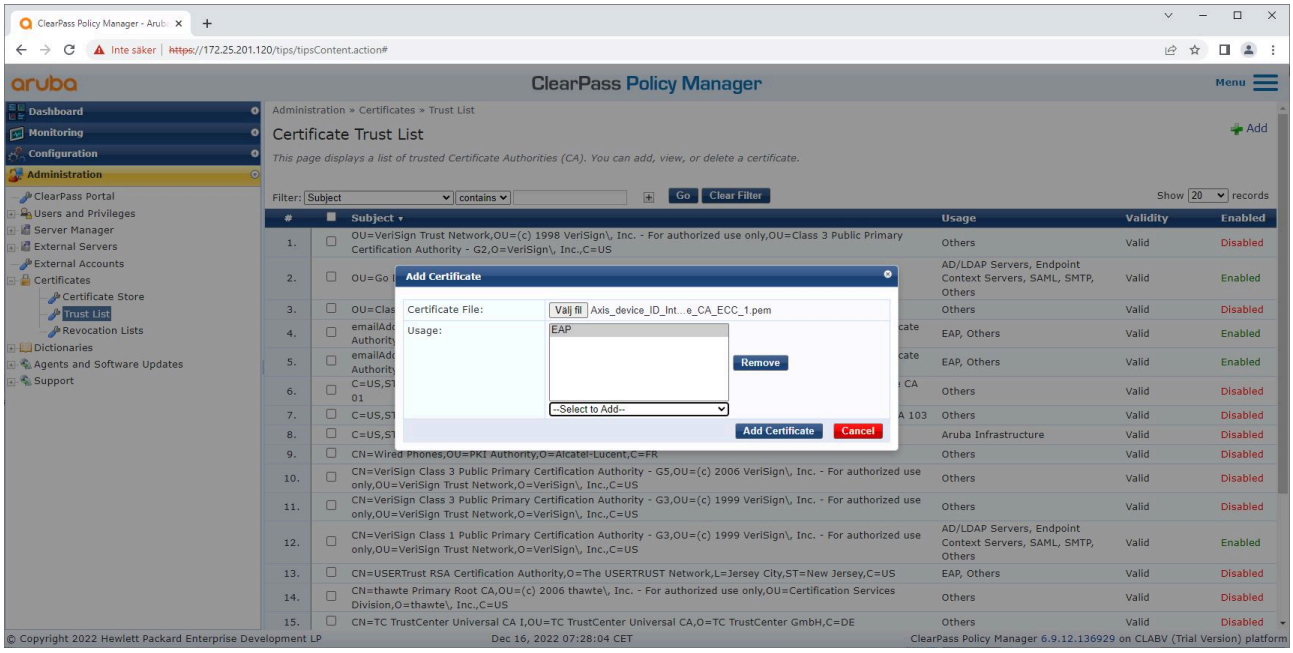
Configurazione HPE Aruba Networking

HPE Aruba Networking ClearPass Policy Manager

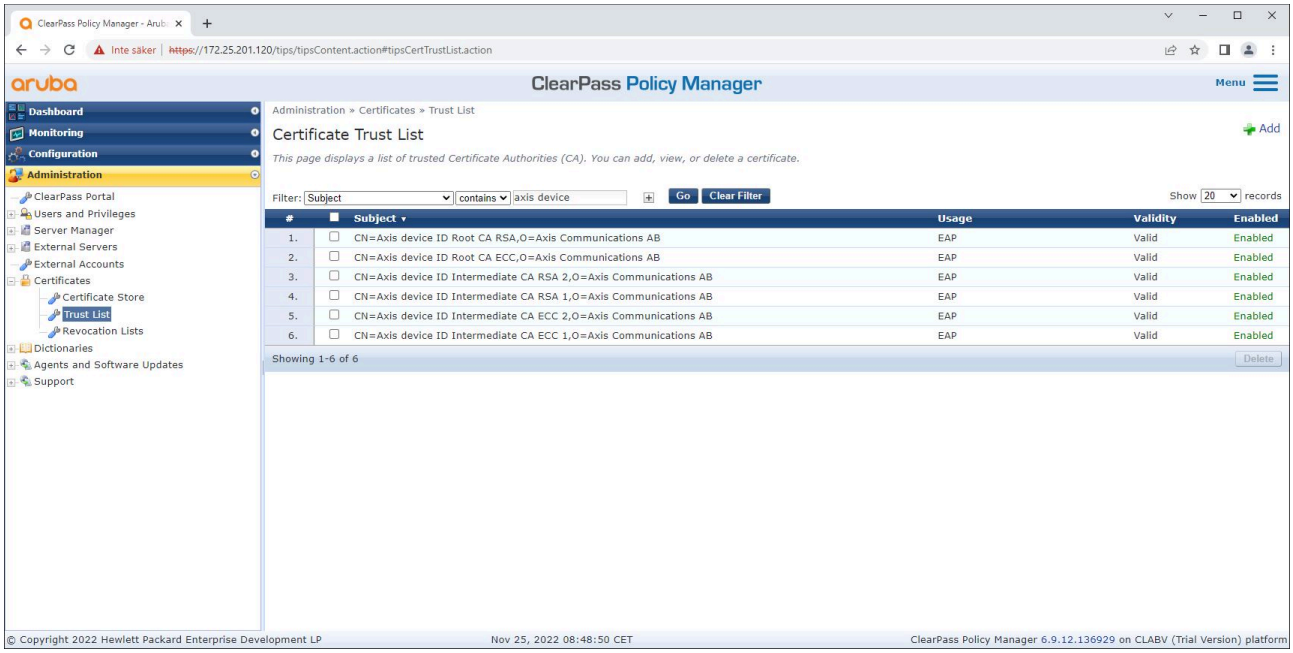
ClearPass Policy Manager fornisce un controllo sicuro degli accessi di rete basato su ruoli e dispositivi per IoT, BYOD, dispositivi aziendali, dipendenti, collaboratori esterni e ospiti su infrastrutture cablate, wireless e VPN multivendor.

Configurazione dell'archivio certificati attendibili

1. Scaricare la catena di certificati IEEE 802.1AR specifica di Axis da axis.com.
2. Caricare le catene di certificati della CA radice e della CA intermedia IEEE 802.1AR specifiche di Axis nell'archivio certificati attendibili.
3. Abilitare ClearPass Policy Manager per autenticare i dispositivi Axis tramite IEEE 802.1X EAP-TLS.
4. Selezionare EAP nel campo di utilizzo. I certificati sono utilizzati per l'autenticazione IEEE 802.1X EAP-TLS.



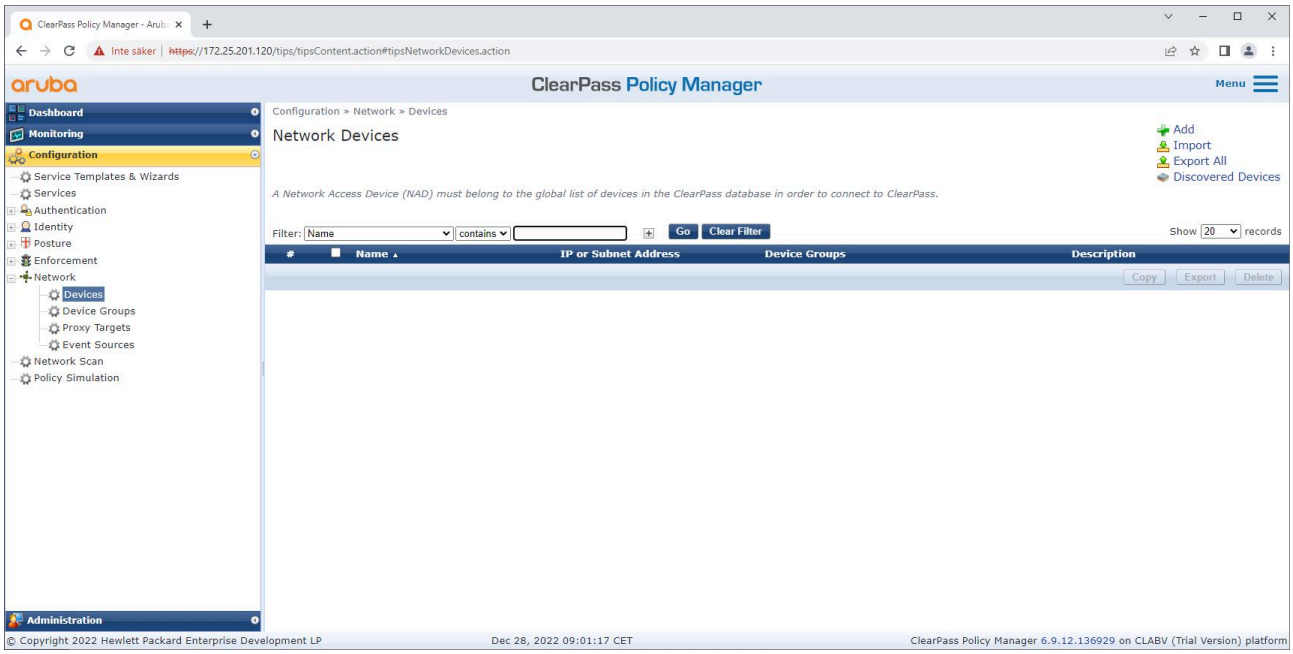
Caricare i certificati IEEE 802.1AR specifici di Axis nell'archivio certificati attendibili di ClearPass Policy Manager.



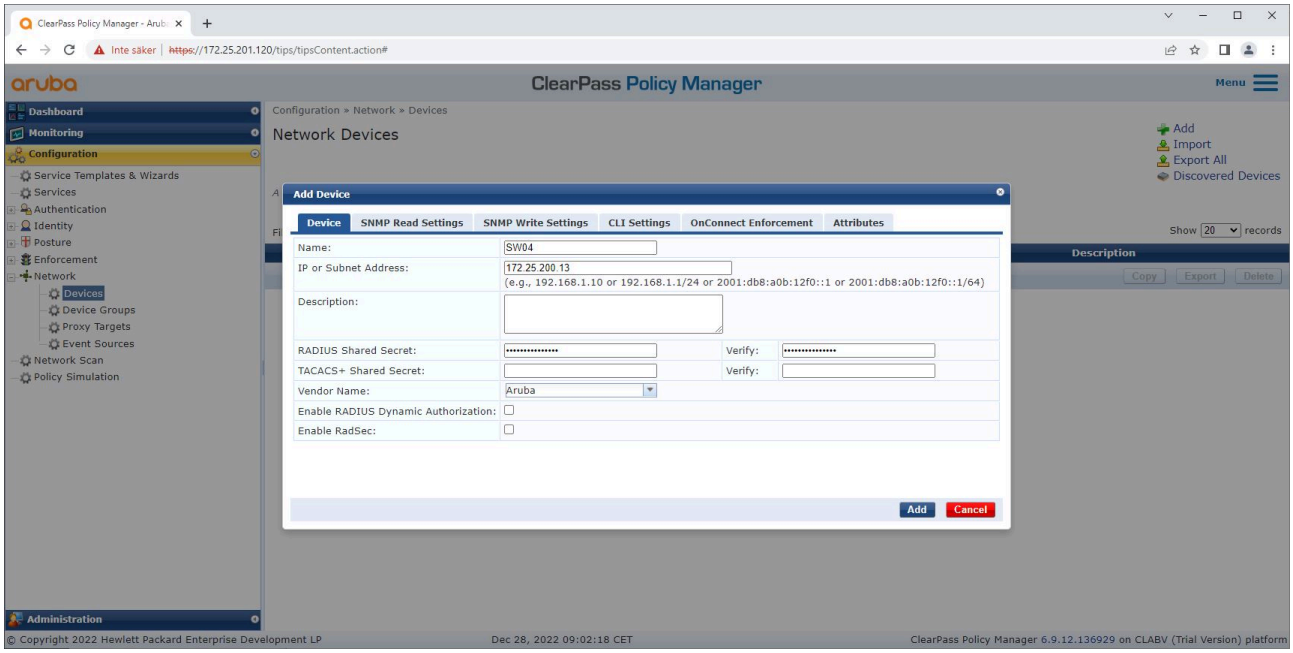
L'archivio certificati attendibili in ClearPass Policy Manager con catena di certificati IEEE 802.1AR specifica di Axis inclusa.

Configurazione del dispositivo/gruppo di rete

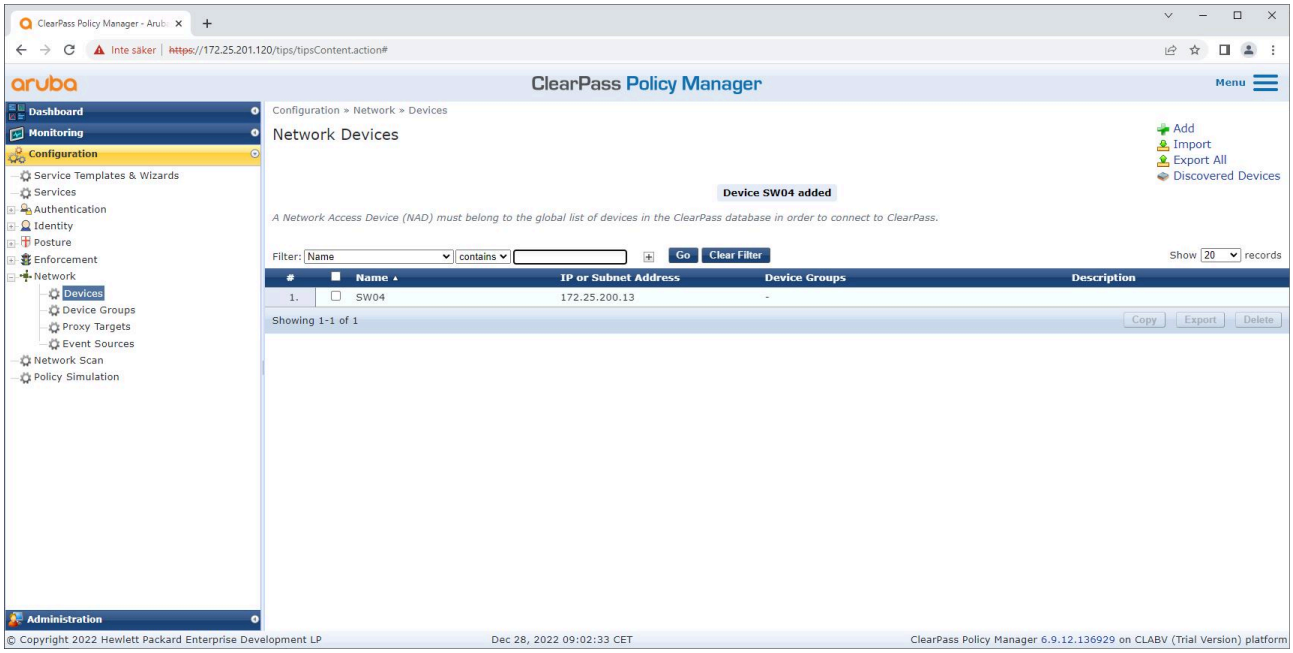
1. Aggiungere dispositivi di accesso alla rete affidabili come gli switch di accesso HPE Aruba Networking a ClearPass Policy Manager. ClearPass Policy Manager deve sapere quali switch di accesso nella rete sono utilizzati per la comunicazione IEEE 802.1X. Si noti inoltre che il segreto condiviso RADIUS deve corrispondere alla configurazione IEEE 802.1X specifica dello switch.
2. Utilizzare la configurazione del gruppo di dispositivi di rete per raggruppare più dispositivi di accesso alla rete attendibili. Il raggruppamento dei dispositivi semplifica la configurazione della politica.



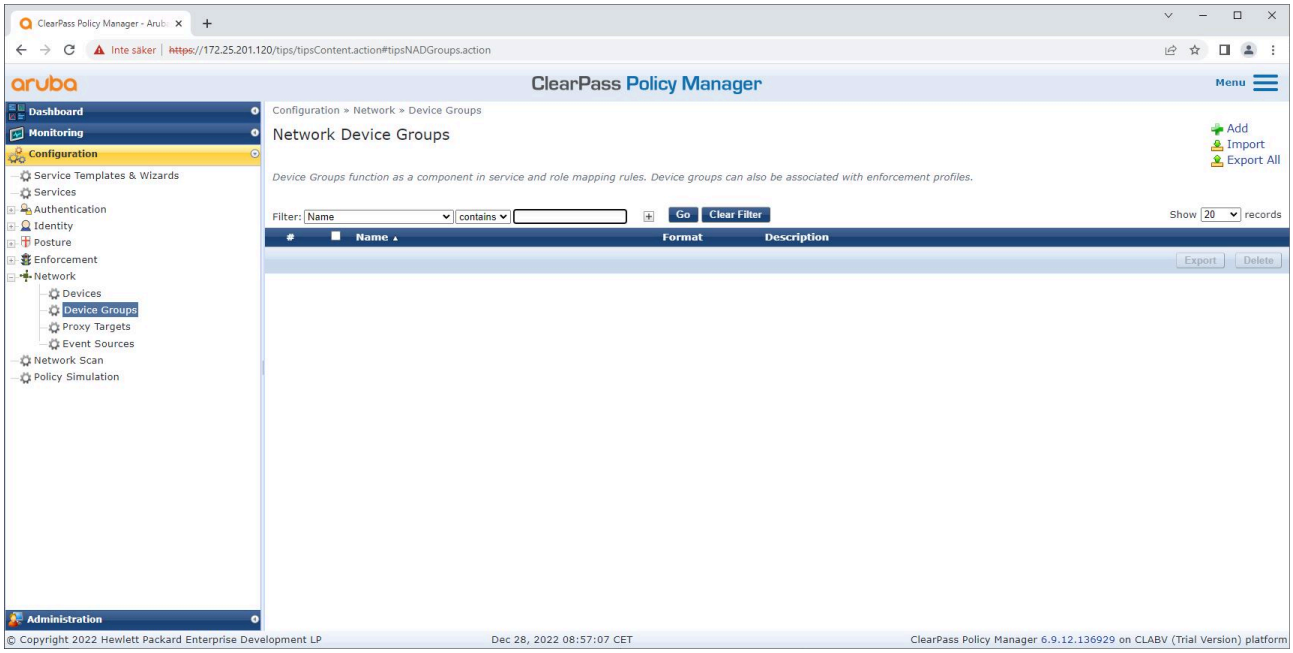
L'interfaccia dei dispositivi di rete attendibili in ClearPass Policy Manager.



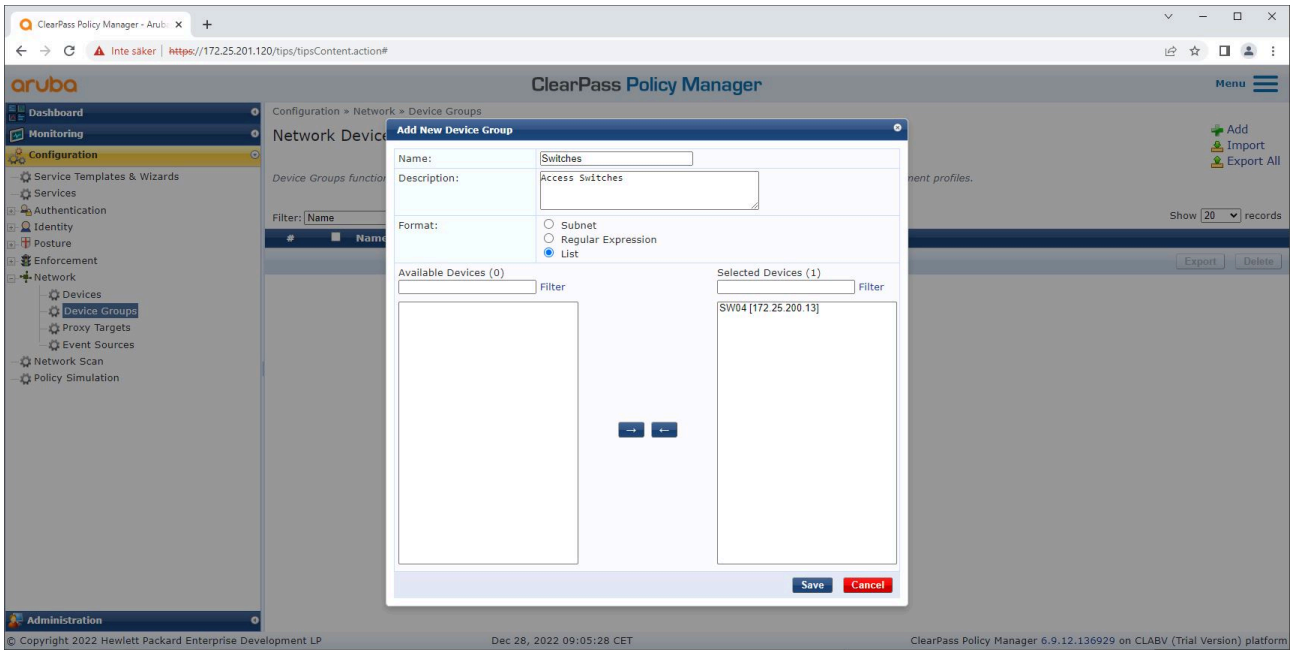
Aggiungere lo switch di accesso HPE Aruba Networking come un dispositivo affidabile in ClearPass Policy Manager. Si noti che il segreto condiviso RADIUS deve corrispondere alla configurazione IEEE 802.1X specifica dello switch.



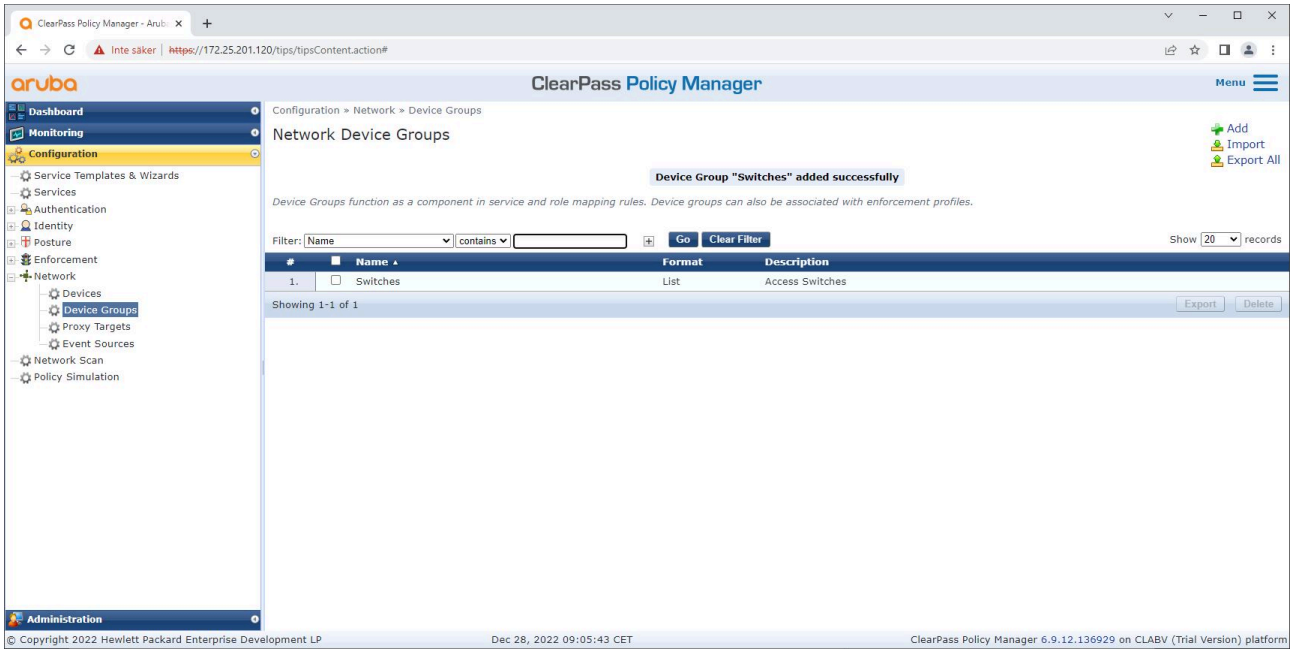
ClearPass Policy Manager con un singolo dispositivo di rete affidabile configurato.



Interfaccia dei gruppi di dispositivo di rete attendibili in ClearPass Policy Manager.



Aggiungere un dispositivo di accesso alla rete attendibile su un nuovo gruppo di dispositivi in ClearPass Policy Manager.

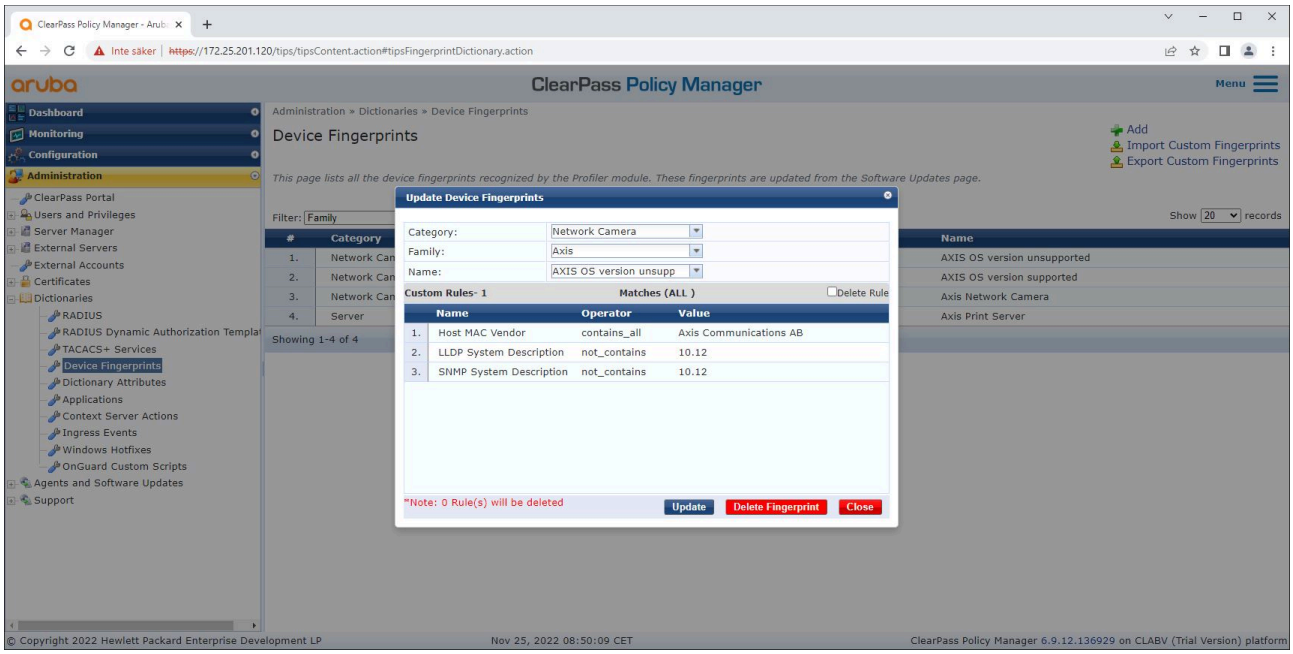


ClearPass Policy Manager con un gruppo di dispositivi di rete configurato che include uno o più dispositivi di rete attendibili.

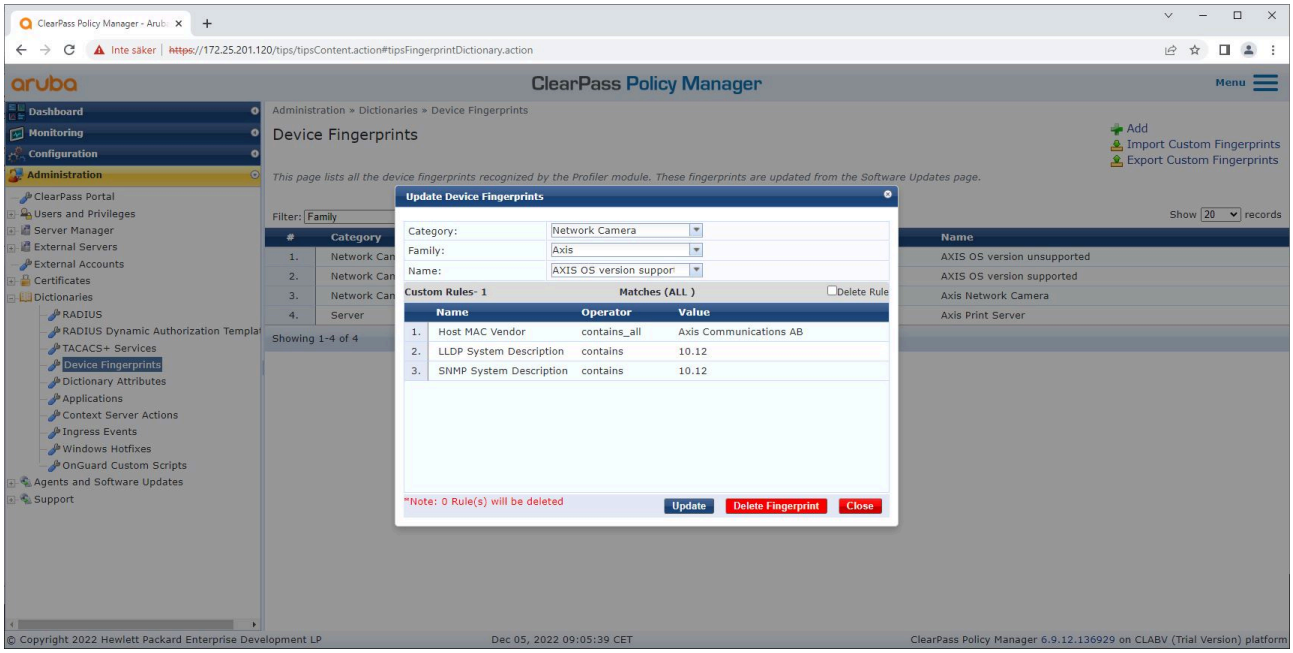
Configurazione dell'impronta digitale del dispositivo

Il dispositivo Axis può, tramite il rilevamento di rete, distribuire informazioni specifiche sul dispositivo, quali il MAC address e la versione del software del dispositivo. L'utente può utilizzare tali informazioni per la creazione, l'aggiornamento o la gestione dell'impronta digitale di un dispositivo in ClearPass Policy Manager. L'utente può anche concedere o negare l'accesso a seconda della versione di AXIS OS.

1. Andare a **Administration > Dictionaries > Device Fingerprints (Amministrazione > Dizionari > Impronte digitali del dispositivo)**.
2. Selezionare un'impronta digitale del dispositivo esistente o creare una nuova impronta digitale del dispositivo.
3. Configurare le impostazioni dell'impronta digitale del dispositivo.



La configurazione dell'impronta digitale del dispositivo in ClearPass Policy Manager. I dispositivi Axis che utilizzano versioni di AXIS OS diverse dalla 10.12 non sono contemplati in questo esempio.



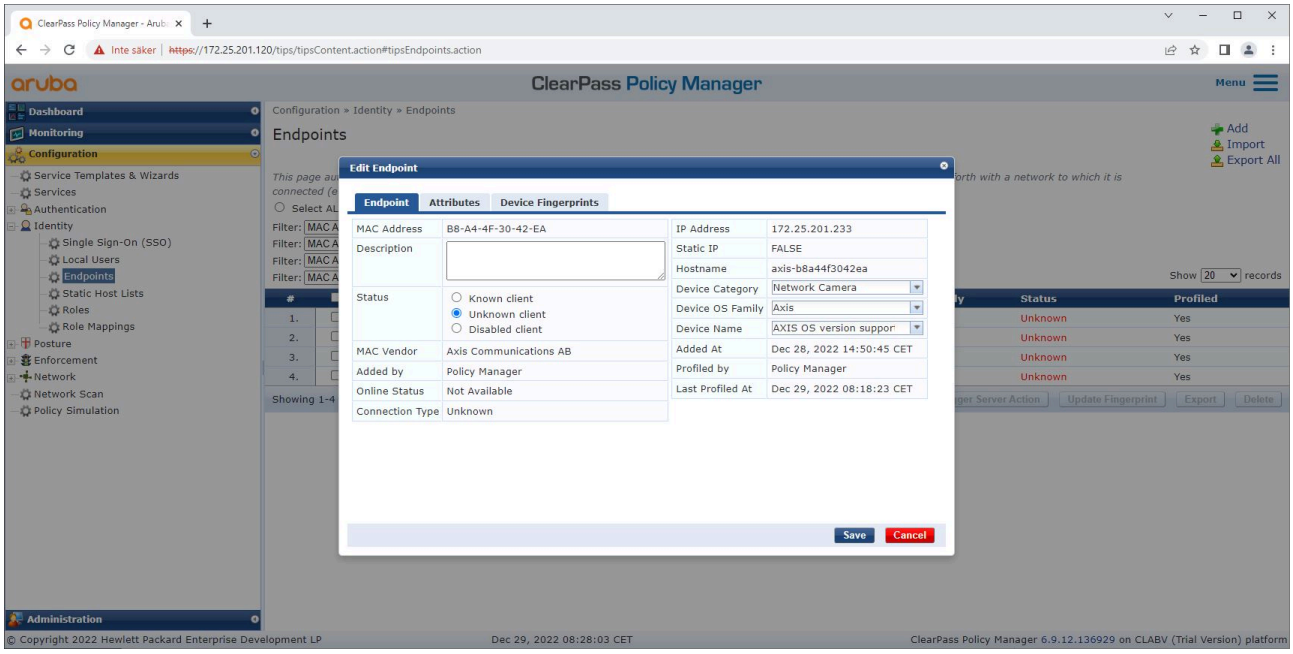
La configurazione dell'impronta digitale del dispositivo in ClearPass Policy Manager. I dispositivi Axis che utilizzano versioni di AXIS OS diverse dalla 10.12 sono contemplati in questo esempio.

Le informazioni sull'impronta digitale del dispositivo raccolte da ClearPass Manager sono disponibili nella sezione Endpoint.

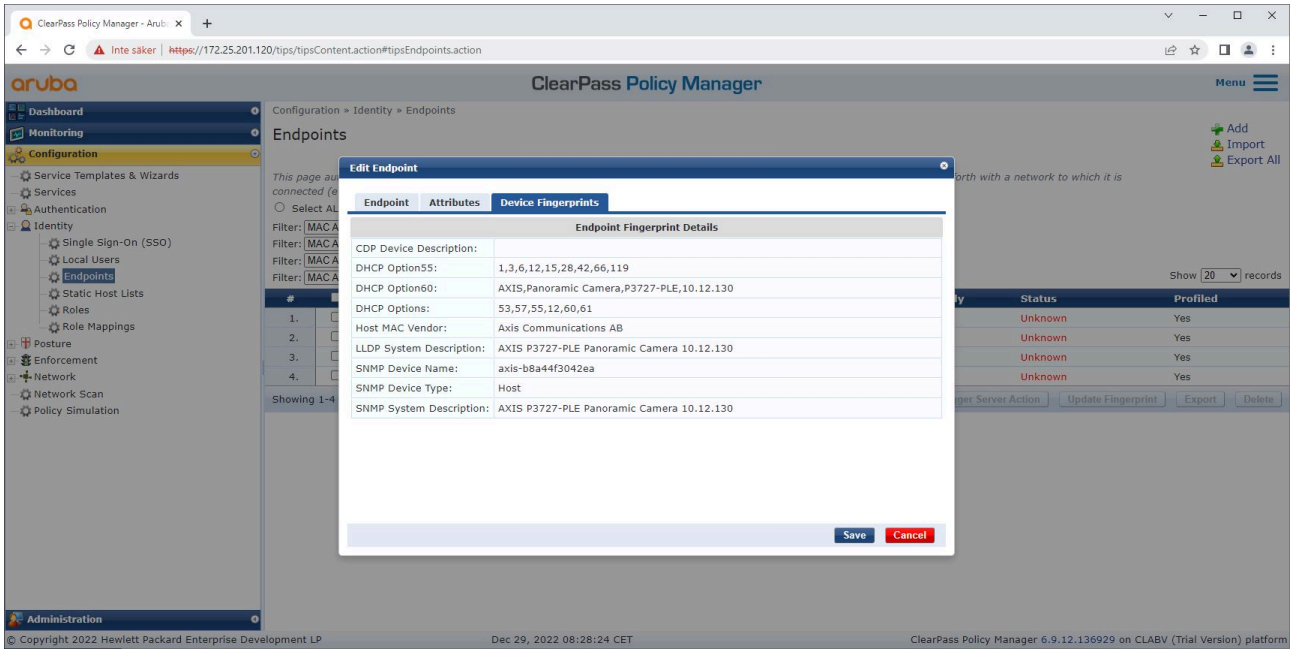
1. Andare a **Configuration > Identity > Endpoints (Configurazione > Identità > Endpoint)**.
2. Selezionare il dispositivo che desideri visualizzare.
3. Fare clic sulla scheda **Device Fingerprints (Impronte digitali)** del dispositivo.

Nota

SNMP è disabilitato per impostazione predefinita nei dispositivi Axis e raccolto dallo switch di accesso HPE Aruba Networking.



Un dispositivo Axis di cui è stato eseguito il profilo da ClearPass Policy Manager.

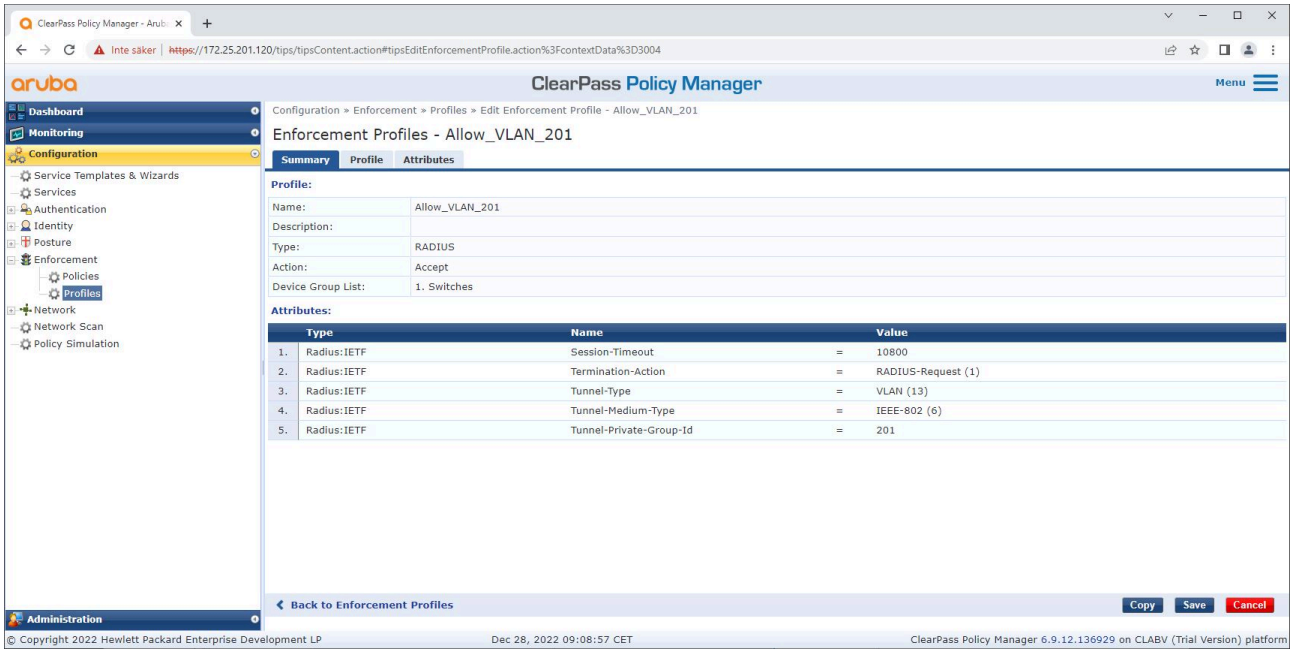


Le Impronte digitali dettagliate di un dispositivo Axis profilato. Si noti che SNMP è disabilitato per impostazione predefinita nei dispositivi Axis. Le informazioni di rilevamento specifiche LLDP, CDP e DHCP sono condivise dal dispositivo Axis nello stato predefinito di fabbrica e vengono inoltrate dallo switch di accesso HPE Aruba Networking a ClearPass Policy Manager.

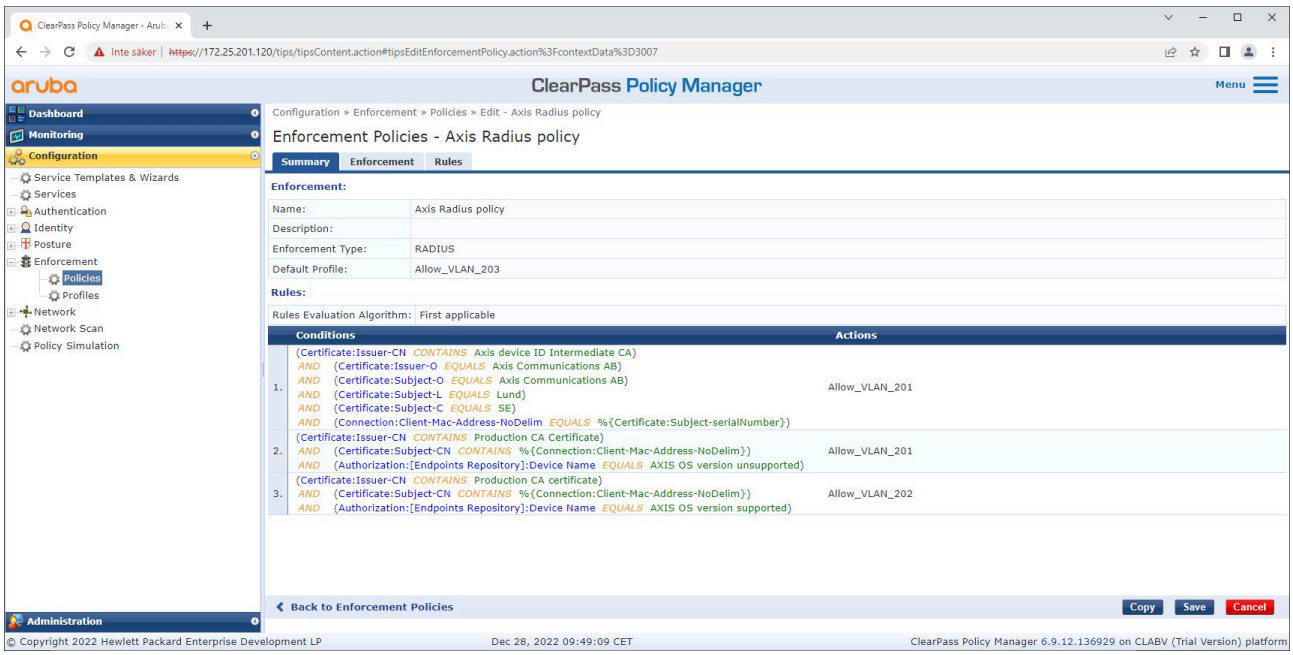
Configurazione del profilo di applicazione

Il profilo esecutivo consente a ClearPass Policy Manager di assegnare un ID VLAN specifico a una porta di accesso sullo switch. Si tratta di una decisione basata su policy che si applica ai dispositivi di rete nel gruppo di dispositivi "switch". Il numero di profili di applicazione necessario dipende dal numero di VLAN in uso. La nostra impostazione dispone di tre VLAN (VLAN 201, 202, 203), che corrispondono a tre profili di applicazione.

Dopo aver configurato i profili di imposizione per la VLAN, è possibile configurare la politica di applicazione stessa. La configurazione della politica di applicazione in ClearPass Policy Manager definisce se ai dispositivi Axis viene concesso l'accesso alle reti di HPE Aruba Networking in base a quattro profili di policy di esempio.



Un profilo di applicazione di esempio per consentire l'accesso alla VLAN 201.



La configurazione della policy di applicazione in ClearPass Policy Manager.

Le quattro politiche di applicazione e le relative azioni sono:

Accesso alla rete negato

L'accesso alla rete viene negato quando non viene eseguita l'autenticazione del controllo degli accessi alla rete IEEE 802.1X.

Rete ospite (VLAN 203)

Al dispositivo Axis viene concesso l'accesso a una rete limitata e isolata se l'autenticazione del controllo degli accessi alla rete IEEE 802.1X non riesce. È quindi necessaria un'ispezione manuale del dispositivo per decidere le azioni appropriate.

Rete di provisioning (VLAN 201)

Al dispositivo Axis viene garantito l'accesso a una rete di provisioning. Questo per fornire funzionalità di gestione dei dispositivi Axis tramite *AXIS Device Manager* e *AXIS Device Manager Extend*. Consente inoltre di configurare i dispositivi Axis con aggiornamenti AXIS OS, certificati di produzione e altre configurazioni. Le seguenti condizioni sono verificate da ClearPass Policy Manager:

- La versione di AXIS OS del dispositivo.
- Il MAC address del dispositivo corrisponde allo schema del MAC address specifico del fornitore con l'attributo del numero di serie del certificato ID del dispositivo Axis.
- Il certificato dell'ID del dispositivo Axis è verificabile e corrisponde agli attributi specifici di Axis come emittente, organizzazione, posizione e paese.

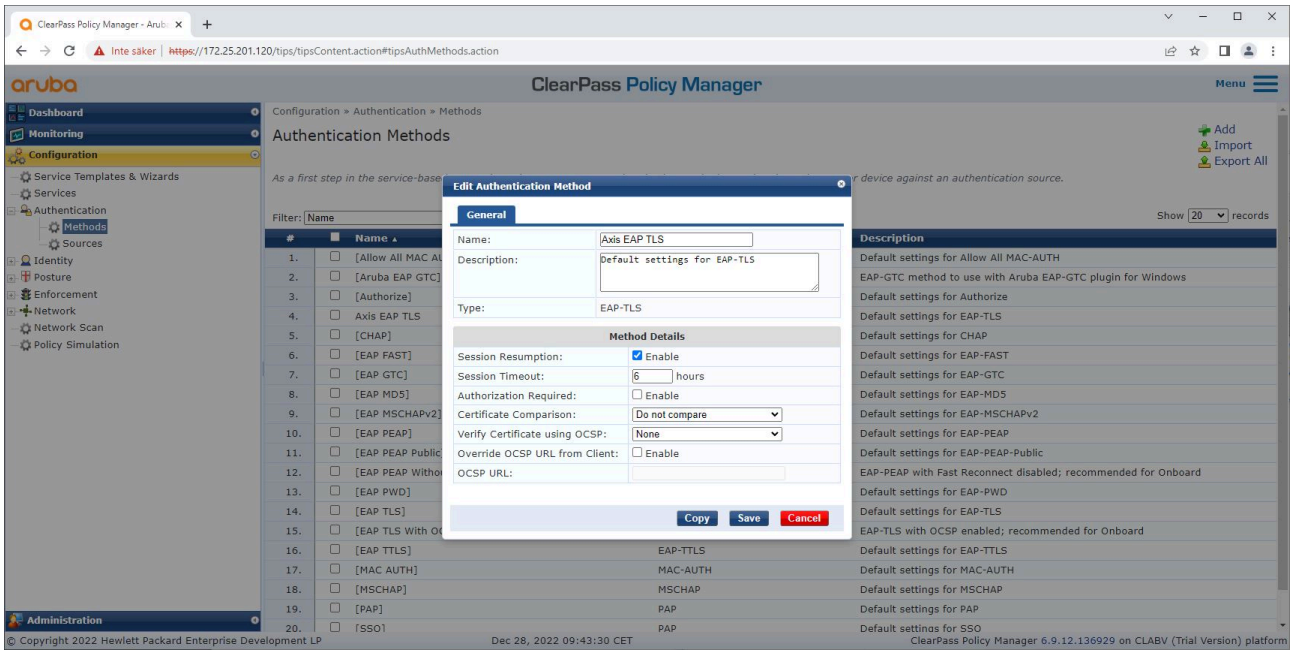
Rete di produzione (VLAN 202)

Al dispositivo Axis viene concesso l'accesso alla rete di produzione in cui opererà. L'accesso è permesso una volta concluso il provisioning del dispositivo dalla rete di provisioning (VLAN 201). Le seguenti condizioni sono verificate da ClearPass Policy Manager:

- La versione di AXIS OS del dispositivo.
- Il MAC address del dispositivo corrisponde allo schema del MAC address specifico del fornitore con l'attributo del numero di serie del certificato ID del dispositivo Axis.
- Il certificato di produzione è verificabile dall'archivio certificati attendibile.

Configurazione del metodo di autenticazione

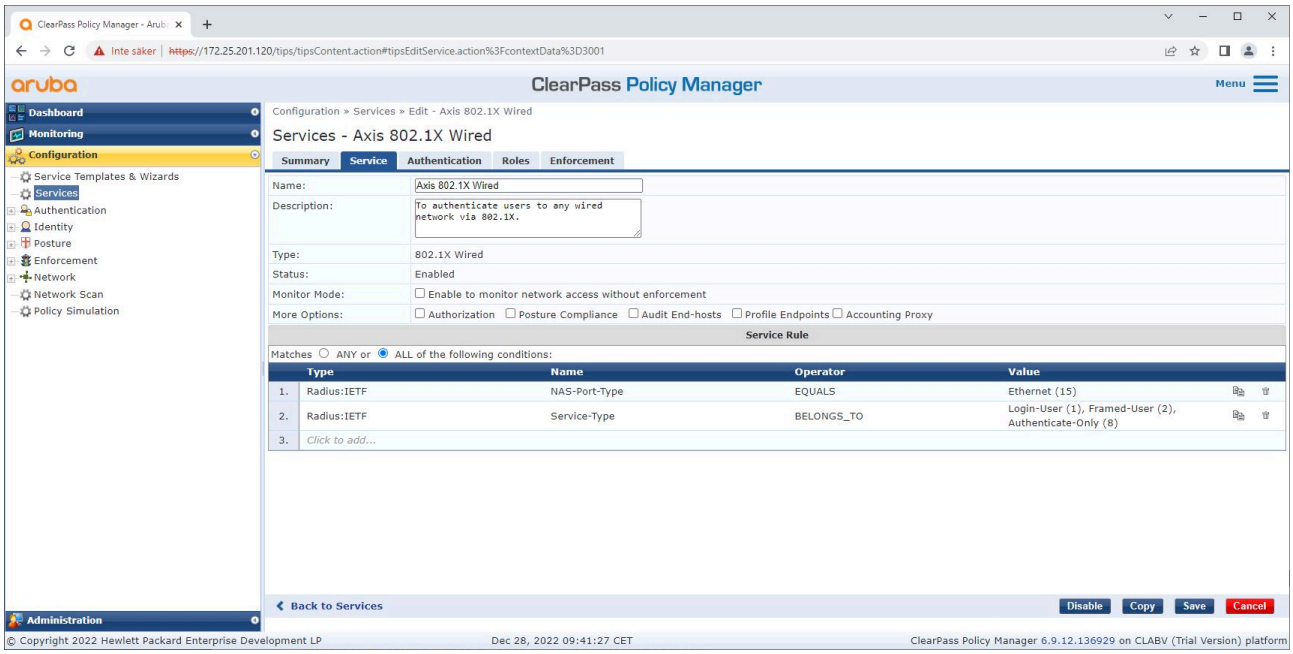
Il metodo di autenticazione definisce il modo in cui un dispositivo Axis tenta di autenticarsi sulla rete. Il metodo preferito è IEEE 802.1X EAP-TLS poiché i dispositivi Axis con Axis Edge Vault vengono forniti con IEEE 802.1X EAP-TLS abilitato per impostazione predefinita.



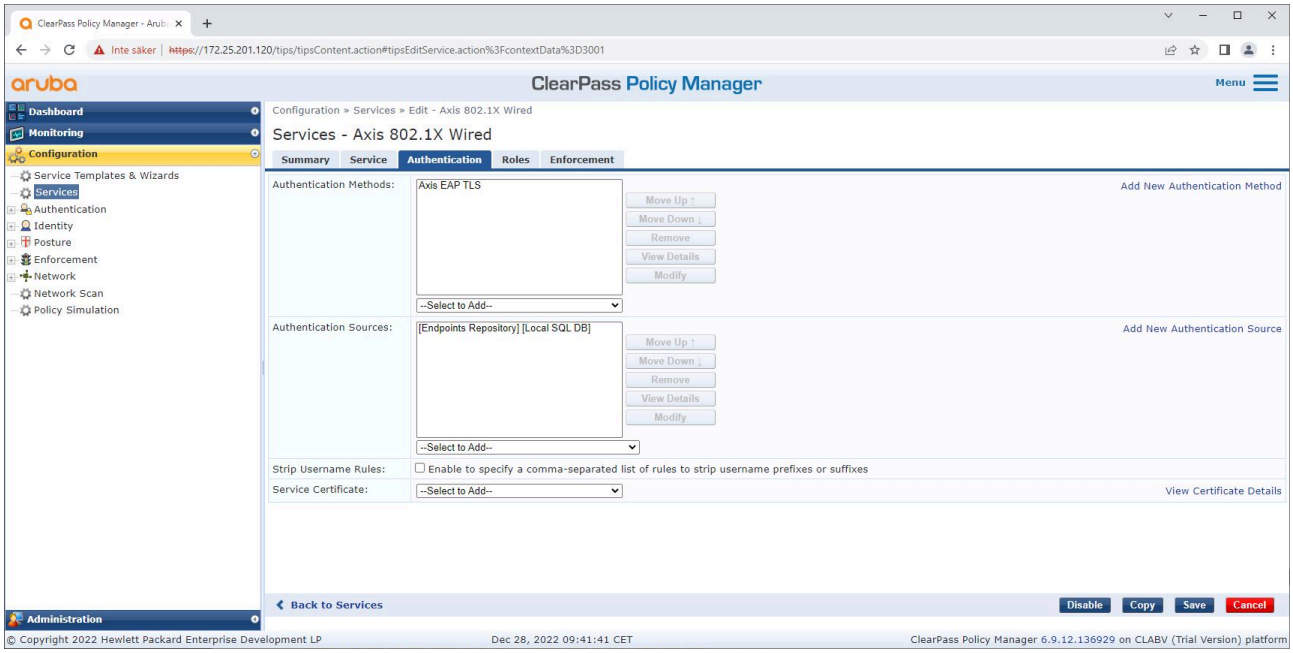
L'interfaccia del metodo di autenticazione di ClearPass Policy Manager, in cui viene definito il metodo di autenticazione EAP-TLS per i dispositivi Axis.

Configurazione del servizio

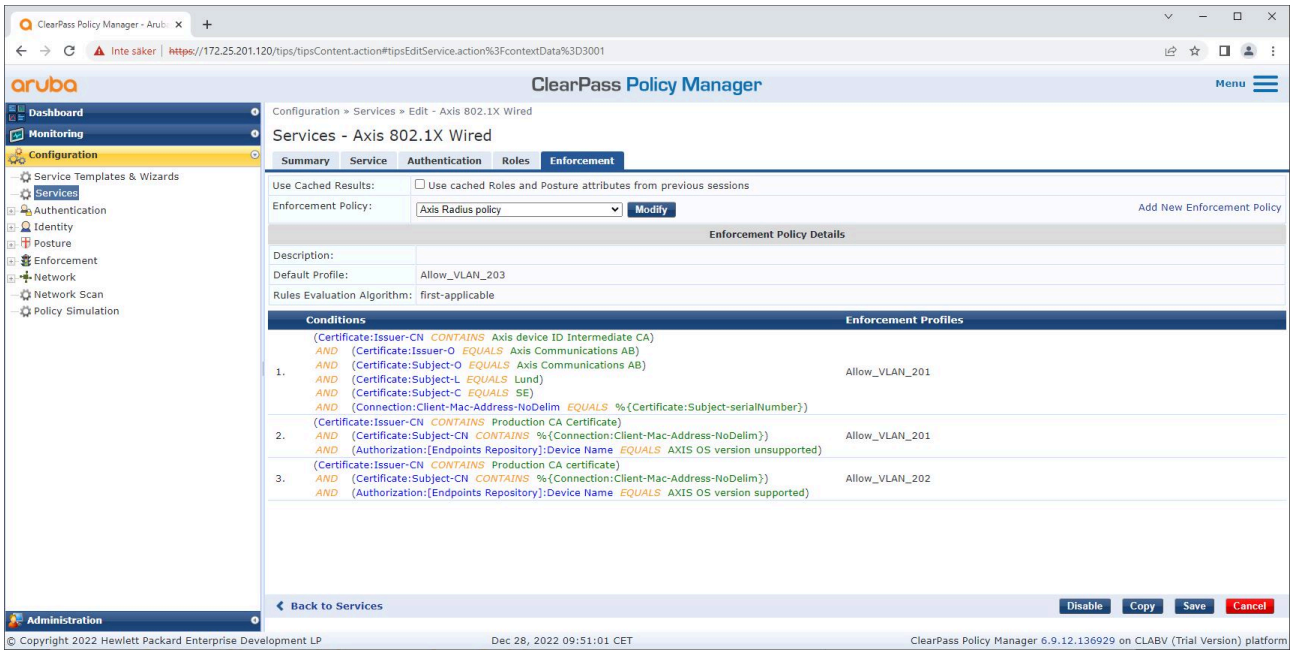
Nella pagina **Services (Servizi)**, i passaggi di configurazione sono riuniti in un singolo servizio che gestisce l'autenticazione e l'autorizzazione dei dispositivi Axis nelle reti HPE Aruba Networking.



Viene creato un servizio Axis dedicato, con IEEE 802.1X come metodo di connessione.



Il metodo di autenticazione EAP-TLS creato in precedenza è configurato per il servizio.



La politica di applicazione creata in precedenza è configurata per il servizio.

Switch di accesso HPE Aruba Networking

I dispositivi Axis sono connessi direttamente agli switch di accesso compatibili con PoE o tramite midspan PoE Axis compatibili. Per eseguire l'onboarding sicuro dei dispositivi Axis nelle reti HPE Aruba Networking, lo switch di accesso deve essere configurato per la comunicazione IEEE 802.1X. Il dispositivo Axis inoltra la comunicazione IEEE 802.1x EAP-TLS a ClearPass Policy Manager che agisce da server RADIUS.

Nota

È configurata anche una ripetizione di autenticazione periodica di 300 secondi per il dispositivo Axis per aumentare la sicurezza complessiva dell'accesso alle porte.

Questo esempio illustra la configurazione globale e delle porte per gli switch di accesso HPE Aruba Networking.

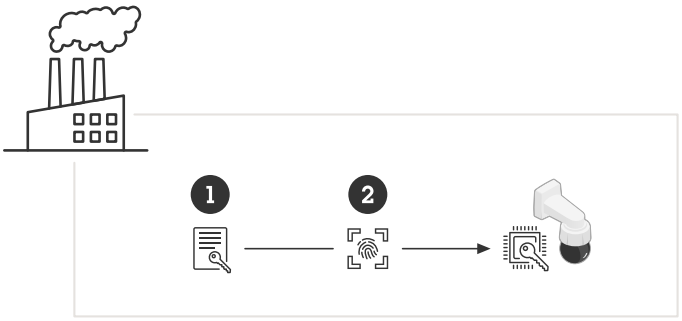
```
radius-server host MyRADIUSIPAddress key "MyRADIUSKey"
```

```
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
```

Axis configurazione

Dispositivo con tecnologia di rete Axis

I dispositivi Axis con supporto per *Axis Edge Vault* sono prodotti con un'identità dispositivo sicura denominata ID dispositivo Axis. L'ID dispositivo Axis si basa sullo standard internazionale IEEE 802.1AR, che definisce un metodo per l'identificazione automatica e sicura dei dispositivi e l'onboarding integrato tramite IEEE 802.1X.



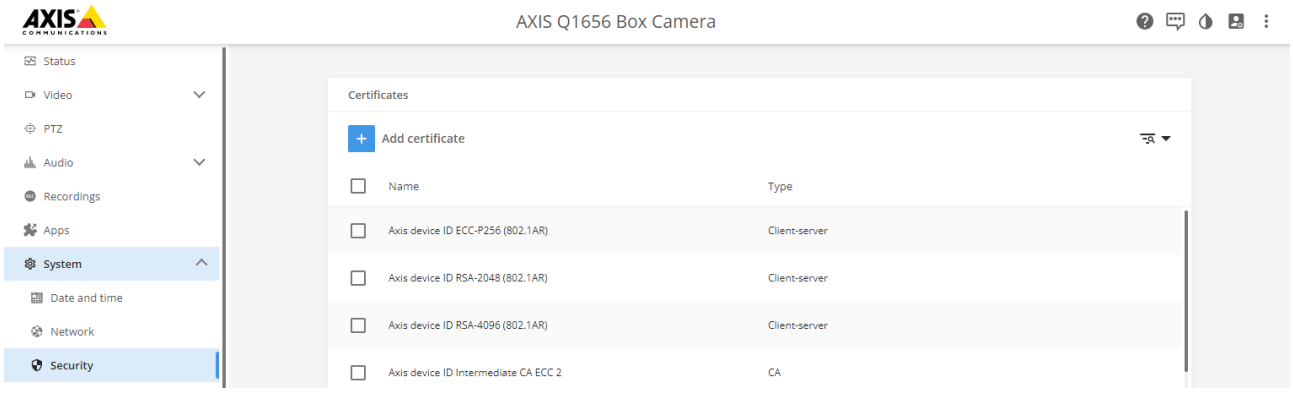
I dispositivi Axis sono prodotti con il certificato ID del dispositivo Axis conforme a IEEE 802.1AR per servizi di identità del dispositivo attendibili

1 *Infrastruttura chiave ID dispositivo Axis (PKI)*
2 *ID dispositivo Axis*

L'archivio chiavi sicuro protetto tramite hardware fornito da un elemento sicuro del dispositivo Axis viene fornito in fabbrica con un certificato univoco del dispositivo e le chiavi corrispondenti (ID dispositivo Axis) che possono dimostrare a livello globale l'autenticità del dispositivo Axis. *Axis Product Selector* può essere utilizzato per trovare quali dispositivi Axis supportano Axis Edge Vault e Axis Device ID.

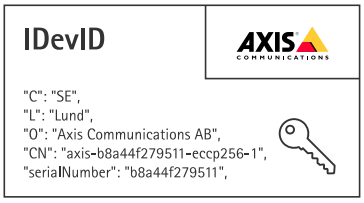
Nota

Il numero di serie di un dispositivo Axis è il suo indirizzo MAC.



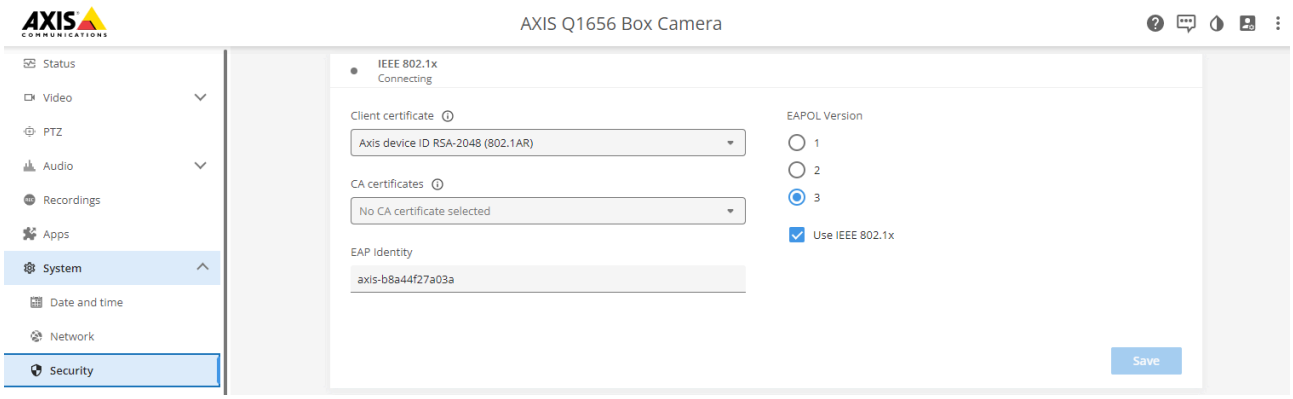
L'archivio certificati del dispositivo Axis nello stato predefinito di fabbrica, con l'ID dispositivo Axis.

Il certificato ID dispositivo Axis conforme a IEEE 802.1AR include informazioni sul numero di serie e altre informazioni specifiche del fornitore. Queste informazioni vengono utilizzate da ClearPass Policy Manager per l'analisi e il processo decisionale per concedere l'accesso alla rete. Le informazioni riportate di seguito possono essere ottenute da un certificato ID dispositivo Axis.



Paese	SE
Luogo	Lund
Organizzazione dell'emittente	Axis Communications AB
Nome comune dell'emittente	ID dispositivo Axis intermedio
Organizzazione	Axis Communications AB
Nome comune	axis-b8a44f279511-eccp256-1
Numero di serie	b8a44f279511

Il nome comune è composto da una combinazione di nome dell'azienda Axis, numero di serie del dispositivo, seguito dall'algoritmo crittografico (ECC P256, RSA 2048, RSA 4096). A partire da AXIS OS 10.1 (2020-09), IEEE 802.1X è abilitato per impostazione predefinita con l'ID del dispositivo Axis preconfigurato. Ciò consente al dispositivo di autenticarsi su reti abilitate IEEE 802.1X.



Il dispositivo Axis è nello stato predefinito di fabbrica con IEEE 802.1X abilitato e il certificato ID dispositivo Axis preselezionato.

AXIS Device Manager

AXIS Device Manager e *AXIS Device Manager Extend* possono essere utilizzati nella rete per configurare e gestire più dispositivi Axis in modo economico. AXIS Device Manager è un'applicazione basata su Microsoft Windows® che viene installata localmente su un computer in rete, mentre AXIS Device Manager Extend si affida all'infrastruttura cloud per svolgere la gestione dei dispositivi multisito. Entrambi offrono funzionalità di gestione e configurazione semplici, come:

- Installazione di aggiornamenti di AXIS OS.
- Applicazione di configurazioni di sicurezza informatica quali certificati HTTPS e IEEE 802.1X.
- Configurazione di impostazioni specifiche del dispositivo, come impostazioni immagini e altre.

Funzionamento sicuro della rete: IEEE 802.1AE MACsec

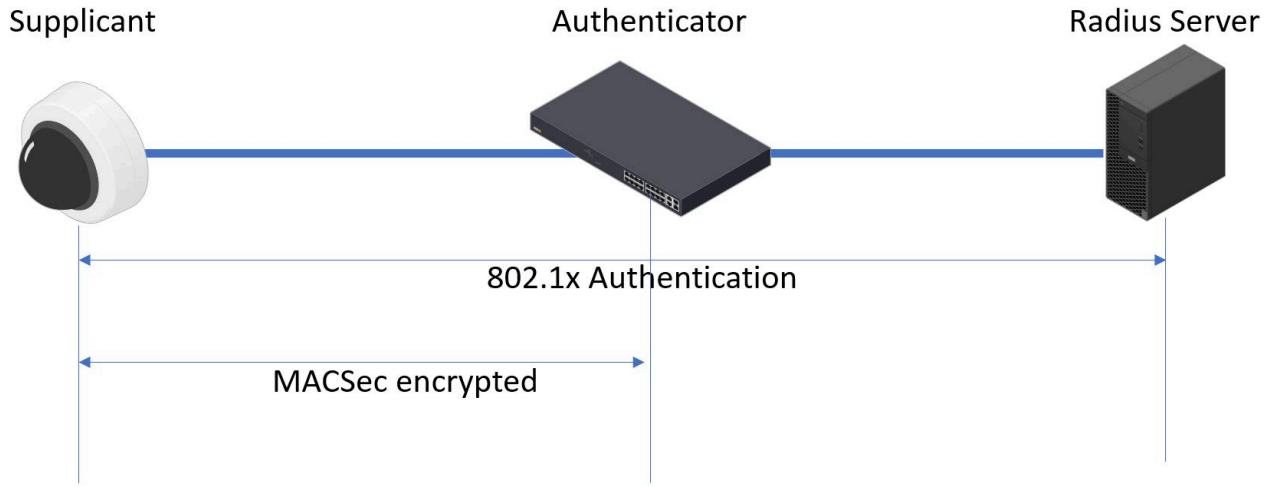
Per guardare questo video, andare alla versione web di questo documento.

Crittografia di rete zero-trust con sicurezza IEEE 802.1AE MACsec di livello 2

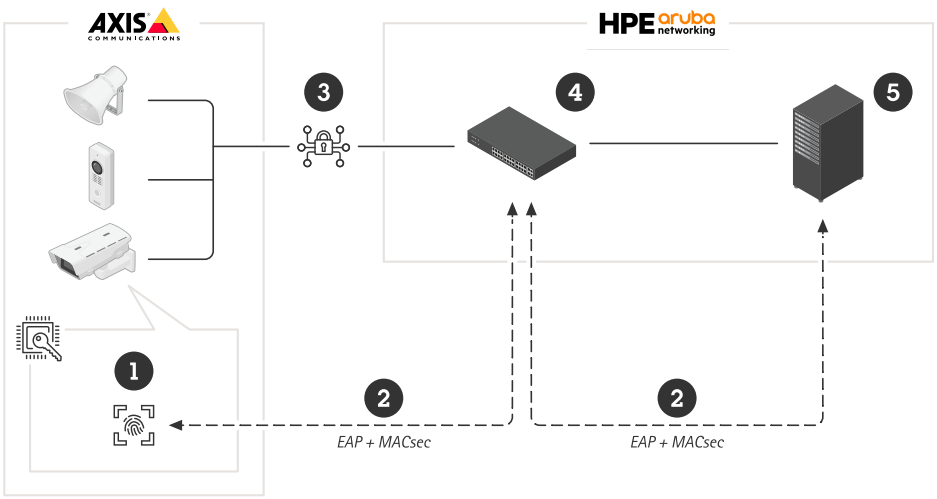
IEEE 802.1AE MACsec (Media Access Control Security) è un protocollo di rete ben definito che garantisce la sicurezza crittografica dei collegamenti Ethernet punto-punto a livello 2 della rete. Garantisce la riservatezza e l'integrità delle trasmissioni di dati tra due host.

Lo standard IEEE 802.1AE MACsec descrive due modalità operative:

- Modalità chiave Pre-Shared Key/Static CAK configurabile manualmente
- Sessione master automatica/Modalità Dynamic CAK che utilizza IEEE 802.1X EAP-TLS



In AXIS OS 10.1 (2020-09) e versioni successive, IEEE 802.1X è abilitato per impostazione predefinita per dispositivi compatibili con l'ID dispositivo Axis. In AXIS OS 11.8 e versioni successive, è supportato MACsec con modalità dinamica automatica utilizzando IEEE 802.1X EAP-TLS abilitato per impostazione predefinita. Quando si collega un dispositivo Axis con i valori predefiniti di fabbrica, viene eseguita l'autenticazione di rete IEEE 802.1X e, in caso di esito positivo, viene provata anche la modalità MACsec Dynamic CAK.



L'ID del dispositivo Axis archiviato in modo sicuro (1), un'identità del dispositivo sicuro conforme a IEEE 802.1AR, viene utilizzato per l'autenticazione nella rete (4, 5) tramite il controllo degli accessi di rete

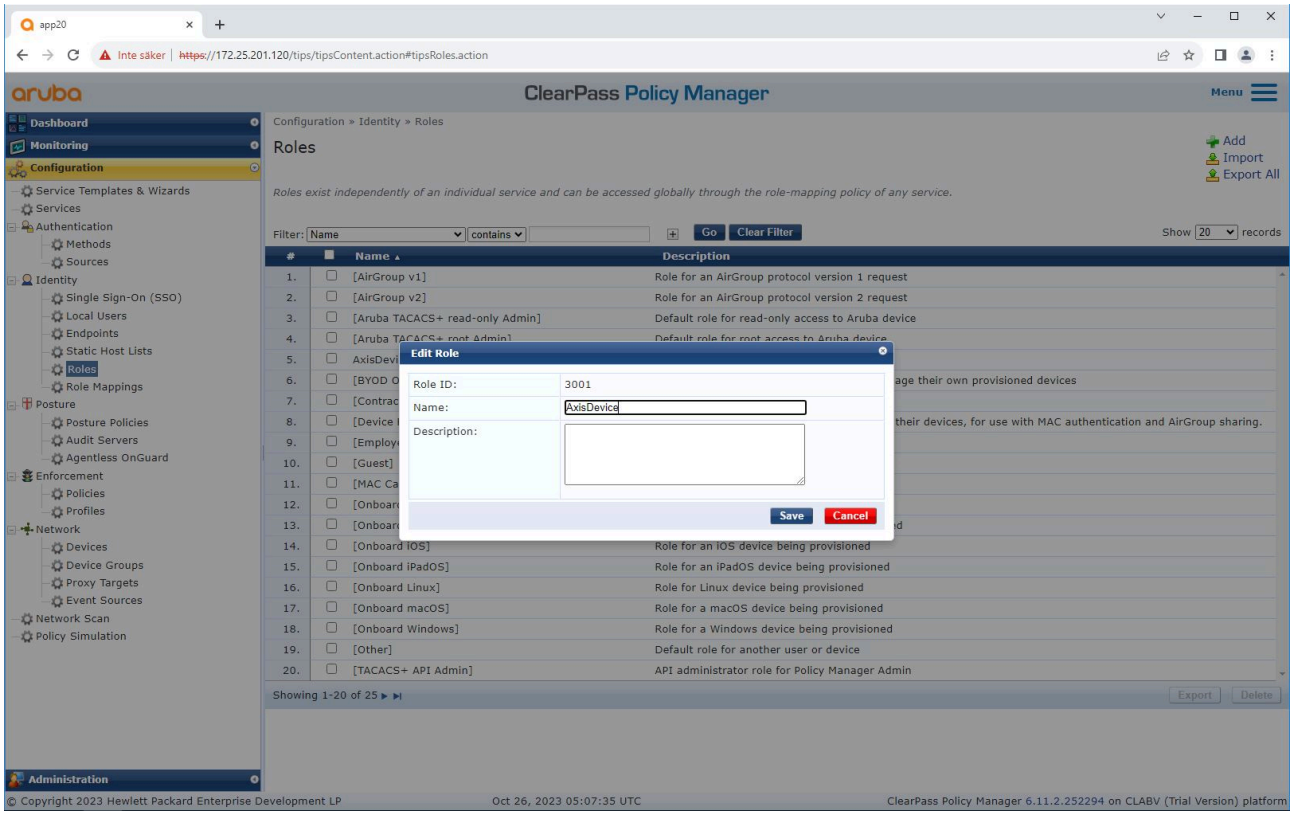
basato su porta IEEE 802.1X EAP-TLS (2). Attraverso la sessione EAP-TLS, le chiavi MACsec vengono scambiate automaticamente per impostare un collegamento sicuro (3), proteggendo tutto il traffico di rete dal dispositivo Axis allo switch di accesso HPE Aruba Networking.

IEEE 802.1AE MACsec richiede la preparazione della configurazione sia dello switch di accesso HPE Aruba Networking sia di ClearPass Policy Manager. Non è richiesta alcuna configurazione sul dispositivo Axis per consentire la comunicazione crittografata MACsec IEEE 802.1AE tramite EAP-TLS.

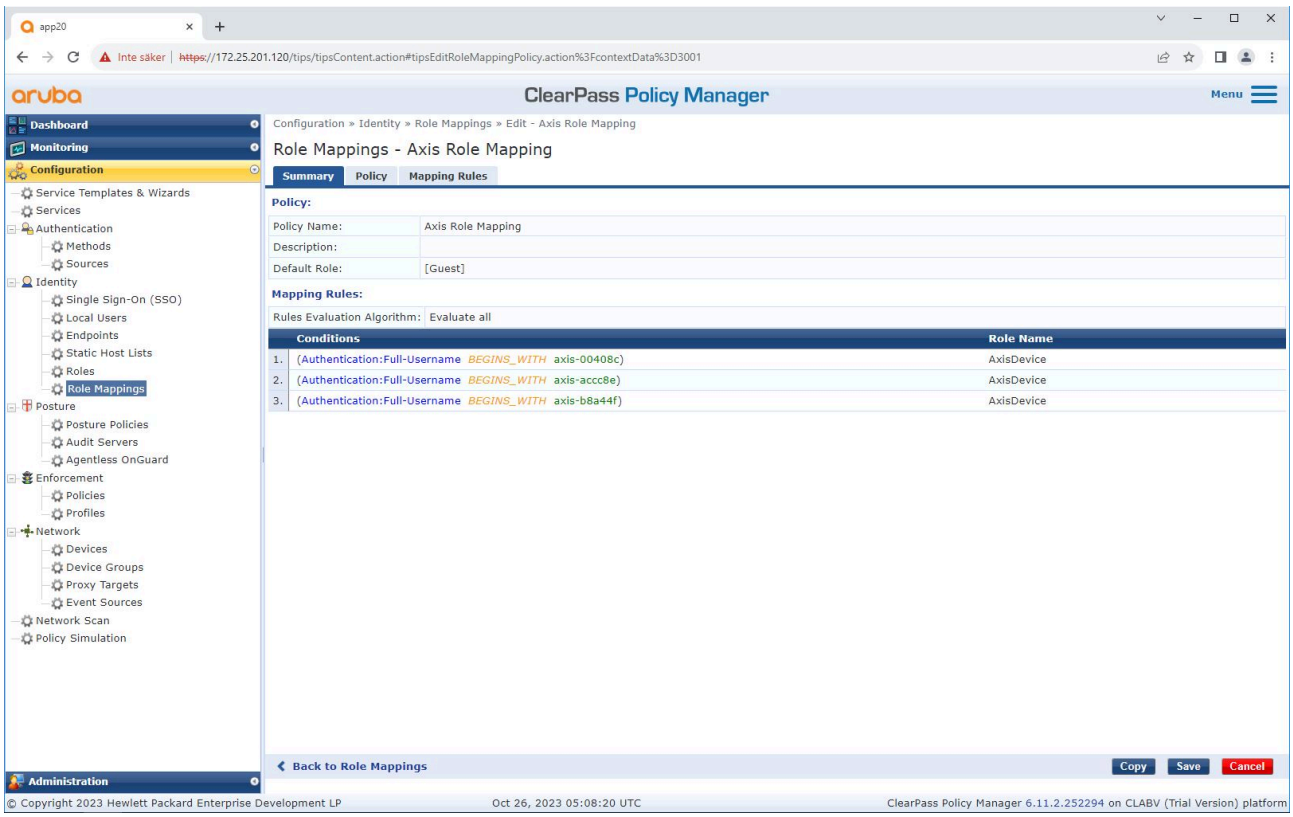
Se lo switch di accesso HPE Aruba Networking non supporta MACsec con EAP-TLS, è allora possibile utilizzare e configurare manualmente la modalità Pre-Shared Key.

HPE Aruba Networking ClearPass Policy Manager

Ruolo e policy di mappatura del ruolo



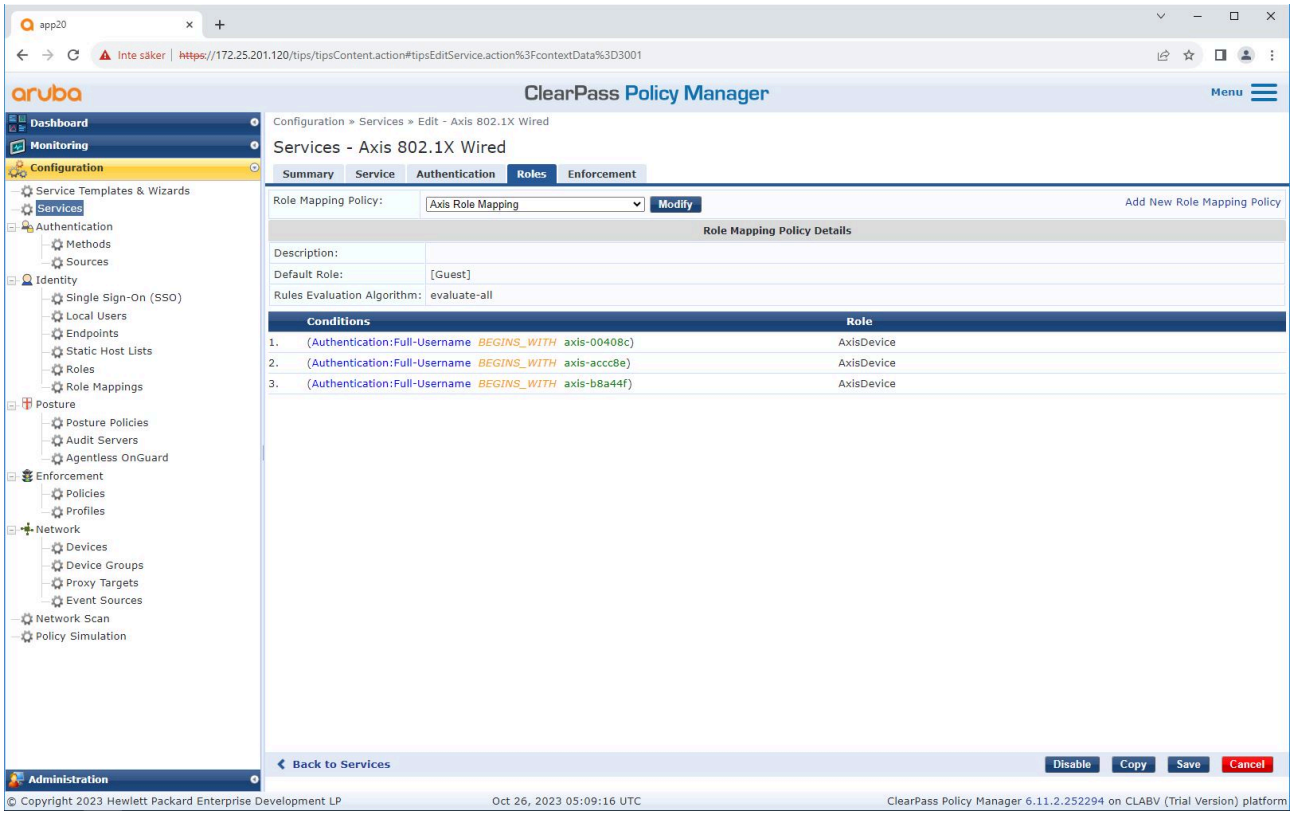
Aggiungere un nome ruolo per i dispositivi Axis. Il nome è quello del ruolo di accesso alla porta nella configurazione dello switch di accesso.



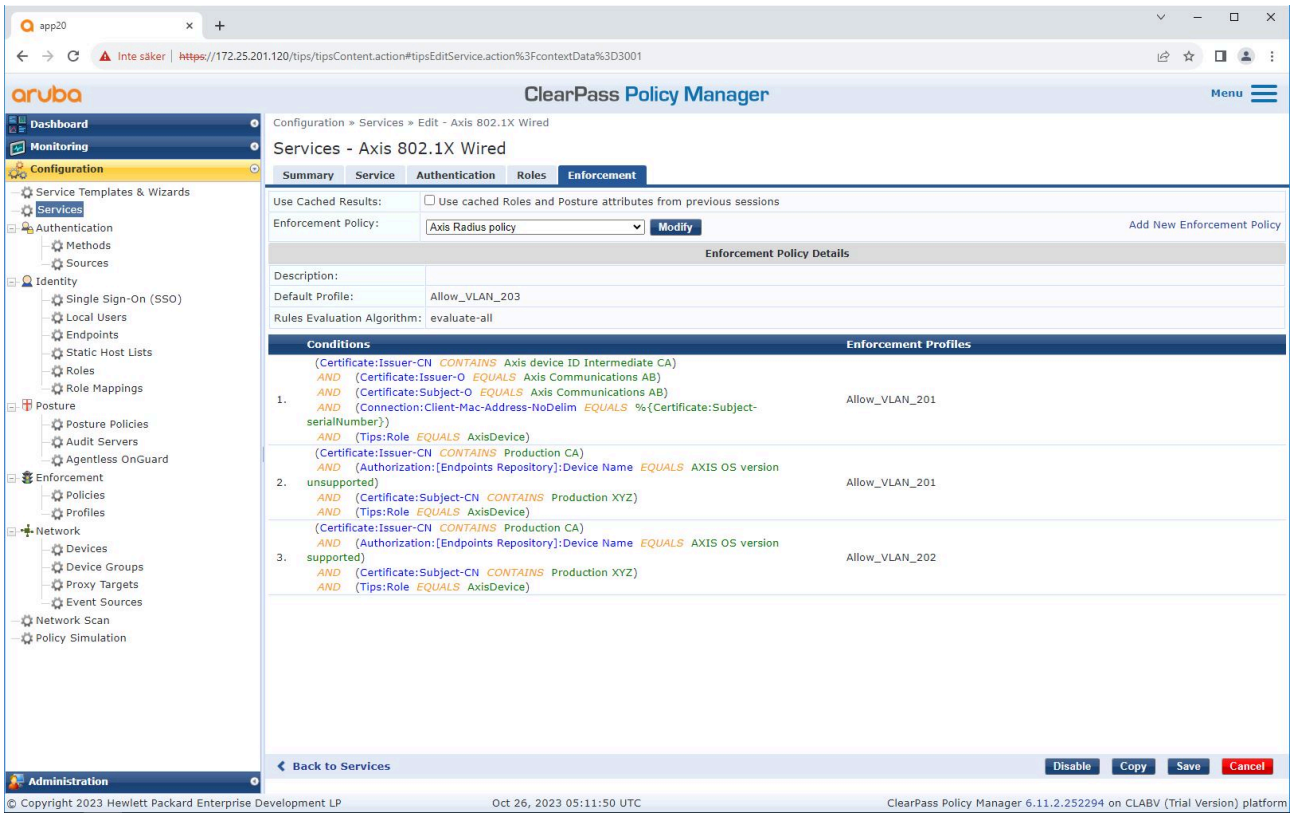
Si prega di aggiungere una policy di mappatura dei ruoli Axis per il ruolo del dispositivo Axis creato in precedenza. Le condizioni definite sono necessarie affinché un dispositivo venga mappato al ruolo del dispositivo Axis. Se le condizioni non vengono soddisfatte, il dispositivo diventa parte del ruolo [Guest].

Per impostazione predefinita, i dispositivi Axis utilizzano il formato di identità EAP "axis-serialnumber". Il numero di serie di un dispositivo Axis è il suo indirizzo MAC. Ad esempio "axis-b8a44f45b4e6".

Configurazione del servizio

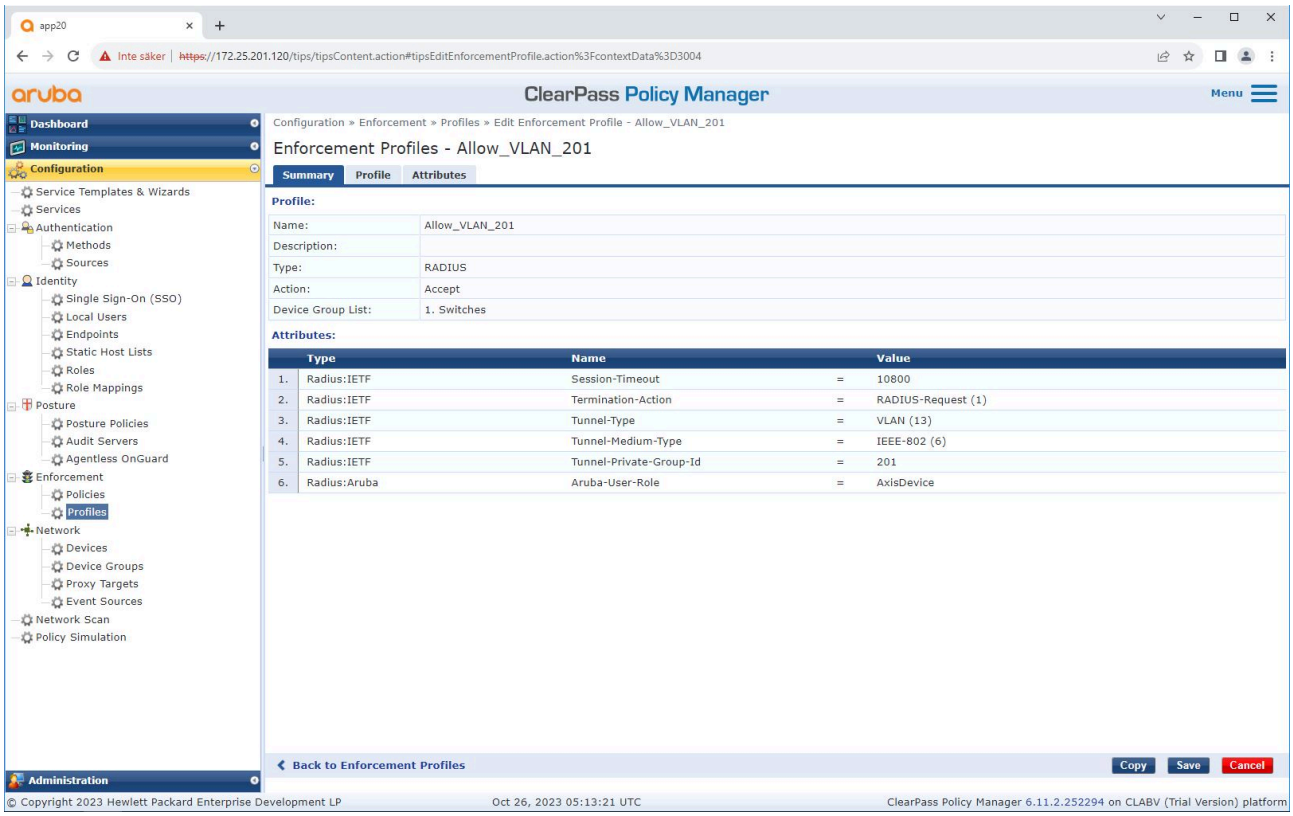


Aggiungere la policy di mappatura dei ruoli Axis creata in precedenza al servizio che definisce IEEE 802.1X come il metodo di connessione per l'onboarding dei dispositivi Axis.



Aggiungere il nome del ruolo Axis come condizione alle definizioni di policy esistenti.

Profilo esecutivo



Aggiungere il nome del ruolo Axis come un attributo ai profili esecutivi assegnati nel servizio di onboarding IEEE 802.1X.

Switch di accesso HPE Aruba Networking

Oltre alla configurazione di onboarding sicura descritta in *Switch di accesso HPE Aruba Networking, on page 15*, vedere di seguieto l'esempio di configurazione della porta affinché lo switch di accesso HPE Aruba Networking configuri 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
```

Gestione certificati – Registrazione tramite trasporto sicuro (EST)

I certificati digitali sono fondamentali per garantire la sicurezza di dispositivi e reti, ma la loro gestione può essere complessa e richiedere molto tempo. I certificati hanno una scadenza e devono essere rinnovati periodicamente. Senza automazione, questo processo è ripetitivo e manuale, specialmente in implementazioni di grandi dimensioni o in ambienti con tipi di dispositivi misti.

AXIS OS 12.9 introduce il supporto per Registrazione tramite Trasporto sicuro (EST), un protocollo per la fornitura sicura di certificati ai dispositivi. Definito nella RFC 7030, EST è una soluzione basata su standard progettata per semplificare e automatizzare l'intero ciclo di vita del certificato, comprendente:

- Registrazione: emissione sicura di nuovi certificati ai dispositivi
- Rinnovo: sostituzione automatica dei certificati in scadenza
- Nuova registrazione: aggiornamento dei certificati in base alle politiche IT

EST supporta politiche definite dall'IT per gli attributi dei certificati, quali il periodo di validità, il tipo di chiave (RSA/ECC) o la dimensione della chiave, e utilizza esclusivamente HTTPS.

Vantaggi principali di EST

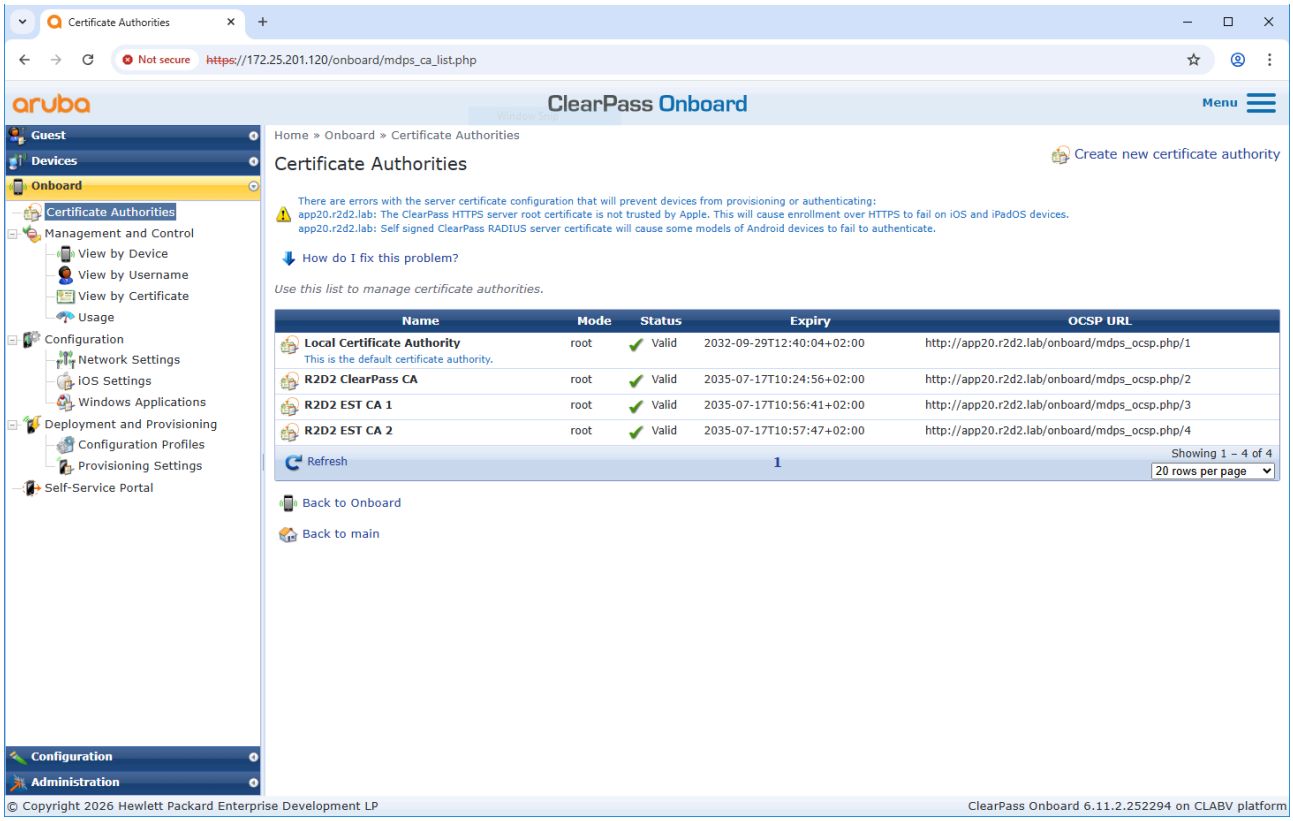
- La politica IT gestisce automaticamente la registrazione, il rinnovo e la nuova registrazione dei certificati, rimuovendo completamente la necessità di configurazioni manuali e dispendiose in termini di tempo.
- Comunicazione sicura all'avanguardia tramite solo HTTPS TLS 1.2/1.3.
- Visibilità/monitoraggio centralizzato per i team IT.
  Basato su standard (RFC 7030) e integrabile con l'Infrastruttura IT.
- Soluzione scalabile per IoT, reti aziendali e gestione dispositivi.

Per la documentazione generale relativa a EST, consultare la nostra *Knowledge Base di AXIS OS*.

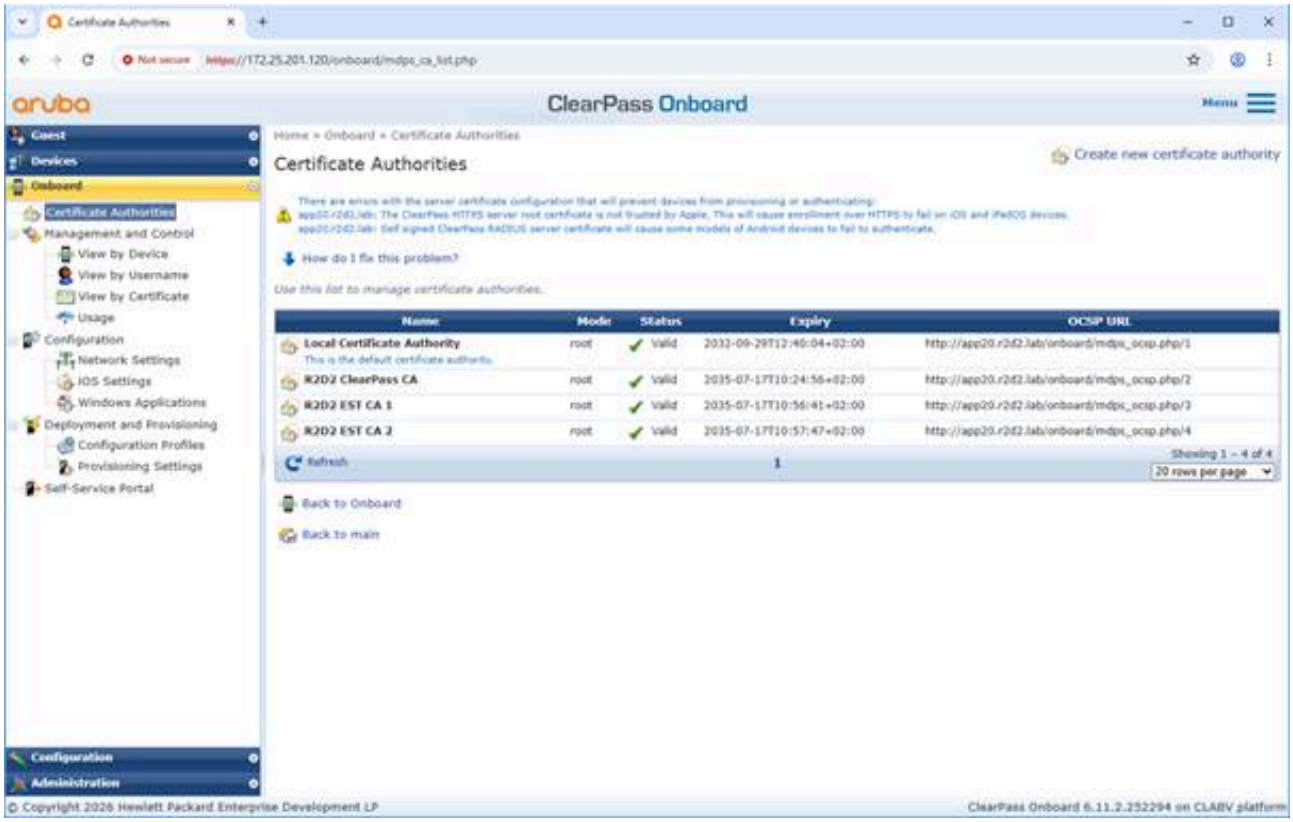
Configurazione HPE Aruba ClearPass integrata

Aruba ClearPass Onboard si integra con EST per distribuire e gestire in modo sicuro i certificati dei dispositivi per l'accesso alla rete. Utilizzando EST, gli endpoint si autenticano su ClearPass e si registrano per ottenere un certificato univoco tramite un canale TLS sicuro, che viene poi utilizzato per l'autenticazione basata su certificato 802.1X e altri servizi. Ciò fornisce un metodo basato su standard, automatizzato e un minor numero di password per applicare politiche di accesso sicuro basate sull'identità del dispositivo.

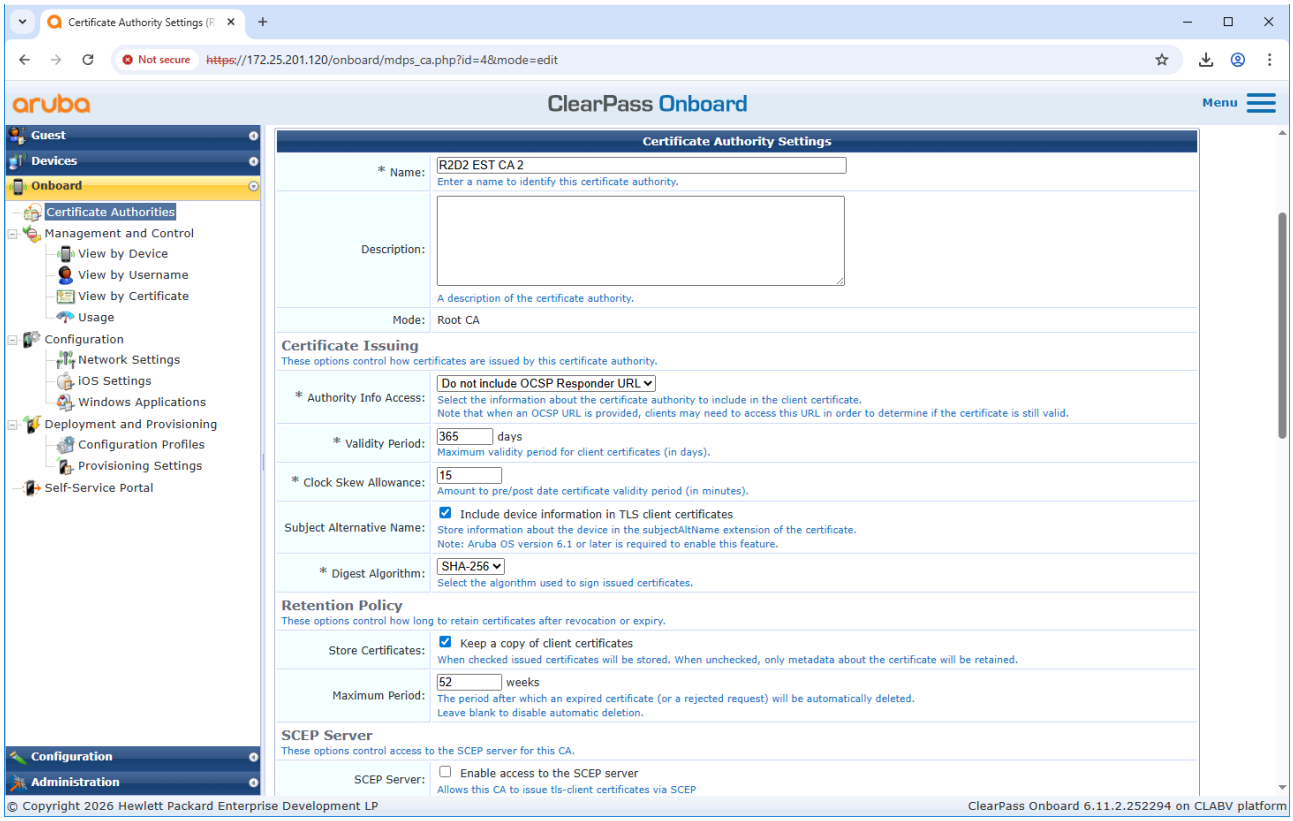
Configurazione dell'autorità di certificazione



Creare una nuova autorità di certificazione all'interno di ClearPass integrato.



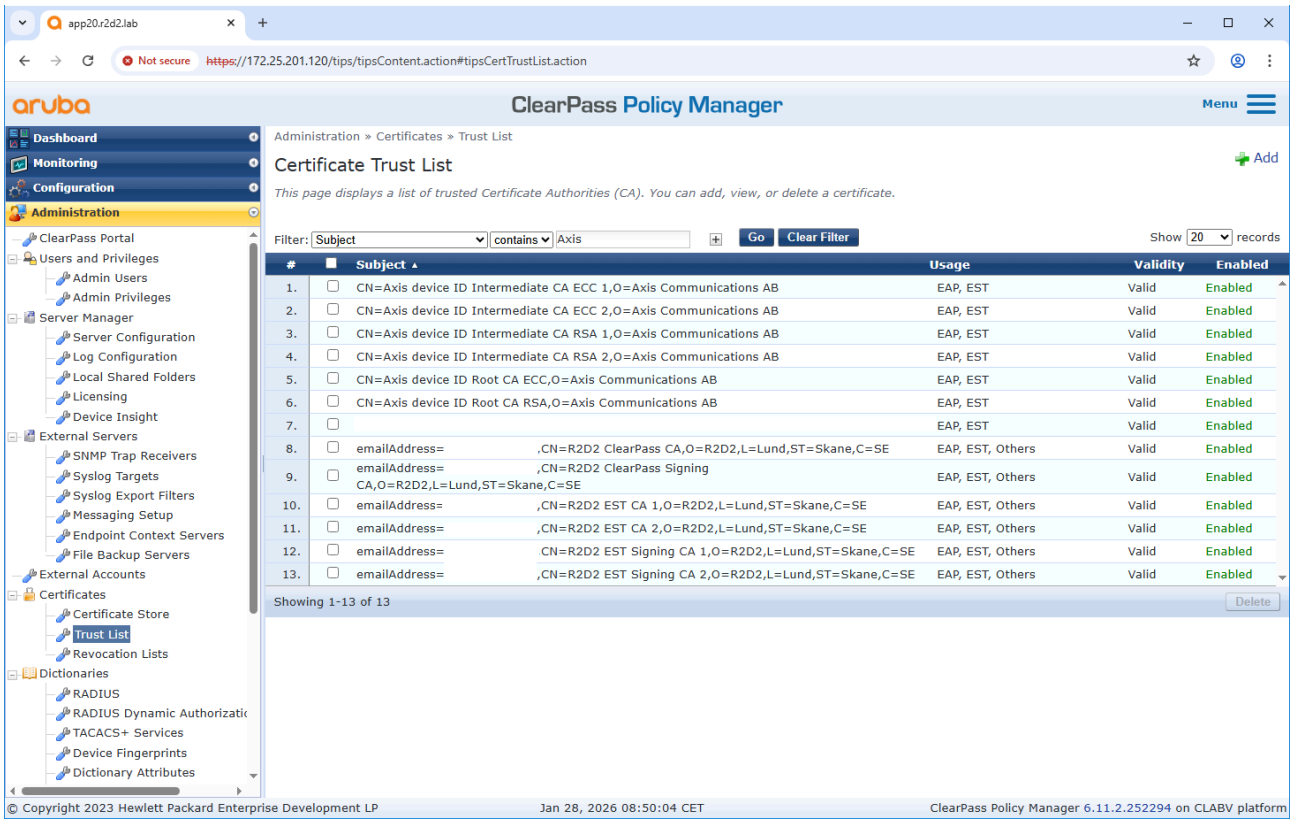
All'interno dell'autorità di certificazione creata, vengono definiti il tipo di chiave, la dimensione della chiave, il periodo di validità e altro ancora.



Abilitare la funzionalità EST Server per l'autorità di certificazione creata. Configurare il metodo di autenticazione EST per l'utilizzo del certificato client.

Configurazione HPE Aruba ClearPass Policy Manager

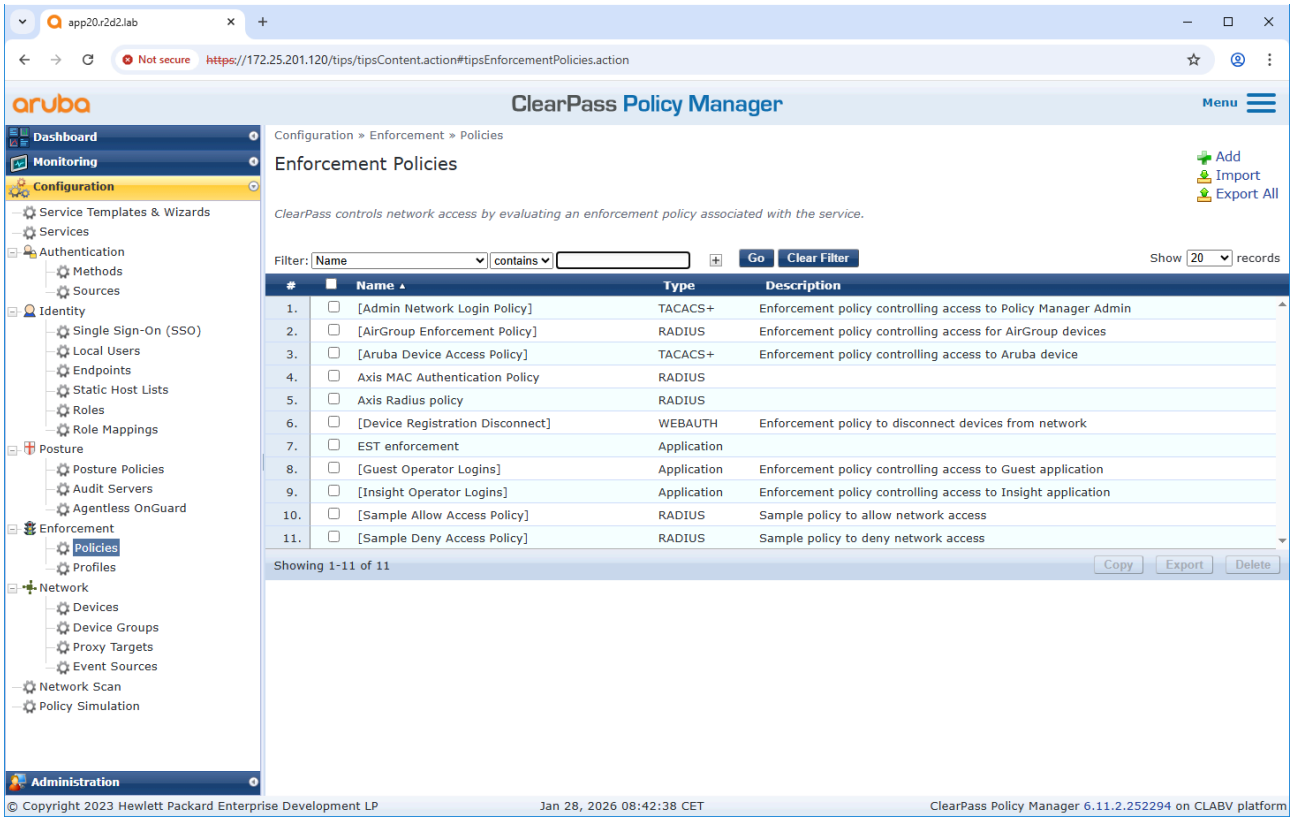
Configurazione dell'archivio certificati attendibili



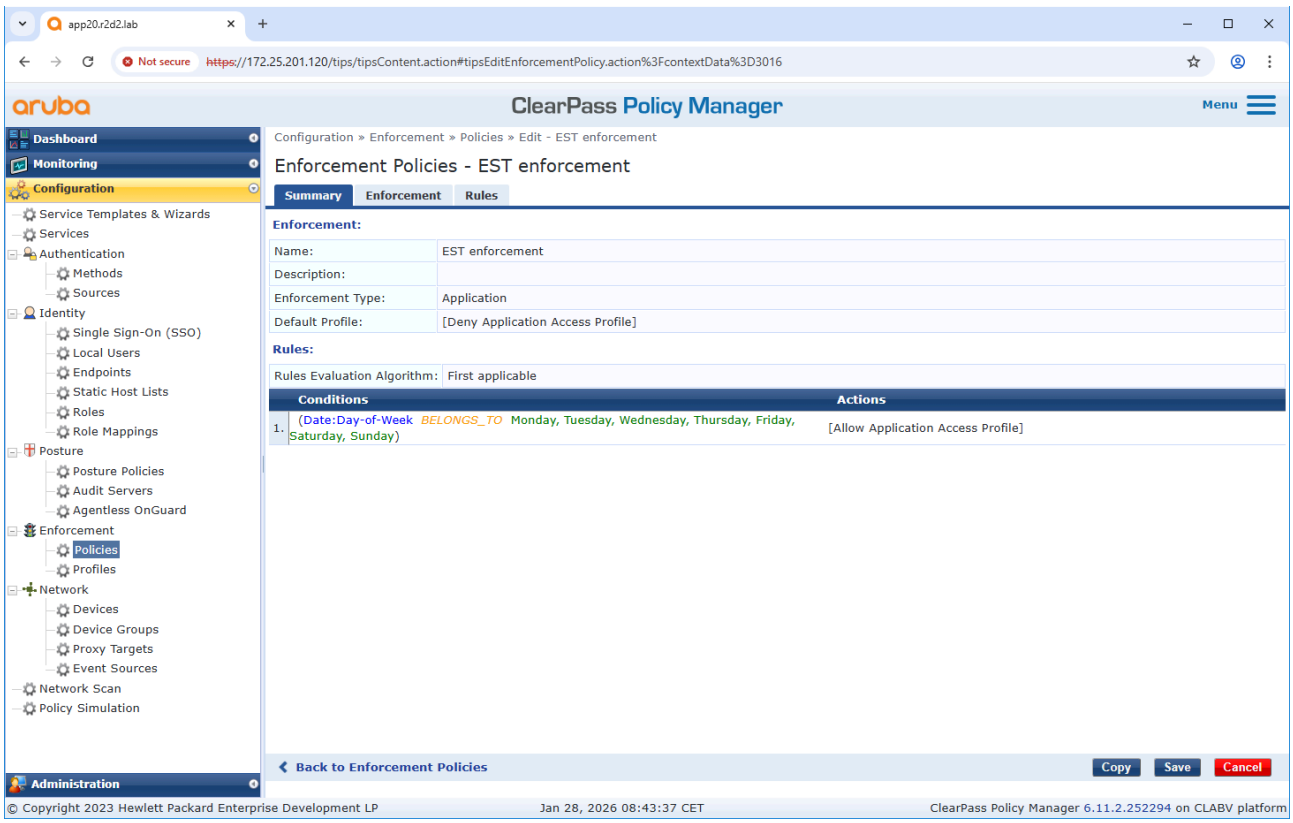
Se non è stato già fatto, caricare i certificati *IEEE 802.1AR specifici di Axis* nell'archivio certificati attendibili di ClearPass Policy Manager. Controllare che l'utilizzo di EST sia stato aggiunto. Verificare questo aspetto anche per l'autorità di certificazione precedentemente creata da ClearPass integrato.

Configurazione della policy di applicazione

Il profilo di applicazione consente a ClearPass Policy Manager di assegnare specifiche applicazioni ad EST. Ad esempio, i nuovi certificati possono essere registrati solo da endpoint specifici o solo in determinati giorni della settimana.

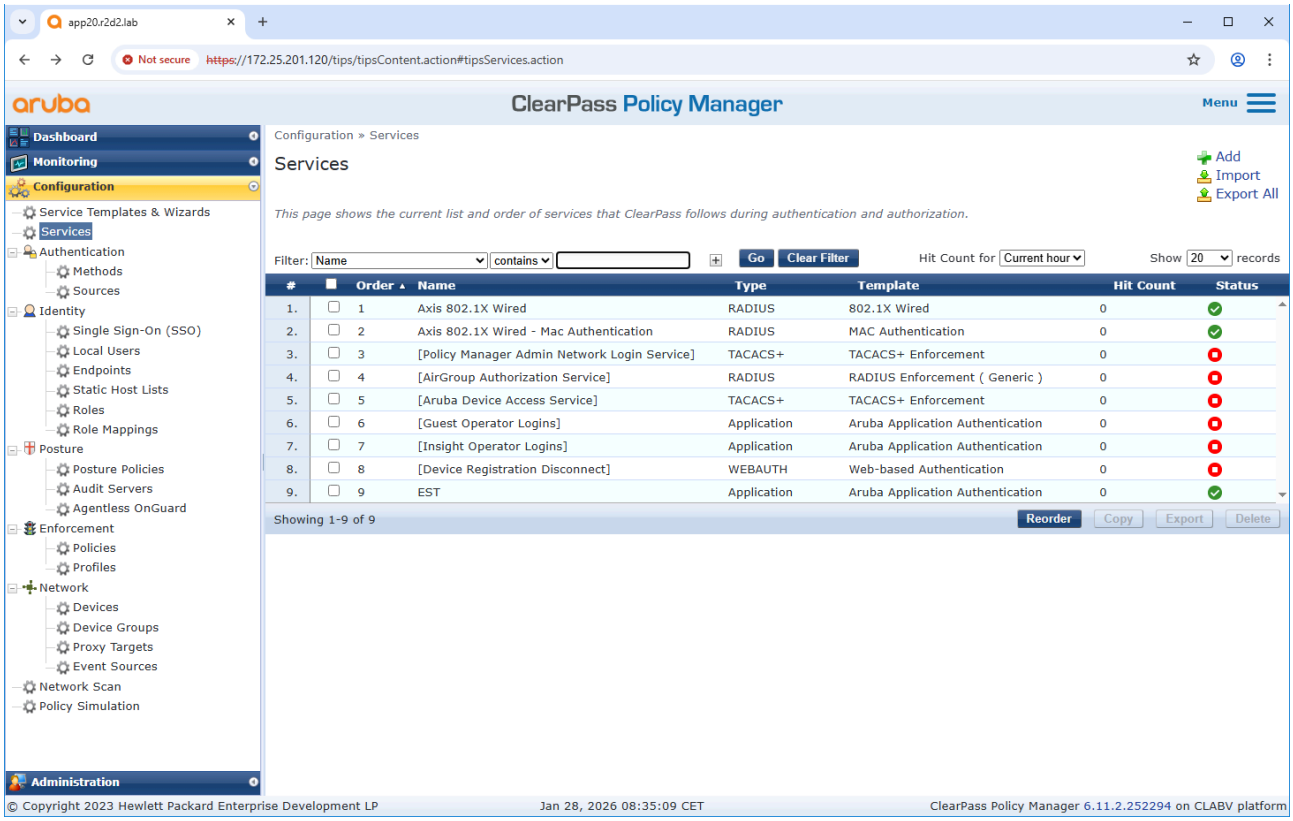


Panoramica delle politiche di applicazione in ClearPass Policy Manager.

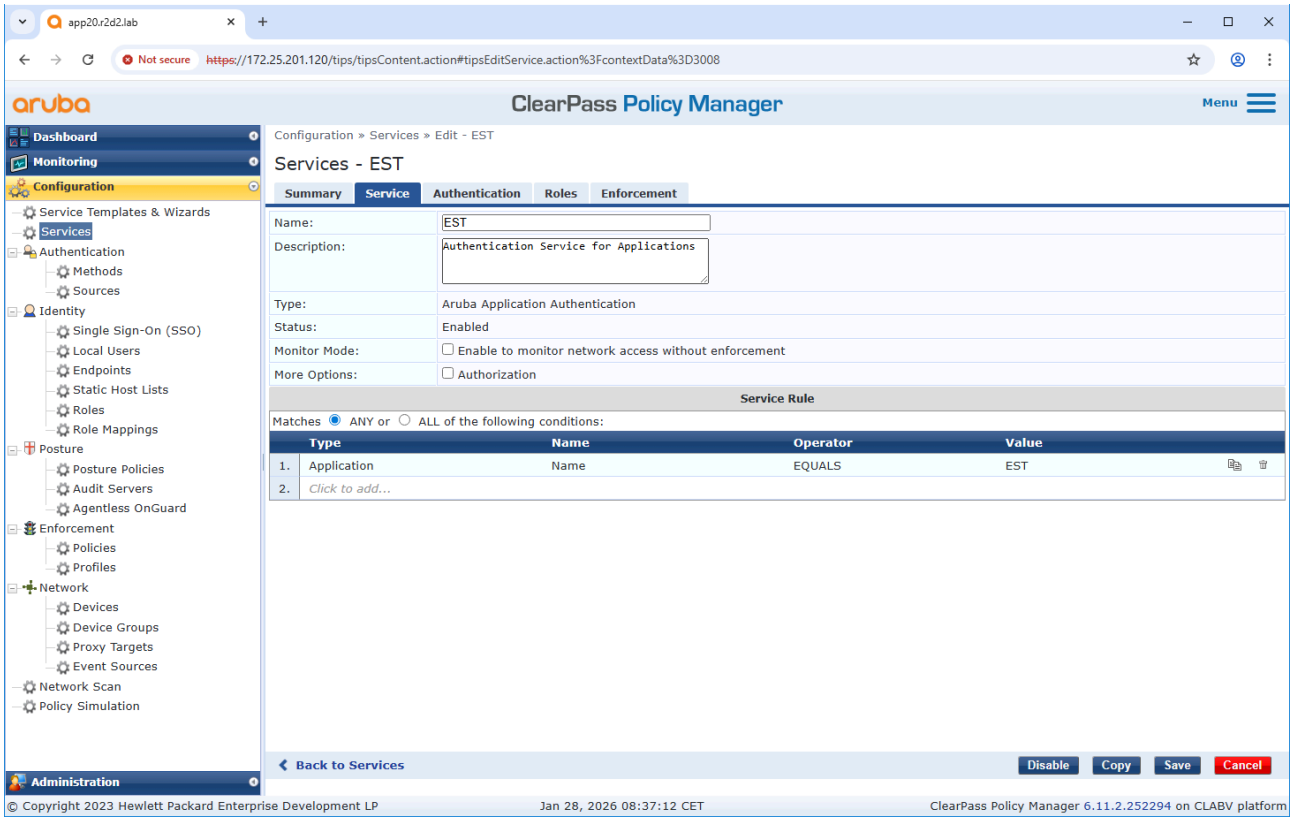


In questa politica di esempio, l'applicazione EST è consentita tutti i giorni della settimana.

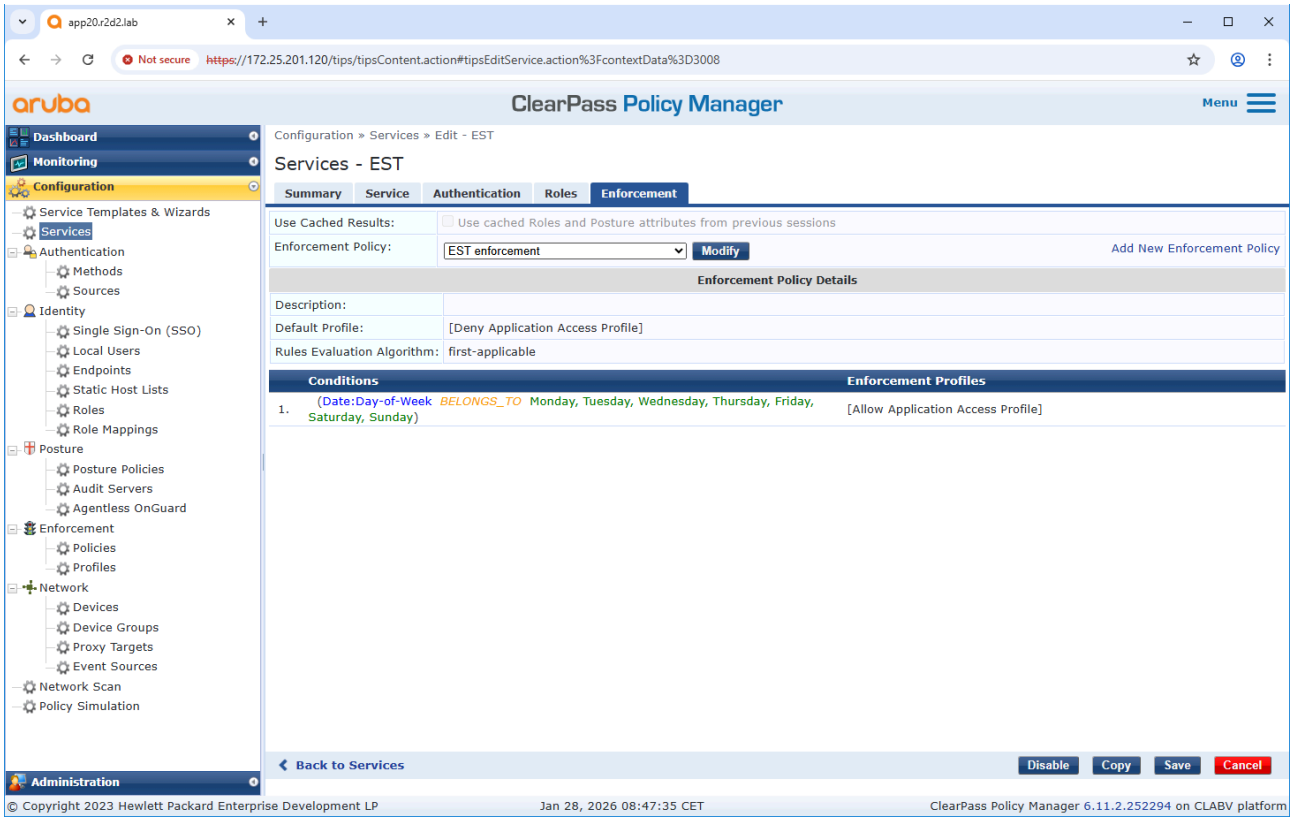
Configurazione del servizio



È necessario creare un servizio EST dedicato.



Il servizio deve essere configurato per l'applicazione EST.



Selezionare la politica di applicazione EST precedentemente creata.

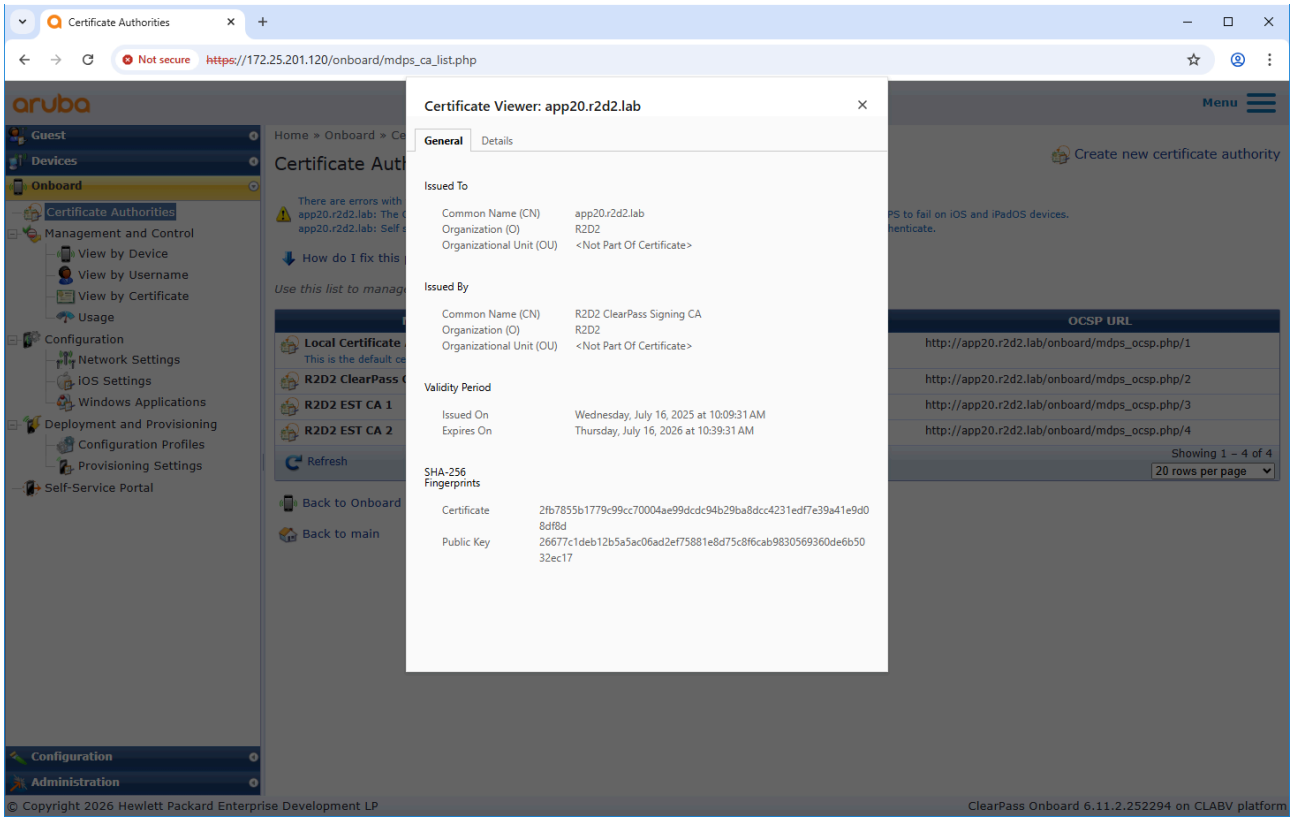
Axis configurazione

La configurazione sul dispositivo Axis viene effettuata in due passaggi.

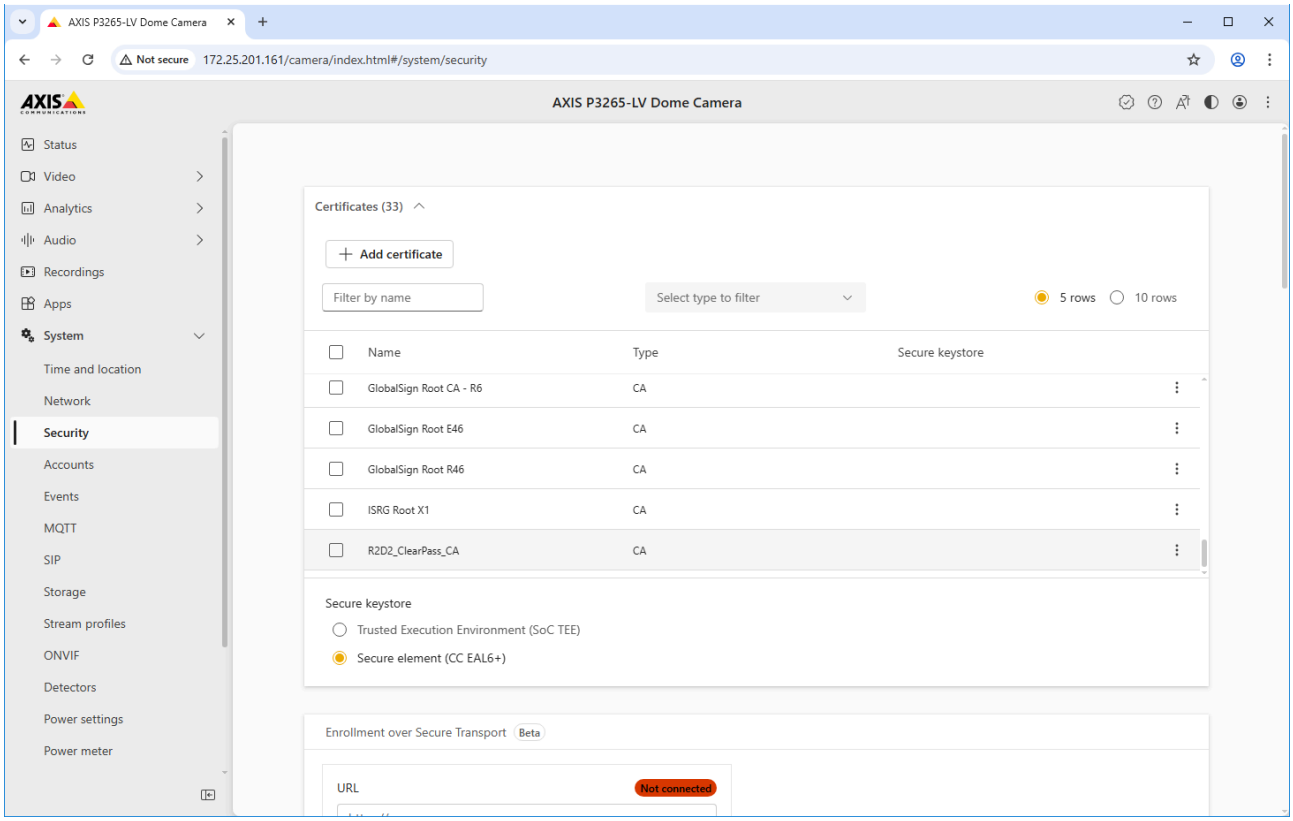
1. Stabilire l'affidabilità con l'endpoint HTTPS integrato in ClearPass.

2. Configurare il client EST sul dispositivo Axis.

Configurazione certificati attendibili

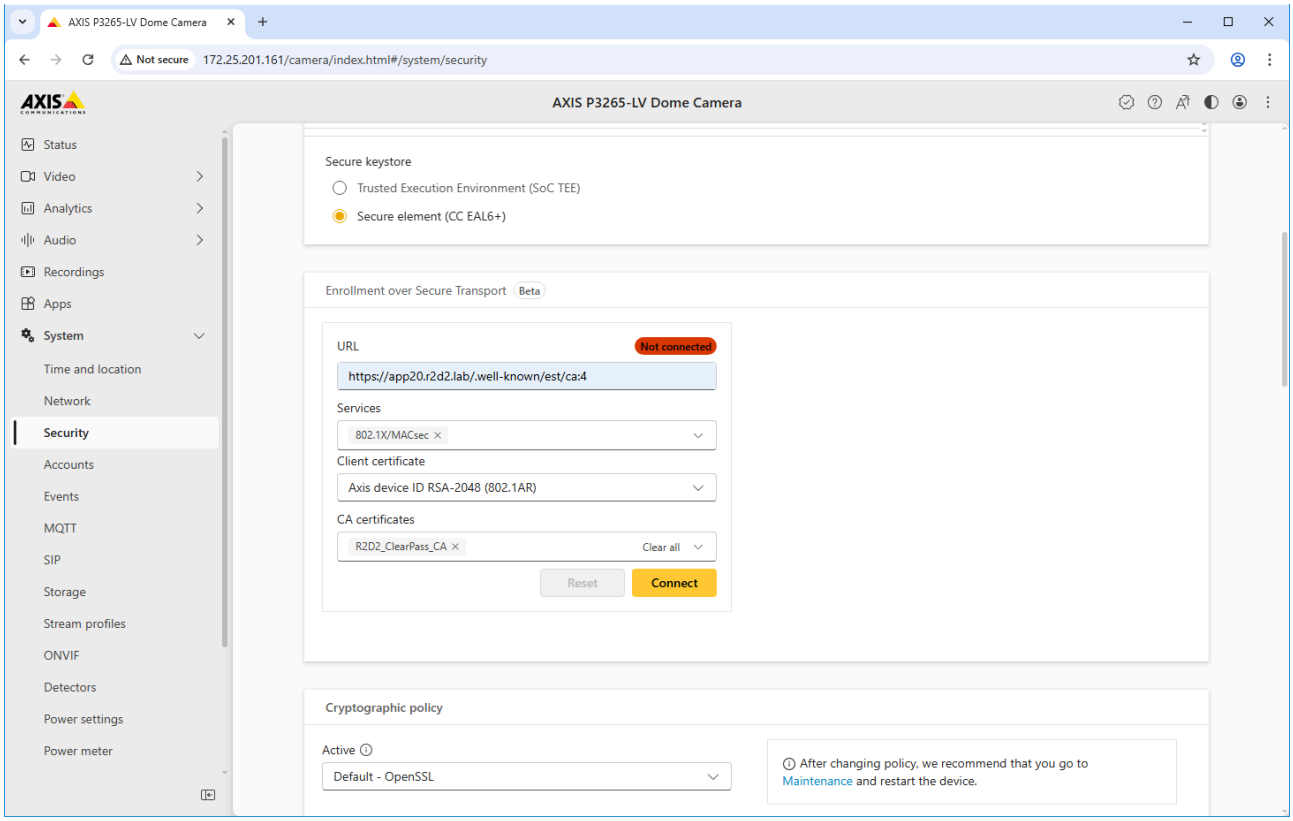


Verificare la catena di certificati dall'endpoint HTTPS integrato in ClearPass.

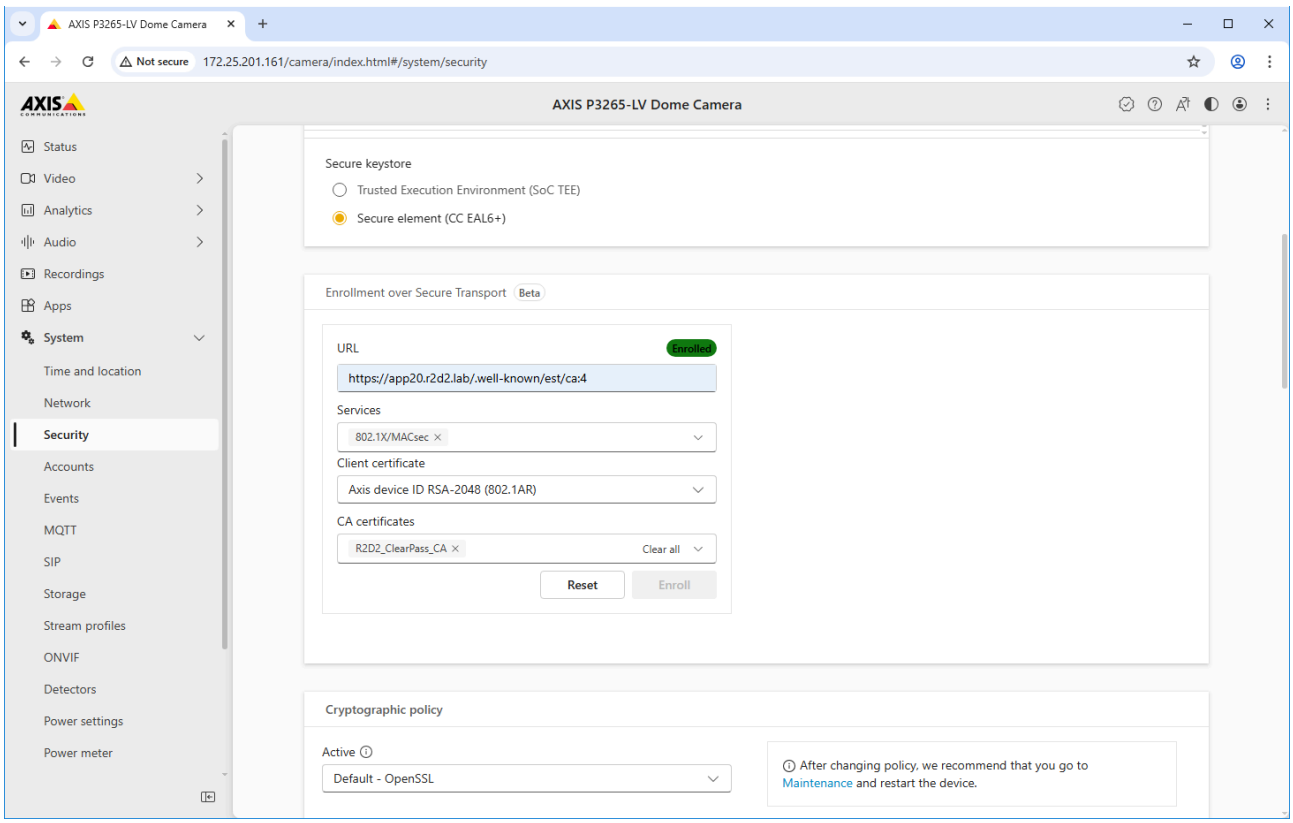


Caricare la CA dall'endpoint HTTPS integrato ClearPass sul dispositivo Axis.

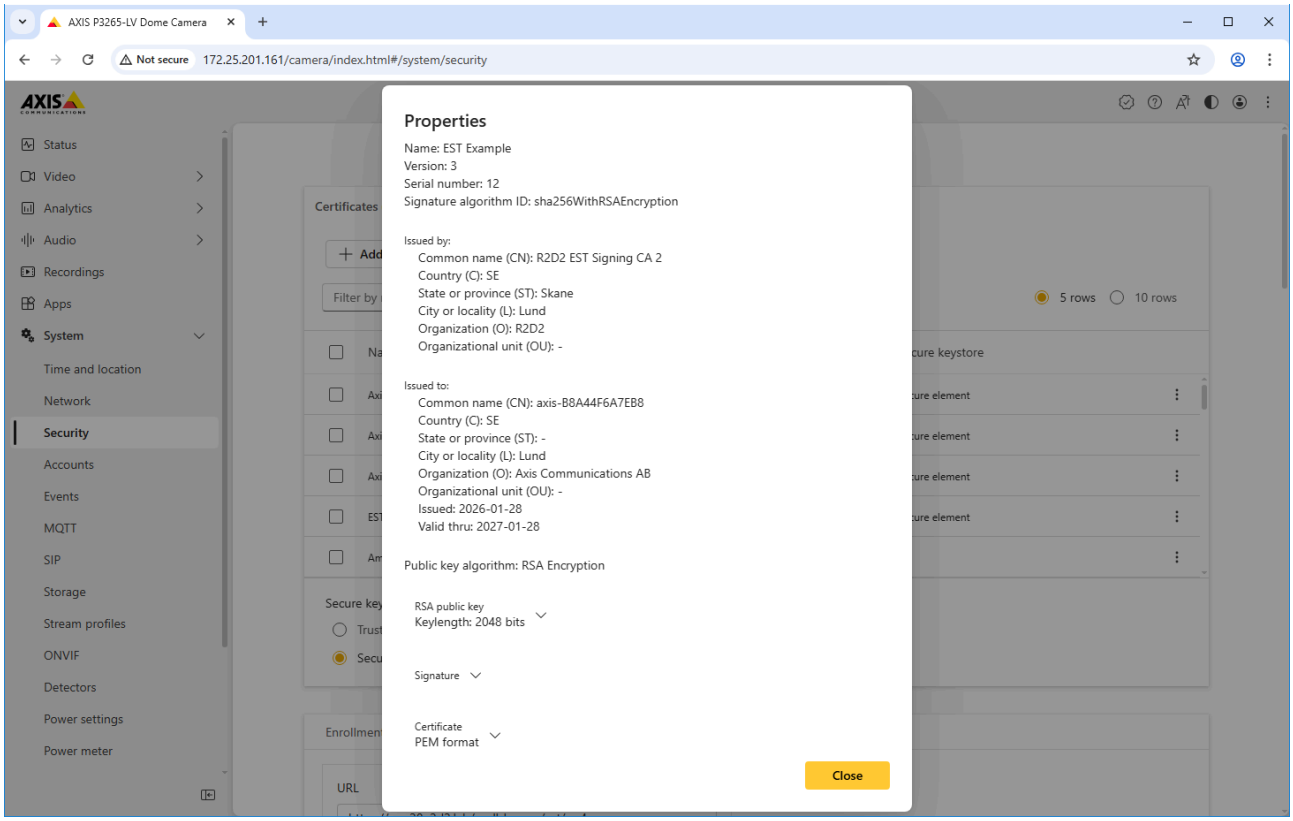
Configurazione client EST



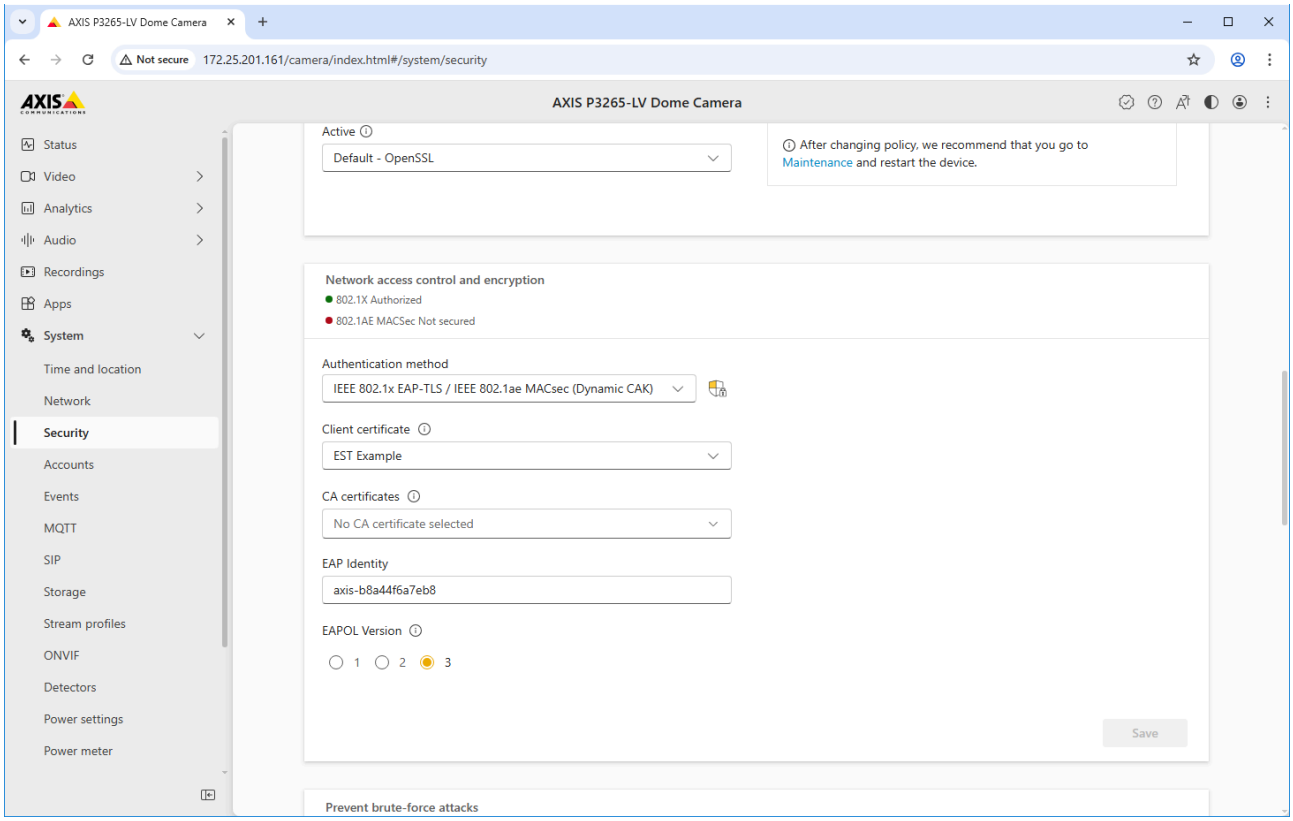
Parametro	Valore
URL	L'URL EST è disponibile nell'autorità di certificazione creata per EST in ClearPass integrato.
Servizi	Selezionare i servizi che devono essere configurati automaticamente con il certificato registrato.
Certificato client	Selezionare un certificato client per l'autenticazione sul server EST integrato in ClearPass. I dispositivi con ID dispositivo Axis vengono automaticamente considerati attendibili per la registrazione, poiché la catena di certificati IEEE 802.1AR specifica per Axis è stata aggiunta all'archivio dei certificati attendibili in ClearPass Policy Manager.
Certificati dell'autorità di certificazione	Selezionare il Certificato CA dall'endpoint HTTPS integrato in ClearPass in modo che il dispositivo Axis riconosca tale endpoint come attendibile.



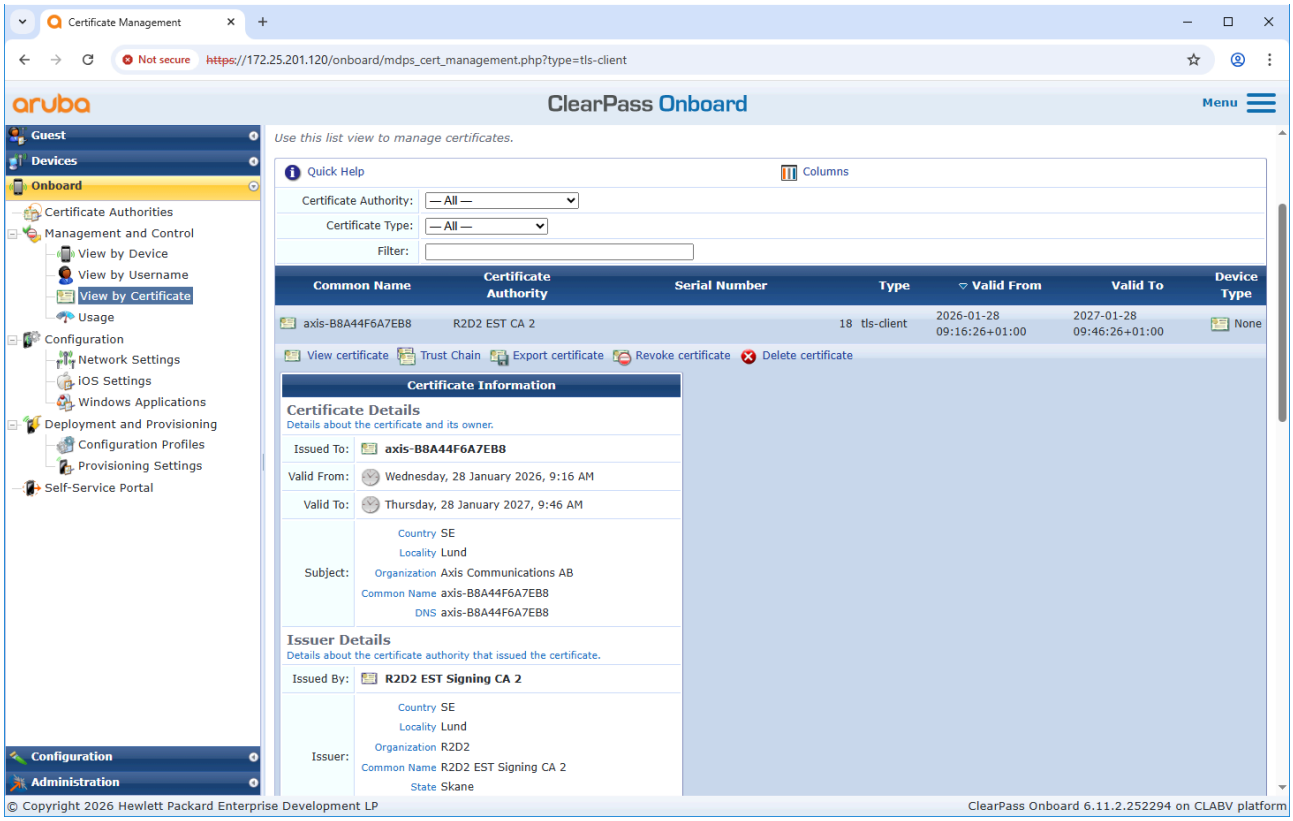
La registrazione è stata completata con successo.



Il certificato EST registrato sul dispositivo Axis.



Il certificato registrato viene automaticamente assegnato al servizio precedentemente selezionato.



È inoltre possibile rivedere il certificato registrato in ClearPass integrato.

Onboarding legacy: autenticazione MAC

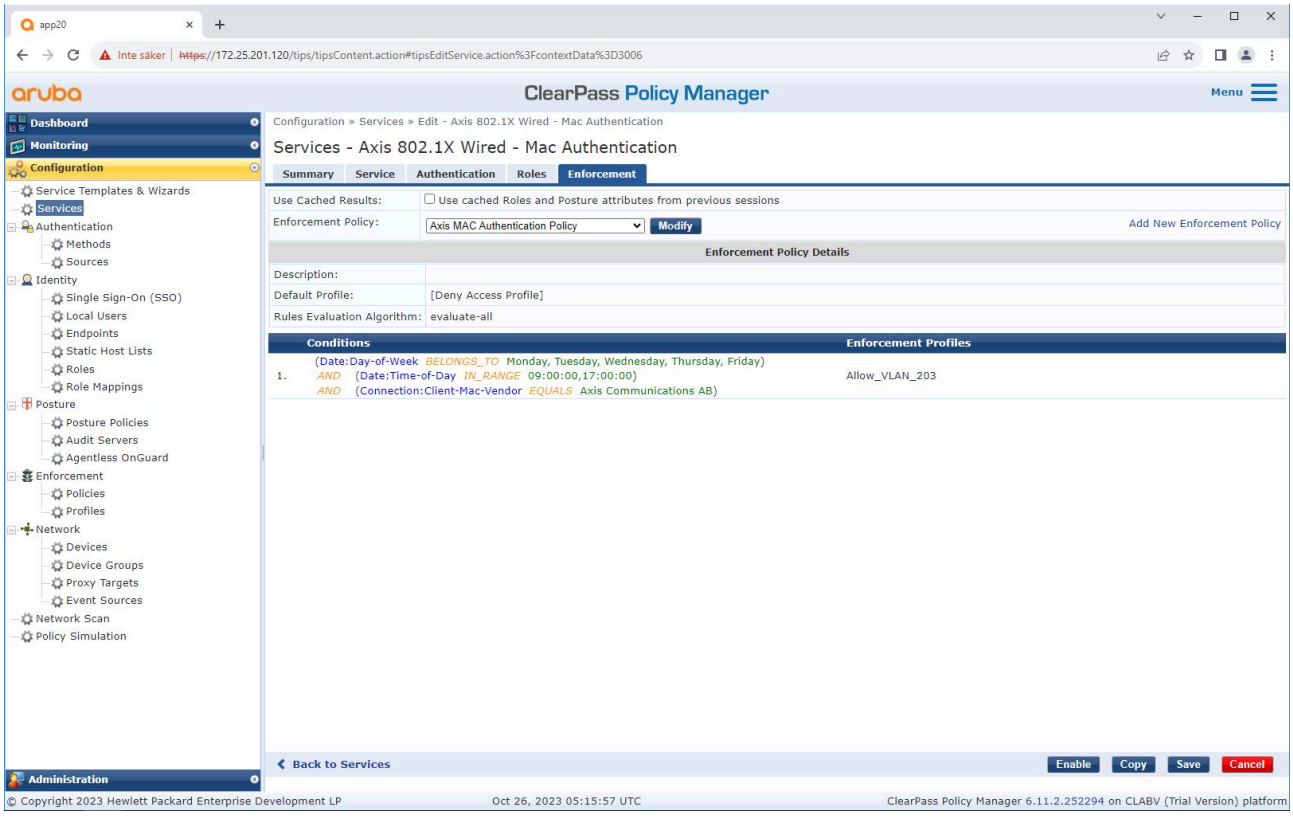
È possibile utilizzare MAC Authentication Bypass (MAB) per integrare dispositivi Axis che non supportano l'onboarding di IEEE 802.1AR con il certificato ID dispositivo Axis e IEEE 802.1X abilitato nello stato predefinito di fabbrica. Se l'onboarding 802.1X non riesce, ClearPass Policy Manager convalida il MAC address del dispositivo Axis e concede l'accesso alla rete.

MAB richiede la preparazione della configurazione sia dello switch di accesso sia di ClearPass Policy Manager. Non è necessaria alcuna configurazione sul dispositivo Axis per consentire l'integrazione di MAB integrato.

HPE Aruba Networking ClearPass Policy Manager

Politica di applicazione

La configurazione della policy di applicazione in ClearPass Policy Manager definisce se ai dispositivi Axis viene concesso l'accesso alle reti alimentate da HPE Aruba Networking in base alle seguenti due condizioni di policy di esempio.



Accesso alla rete negato

Se il dispositivo Axis non soddisfa i criteri di applicazione configurati, gli viene negato l'accesso alla rete.

Rete ospite (VLAN 203)

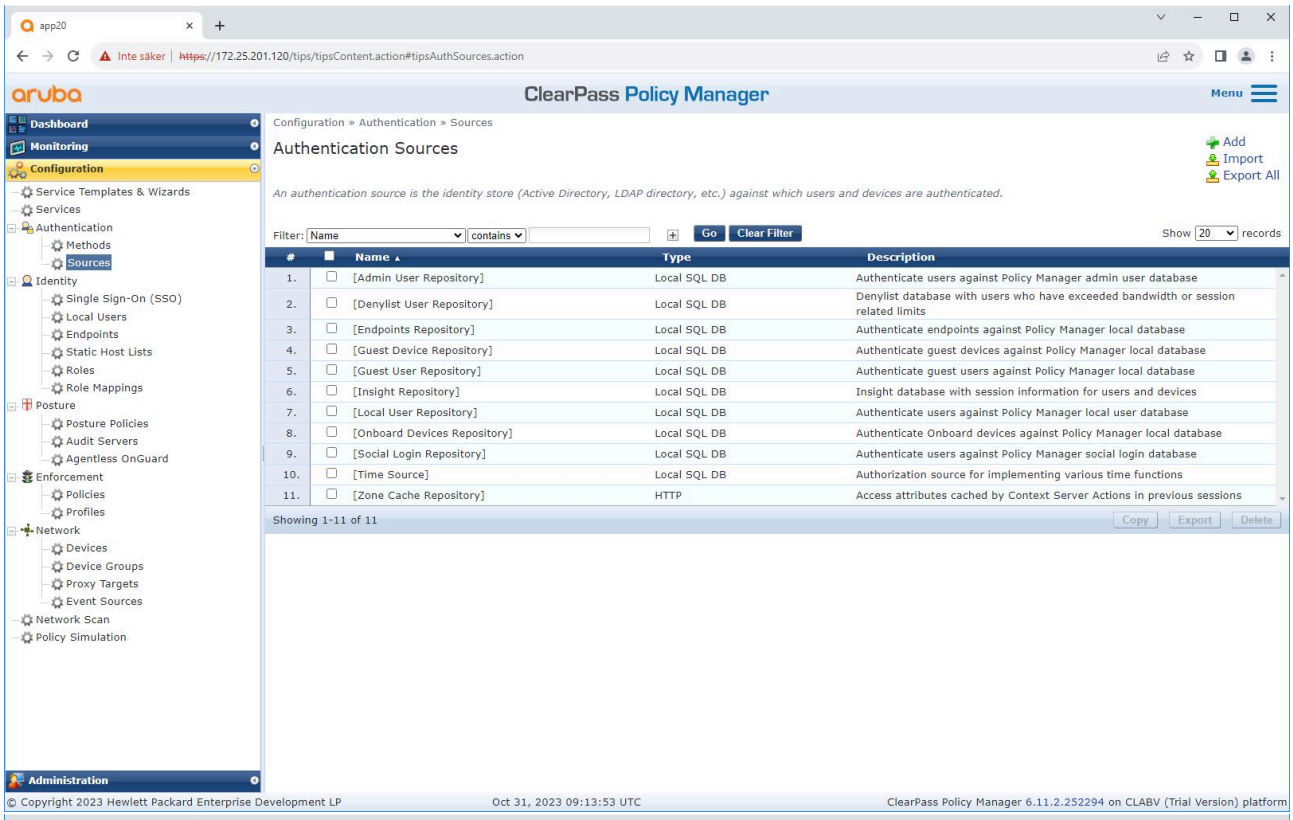
Al dispositivo Axis viene concesso l'accesso a una rete limitata e isolata se vengono soddisfatte le seguenti condizioni:

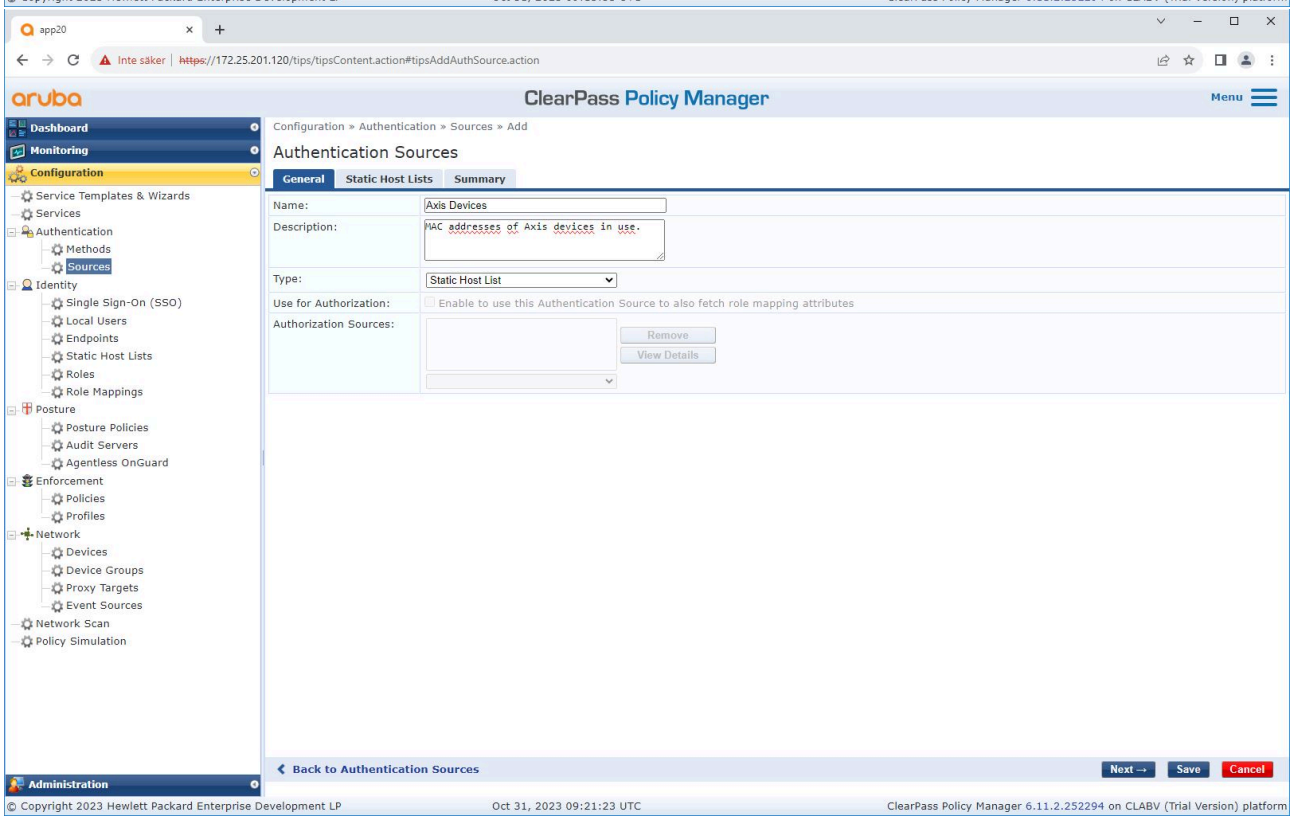
- Il giorno è un giorno feriale, dal lunedì al venerdì.
- L'orario è compreso tra le 09:00 e le 17:00.
- Il fornitore del MAC address corrisponde ad Axis Communications.

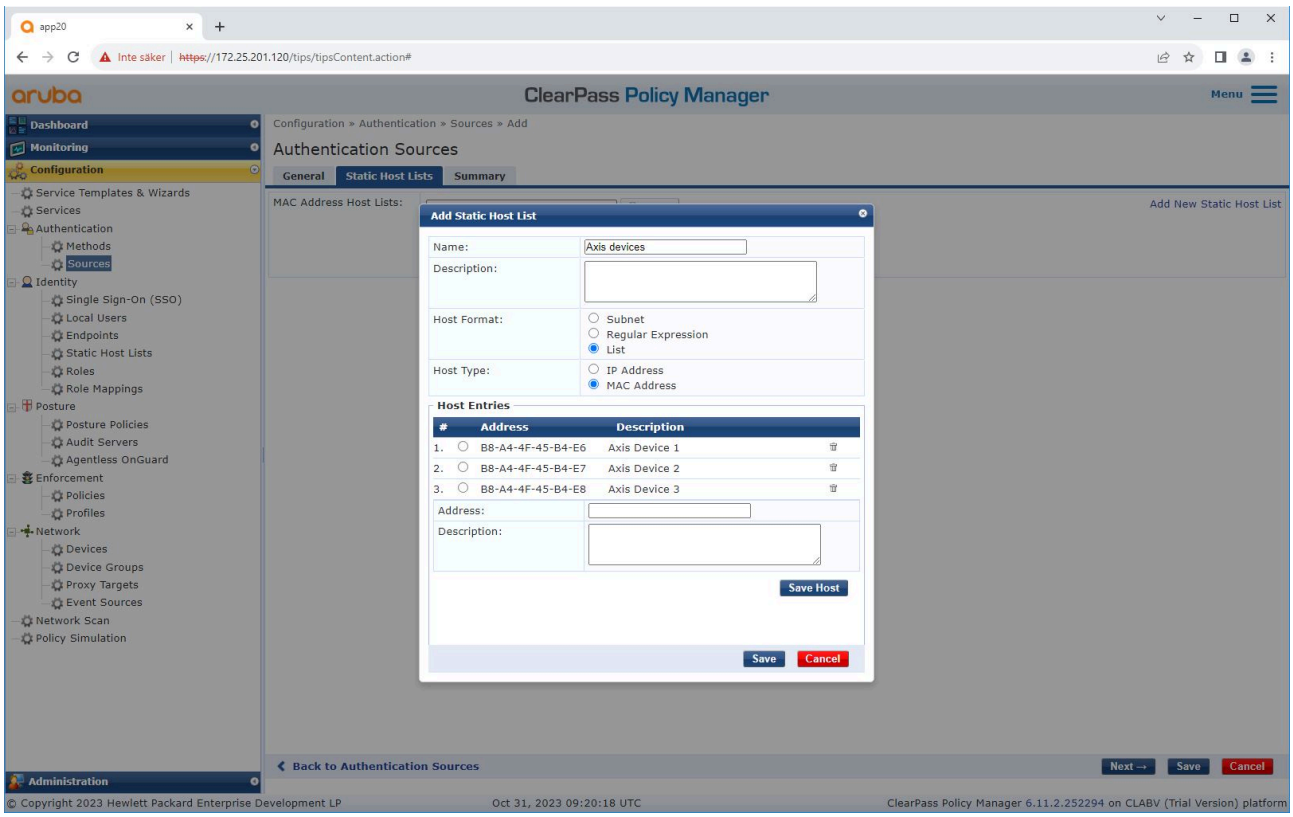
Poiché è possibile falsificare i MAC address, non è consentito l'accesso alla rete di provisioning regolare. Ti consigliamo di utilizzare MAB solo per l'onboarding iniziale e di ispezionare quindi manualmente il dispositivo.

Configurazione di origine

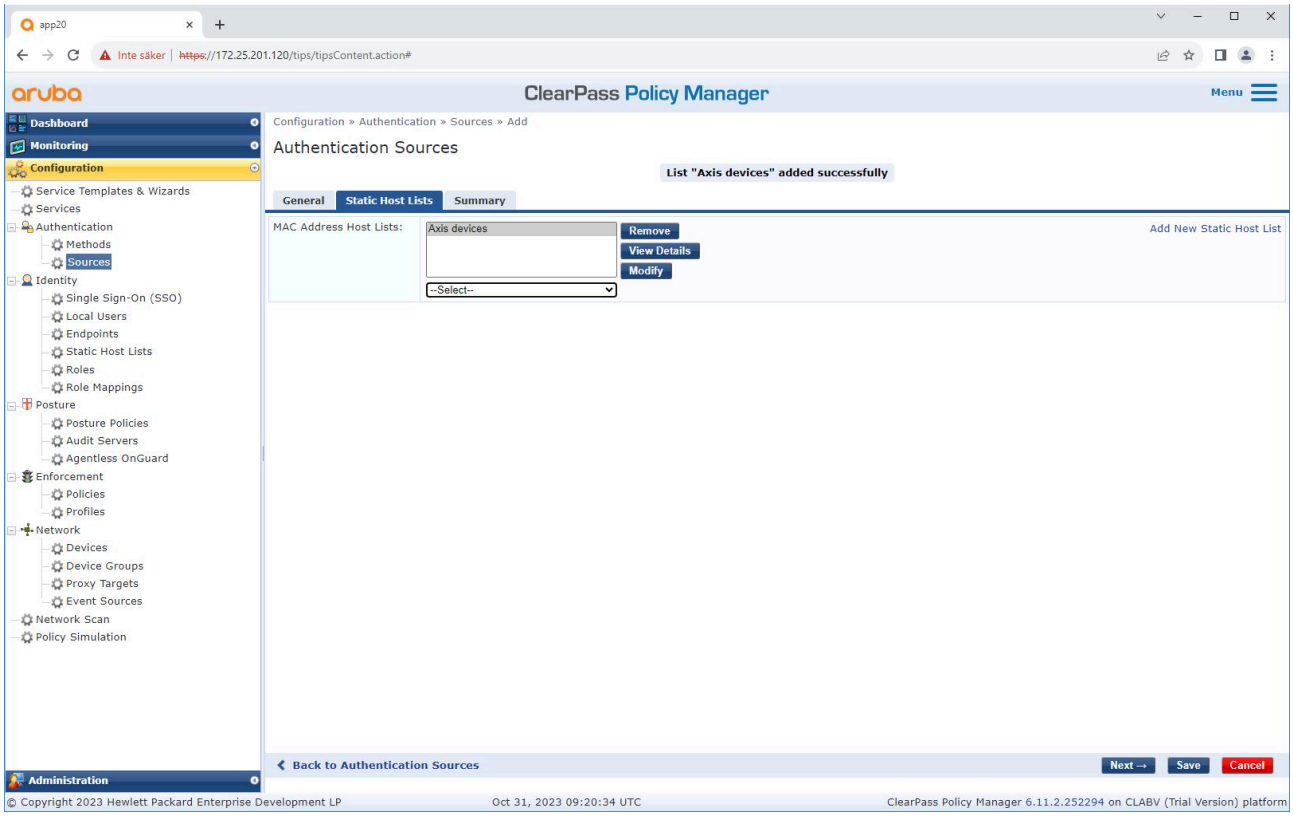
Nella pagina **Sources (Origini)** viene creata una nuova origine di autenticazione per consentire solo MAC address importati manualmente.





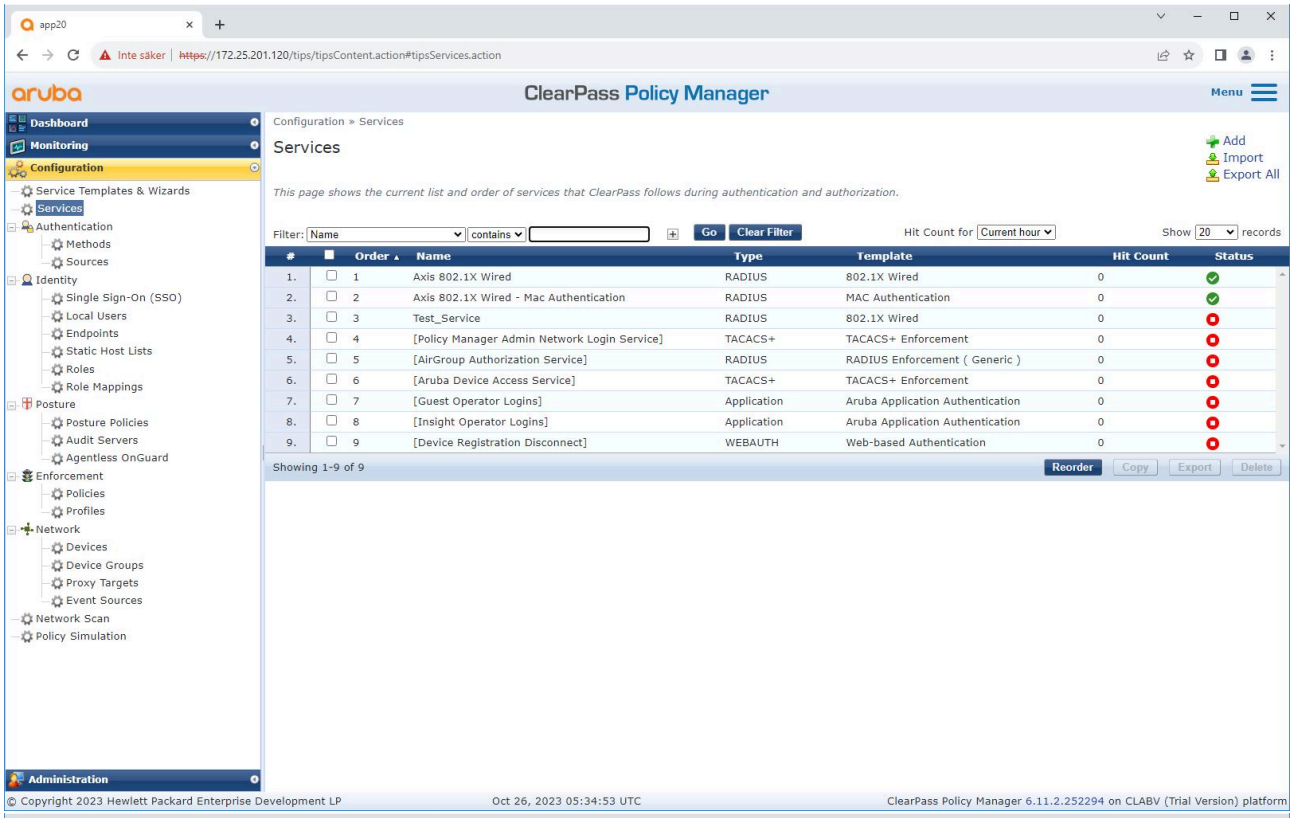


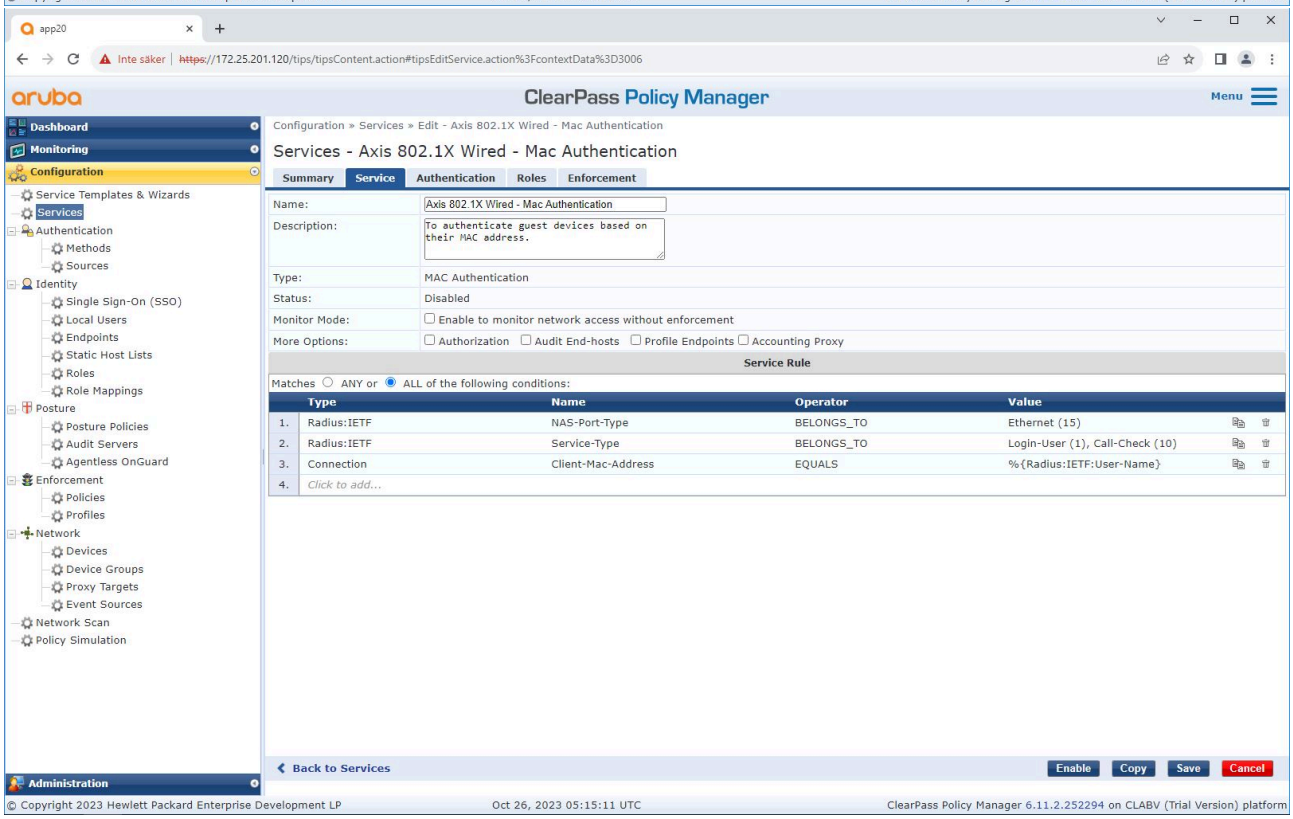
Viene creato un elenco host statico contenente i MAC address Axis.



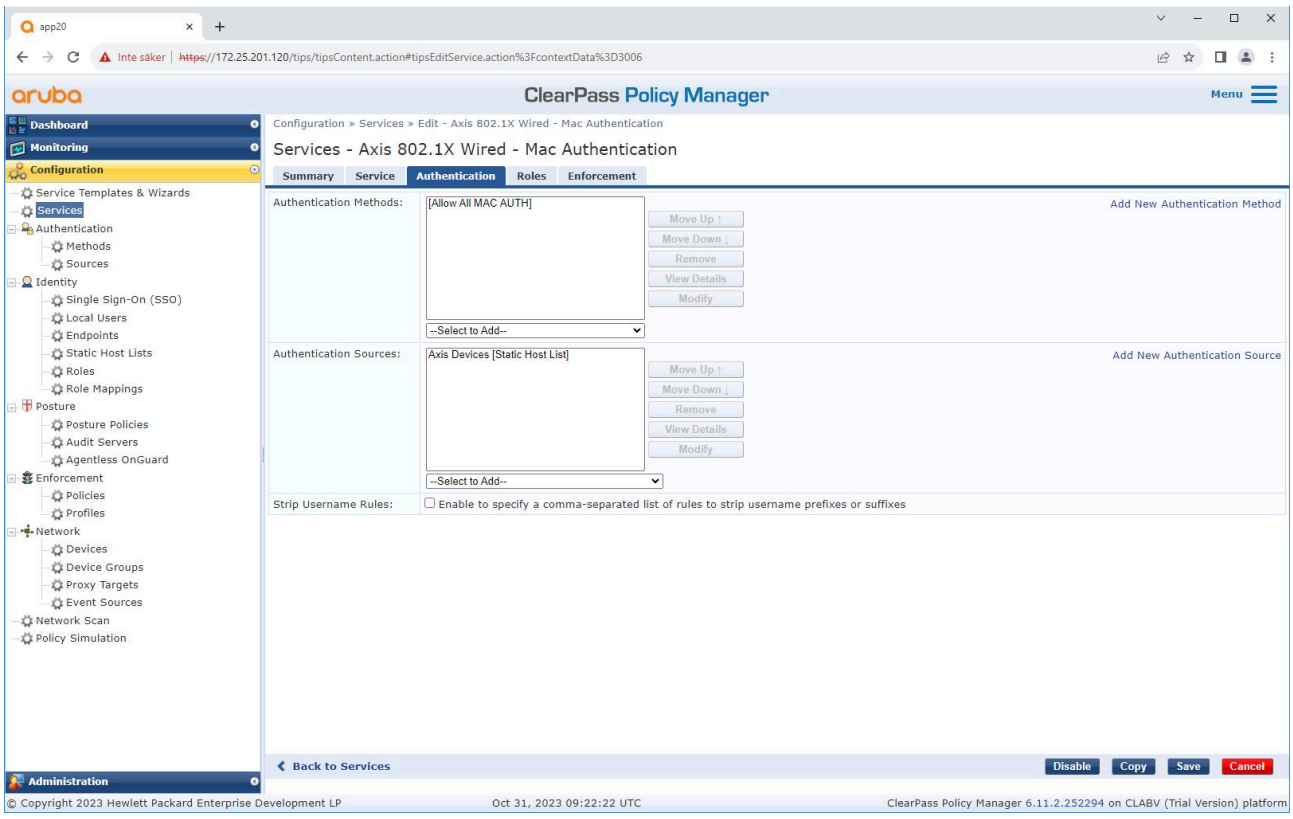
Configurazione del servizio

Nella pagina **Services (Servizi)**, i passaggi di configurazione sono riuniti in un singolo servizio che gestisce l'autenticazione e l'autorizzazione dei dispositivi Axis nelle reti HPE Aruba Networking.





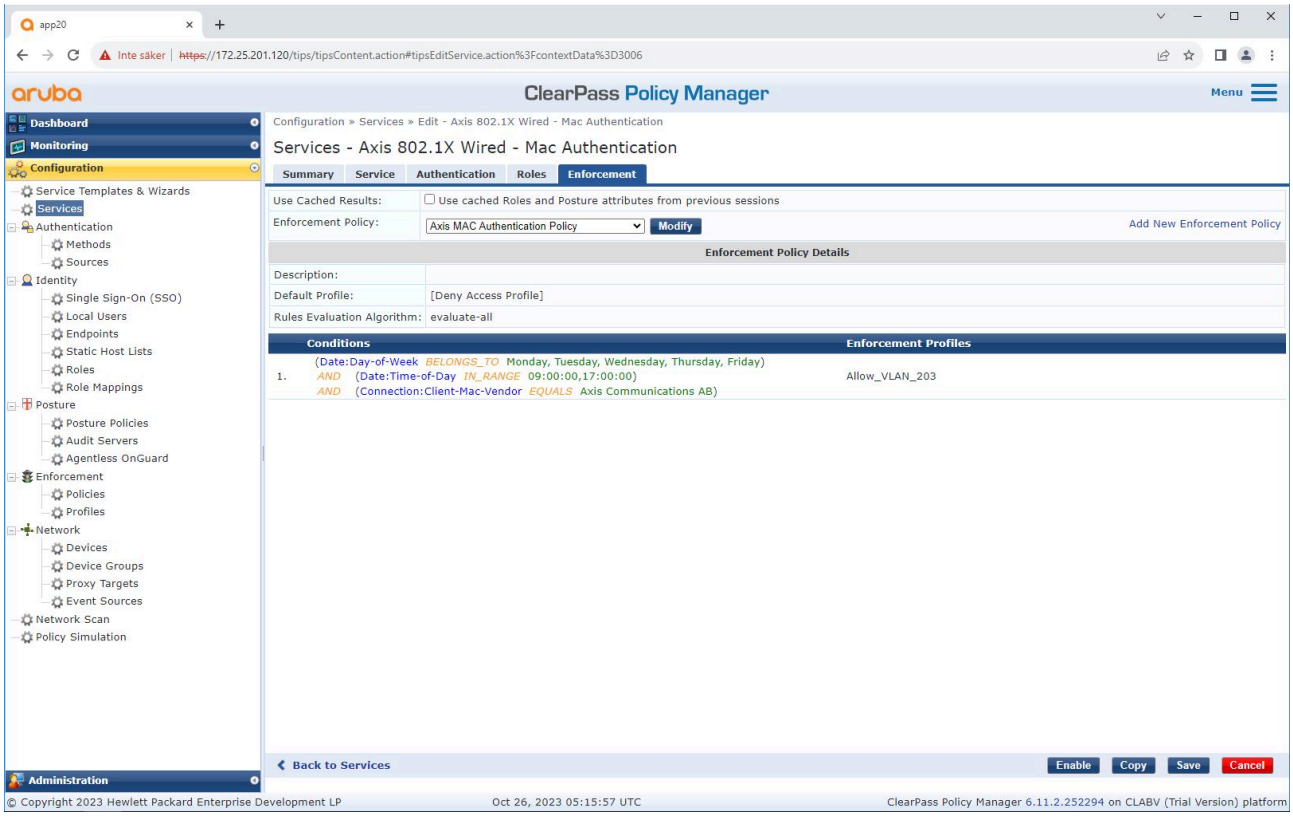
Viene creato un servizio Axis dedicato che definisce MAB come un metodo di connessione.



Il metodo di autenticazione MAC preconfigurato viene configurato per il servizio. Inoltre, viene selezionata la fonte di autenticazione (creata in precedenza) contenente un elenco di MAC address Axis.

Axis Communications utilizza i seguenti OUI del MAC address:

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



Nell'ultimo passaggio, si configura per il servizio la politica di applicazione creata in precedenza.

Switch di accesso HPE Aruba Networking

Oltre alla configurazione di onboarding sicura descritta in *Switch di accesso HPE Aruba Networking, on page 15*, vedere il seguente esempio di configurazione della porta affinché lo switch di accesso HPE Aruba Networking consenta il 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_it

2026-02 (M8.3)

© 2023 – 2026 Axis Communications AB