HPE Aruba Networking

Guida all'integrazione

HPE Aruba Networking

Sommario

HPE Aruba Networking

Introduzione

Introduzione

Questa guida all'integrazione mira a delineare la configurazione delle migliori pratiche su come eseguire l'onboarding e il funzionamento dei dispositivi Axis nelle reti alimentate da 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. Consente l'eliminazione di inutili complessità di sistema quando si utilizzano applicazioni di gestione dei dispositivi Axis combinate con infrastrutture e applicazioni HPE Aruba Networking. Di seguito sono riportati solo alcuni vantaggi che si possono ottenere combinando dispositivi e software Axis con un'infrastruttura HPE Aruba Networking:

- Riduci al minimo la complessità del sistema rimuovendo le reti di gestione temporanea dei dispositivi.
- Risparmia sui costi automatizzando i processi di onboarding e la gestione dei dispositivi.
- Sfrutta i controlli di sicurezza di rete zero-touch forniti dai dispositivi Axis.
- Aumenta la sicurezza complessiva della rete applicando le competenze HPE e Axis.

L'infrastruttura di rete deve essere preparata per verificare in modo sicuro l'integrità dei dispositivi Axis prima di iniziare la configurazione. Ciò consente una transizione fluida definita dal software tra le reti logiche durante tutto il processo di onboarding. È necessario conoscere le seguenti aree prima di eseguire la configurazione:

- 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 degli accessi alla rete e nelle politiche di sicurezza della rete.
- È auspicabile una conoscenza di base dei dispositivi Axis, ma è fornita in tutta la guida.

Onboarding sicuro: IEEE 802.1AR/802.1X

Per guardare questo video, visitare la versione Web di questo documento.

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

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

Autenticazione iniziale

Connetti il dispositivo Axis supportato da Axis Edge Vault per autenticare il dispositivo sulla rete. Il dispositivo utilizza il certificato ID dispositivo Axis IEEE 802.1AR tramite il controllo degli accessi alla rete IEEE 802.1X per autenticarsi.

Per garantire l'accesso alla rete, ClearPass Policy Manager verifica l'ID del dispositivo Axis insieme ad altre impronte digitali specifiche del dispositivo. Le informazioni, come l'indirizzo MAC e l'AXIS OS in esecuzione, vengono utilizzate per prendere una decisione basata sulla politica.

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 alimentata da 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

In seguito all'autenticazione, il dispositivo Axis si sposta nella rete di provisioning (VLAN201) dove AXIS Device Manager è installato. Tramite AXIS Device Manager è possibile eseguire la configurazione del dispositivo, il rafforzamento della sicurezza e gli aggiornamenti 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 deciderà se spostare o meno il dispositivo Axis nella rete di produzione.

Dopo la configurazione, il dispositivo Axis lascia la rete di provisioning e tenta di autenticarsi nuovamente 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 riautenticazione, il dispositivo Axis si sposta nella rete di produzione (VLAN 202). In tale rete, il Video Management System (VMS) si connette al dispositivo Axis e inizia a funzionare.

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

1. *Interruttore di accesso*
2. *Rete di produzione*
3. *ClearPass Policy Manager*
4. *Video Management System*

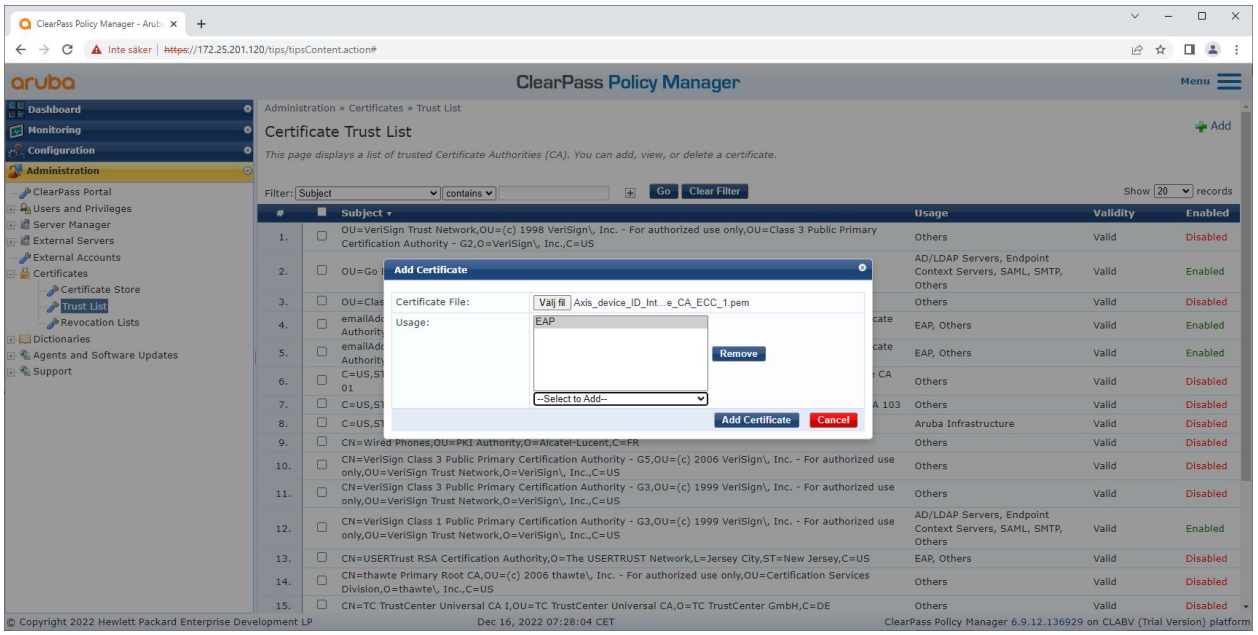
Configurazione HPE Aruba Networking

HPE Aruba Networking ClearPass Policy Manager

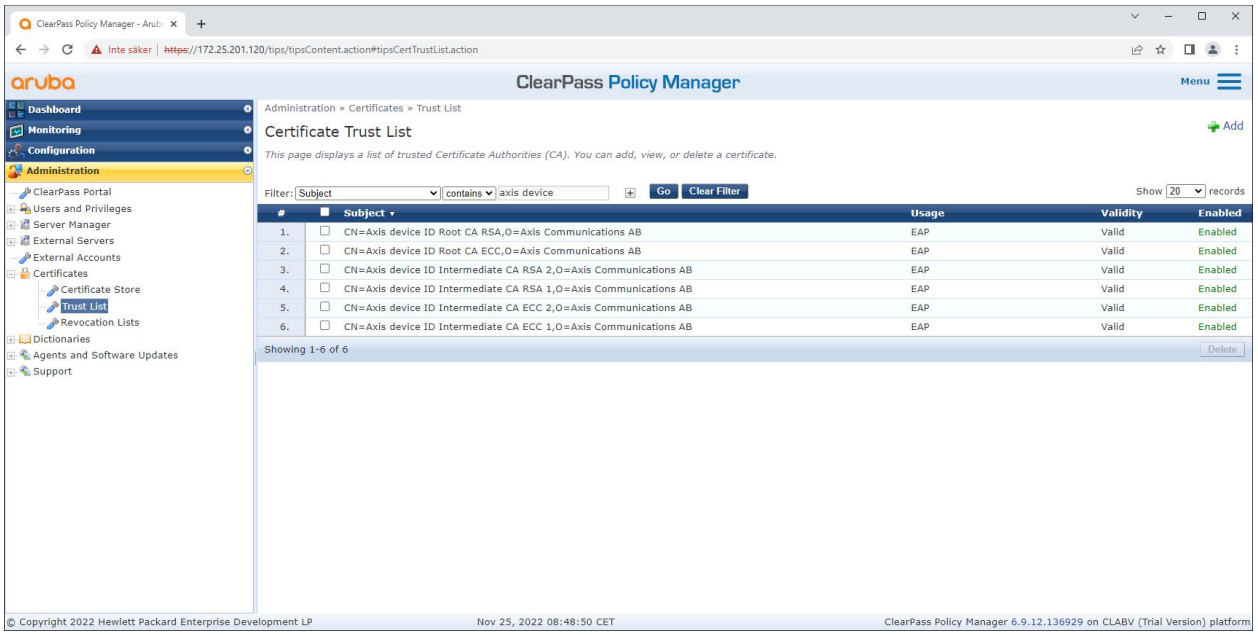
ClearPass Policy Manager fornisce un controllo degli accessi sicuro alla rete basato su ruoli e dispositivi per IoT, BYOD, dispositivi aziendali, dipendenti, collaboratori esterni e ospiti su infrastrutture cablate, wireless e VPN multivendor.

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 root 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.



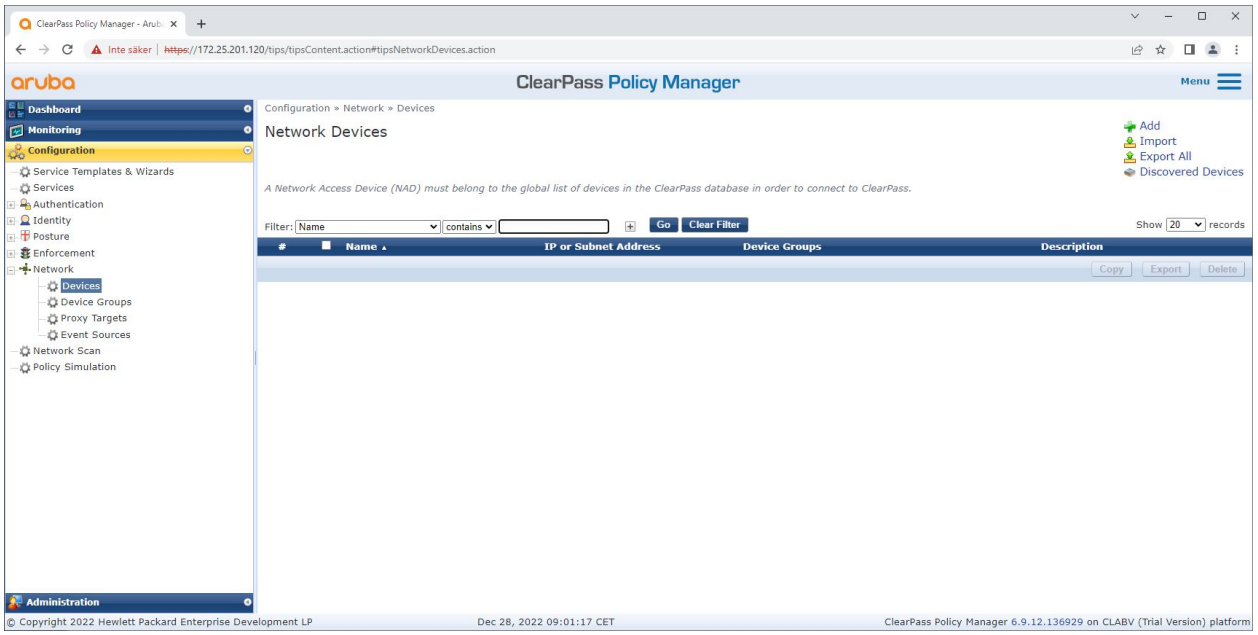
L'archivio certificati attendibili in ClearPass Policy Manager con catena di certificati IEEE 802.1AR specifica di Axis inclusa.

Configurazione del dispositivo/gruppo di rete

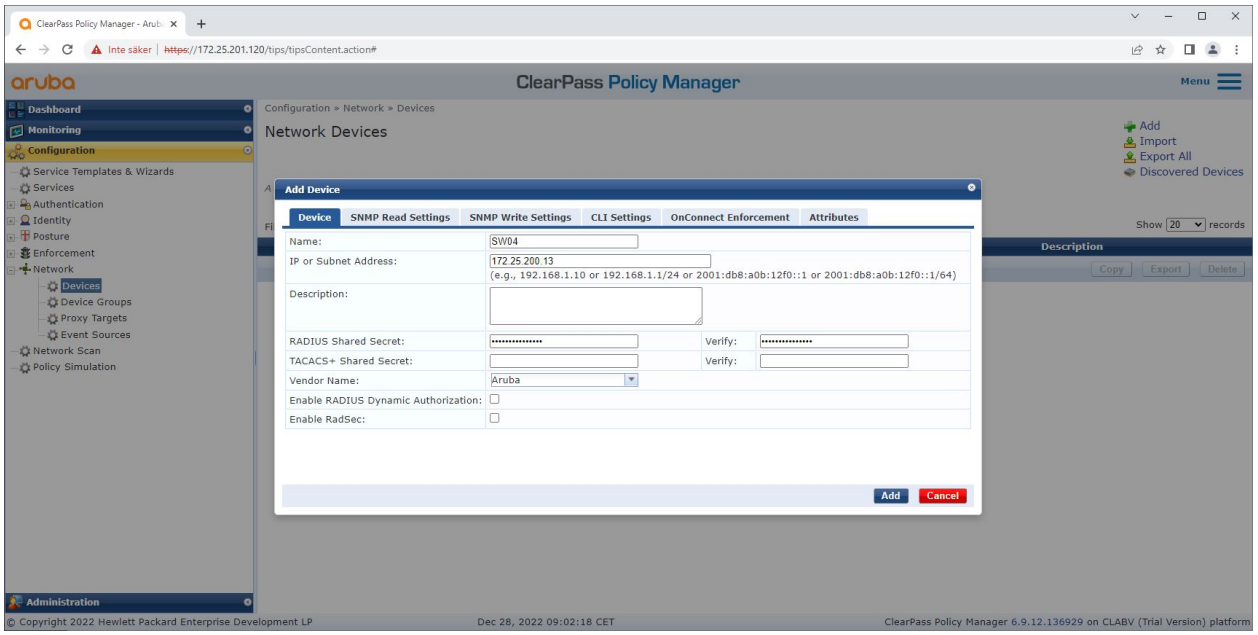
1. Aggiungere dispositivi di accesso alla rete affidabili, come gli switch di accesso HPE Aruba Networking, a ClearPass Policy Manager. ClearPass Policy Manager deve sapere quali switch di accesso nella rete sono utilizzati per la comunicazione IEEE 802.1X.

2. Utilizzare la configurazione del gruppo di dispositivi di rete per raggruppare diversi dispositivi di accesso alla rete attendibili. Il raggruppamento di dispositivi di accesso alla rete attendibili consente una configurazione più semplice della policy.

3. Il segreto condiviso RADIUS deve corrispondere alla configurazione IEEE 802.1X specifica dello switch.

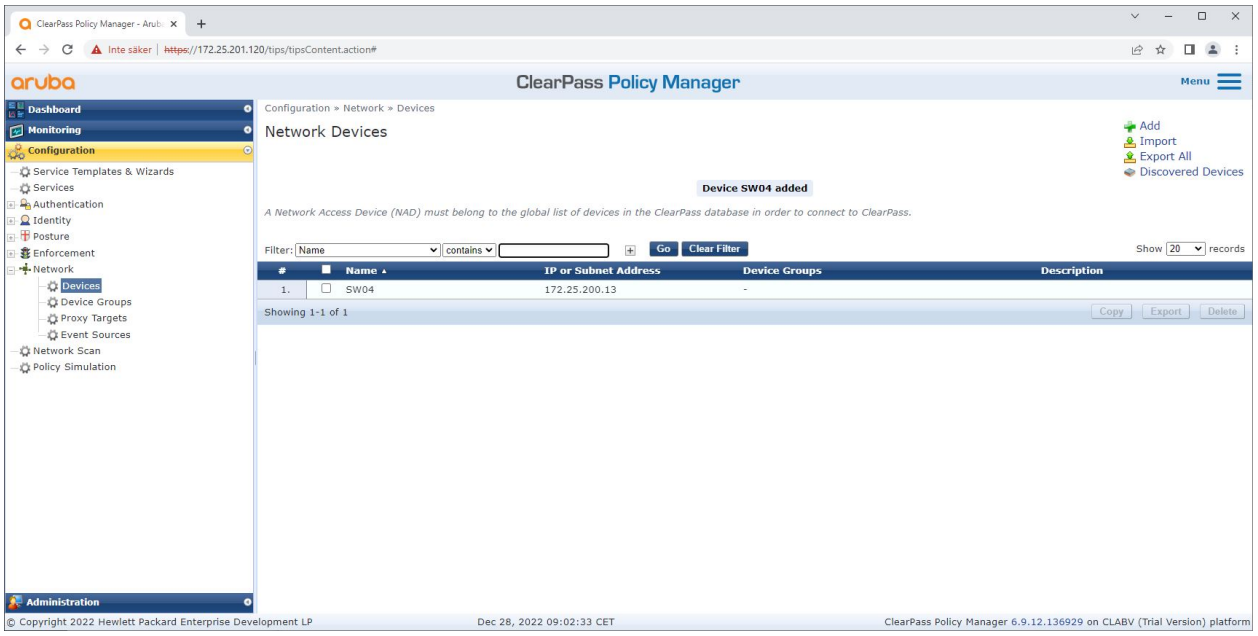


L'interfaccia dei dispositivi di rete attendibili in ClearPass Policy Manager.

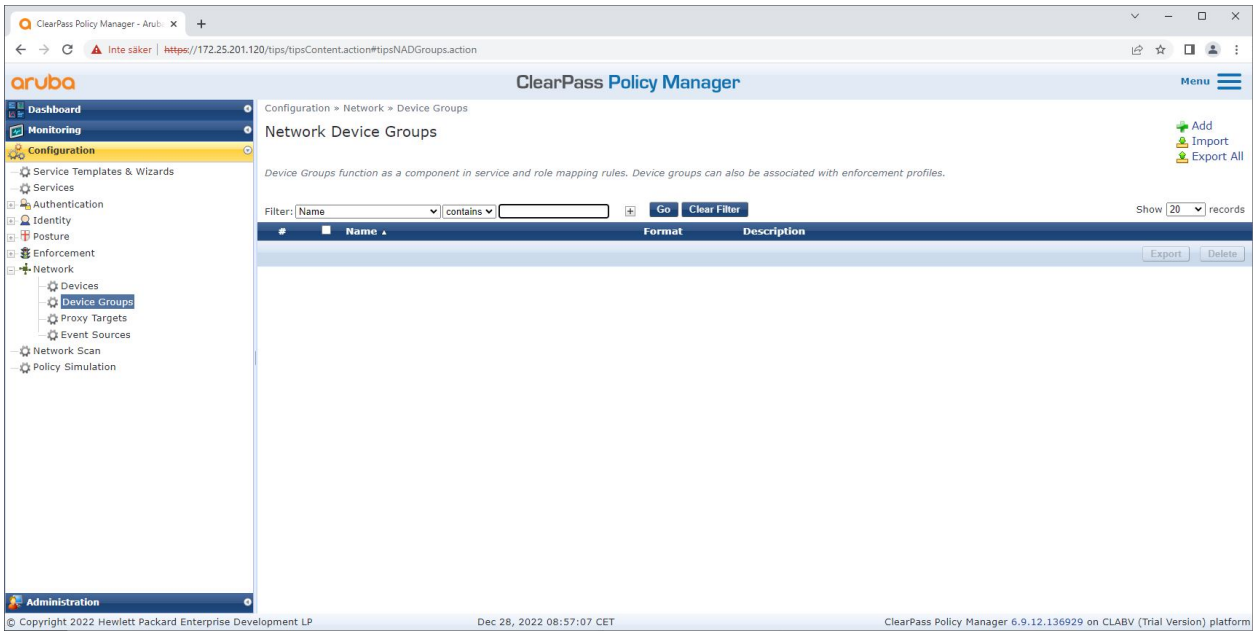


Aggiungere lo switch di accesso HPE Aruba Networking come dispositivo di rete affidabile in Aruba ClearPass Policy Manager. Tieni presente che il segreto condiviso RADIUS deve corrispondere alla configurazione IEEE 802.1X specifica dello switch.

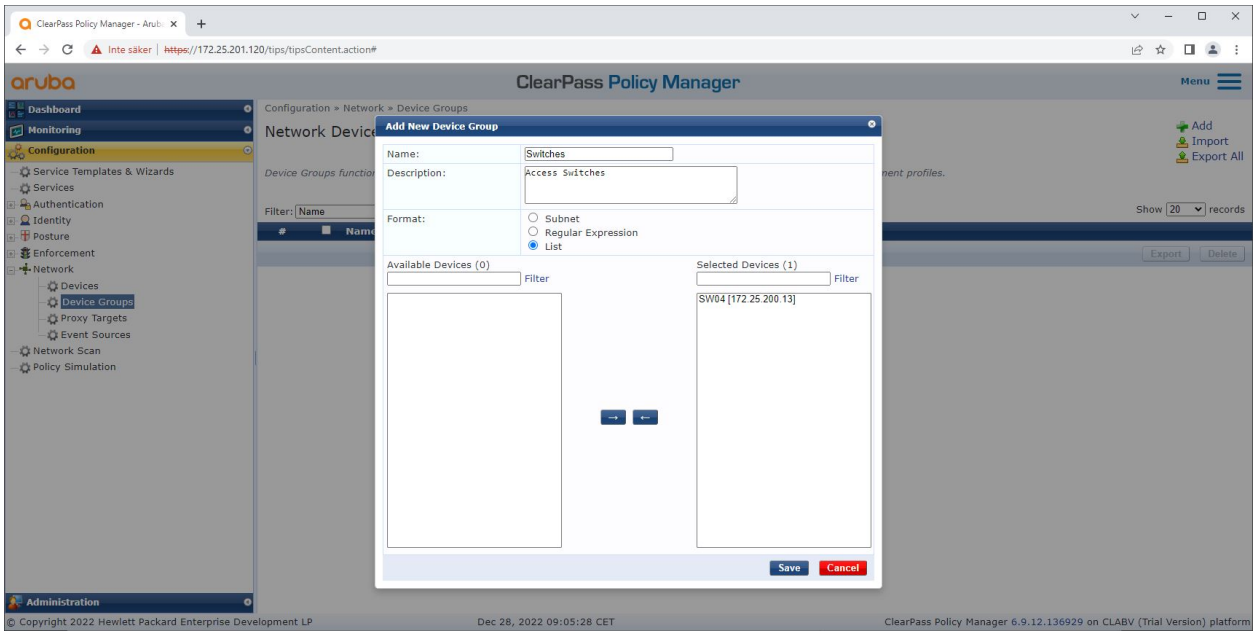
Onboarding sicuro: IEEE 802.1AR/802.1X



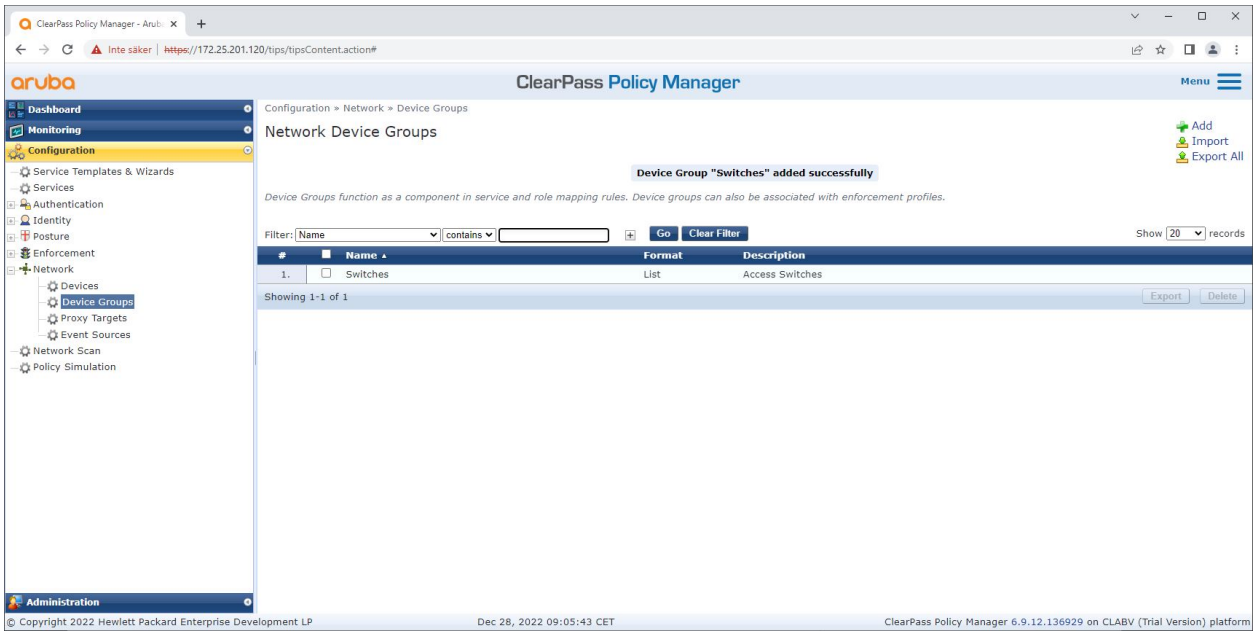
ClearPass Policy Manager con un dispositivo di rete affidabile configurato.



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



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



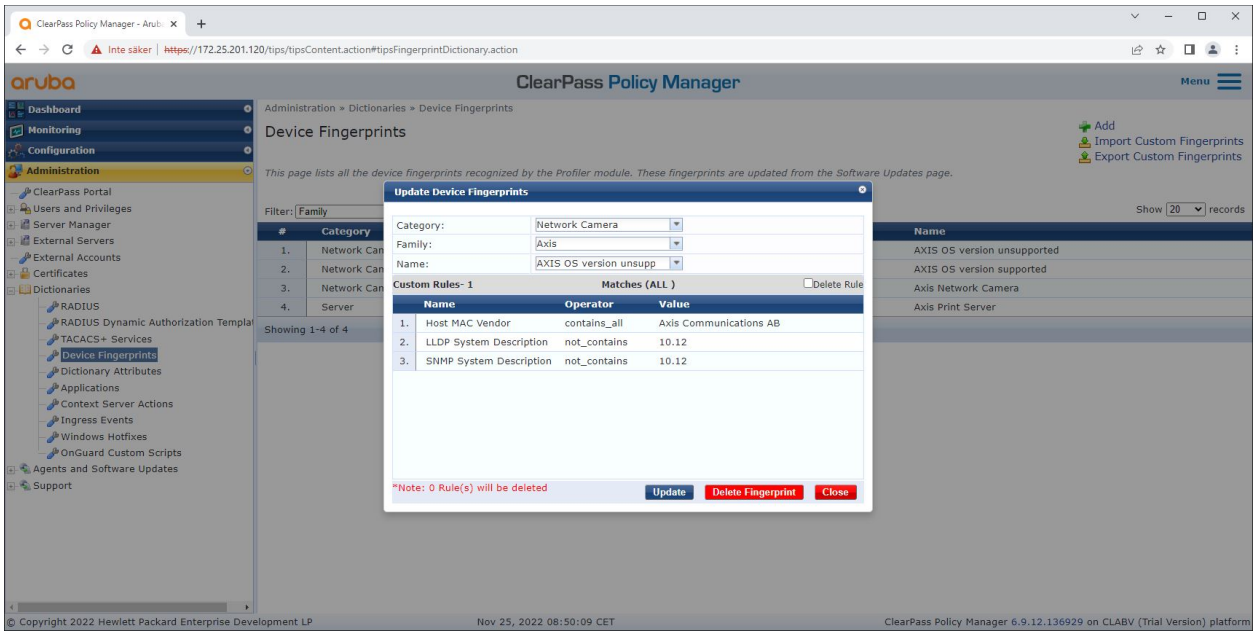
ClearPass Policy Manager con gruppo di dispositivi di rete configurato che include uno o più dispositivi di rete attendibili.

Configurazione dell'impronta digitale del dispositivo

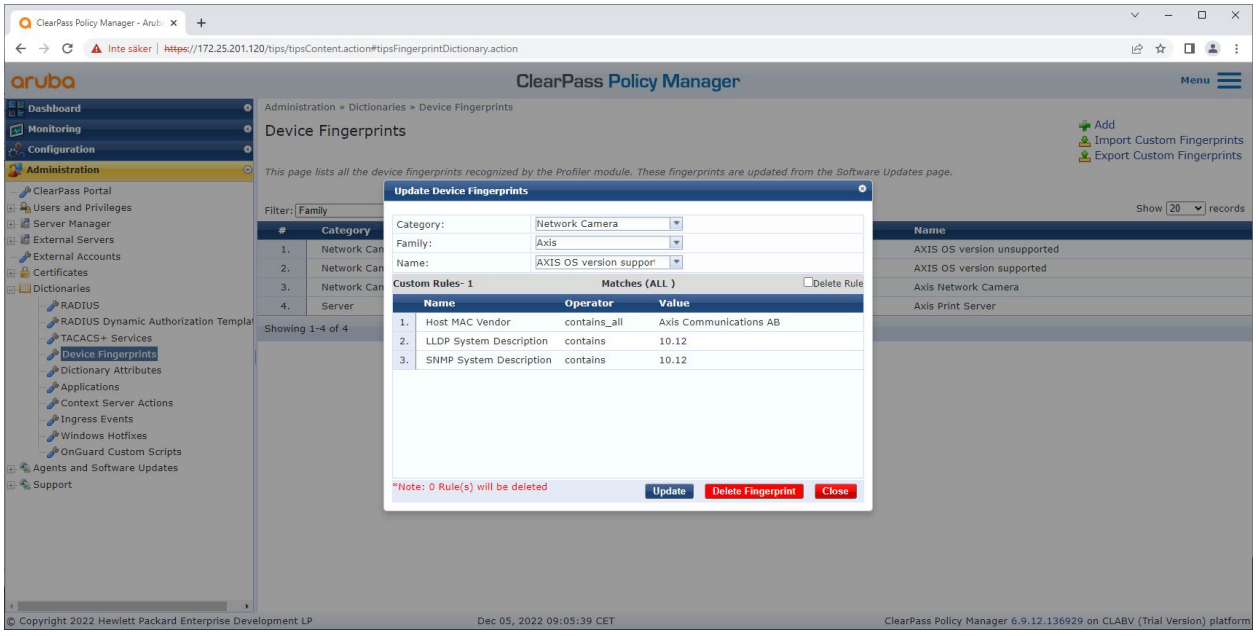
Il dispositivo Axis può distribuire informazioni specifiche sul dispositivo, come l'indirizzo MAC e la versione del software dispositivo, tramite il rilevamento della rete. Usare tali informazioni per la creazione, l'aggiornamento o la gestione dell'impronta digitale di un dispositivo in ClearPass Policy Manager. Si può anche concedere o negare l'accesso secondo la 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 eseguono qualsiasi altra versione di AXIS OS diversa dalla 10.12 sono considerati non supportati.



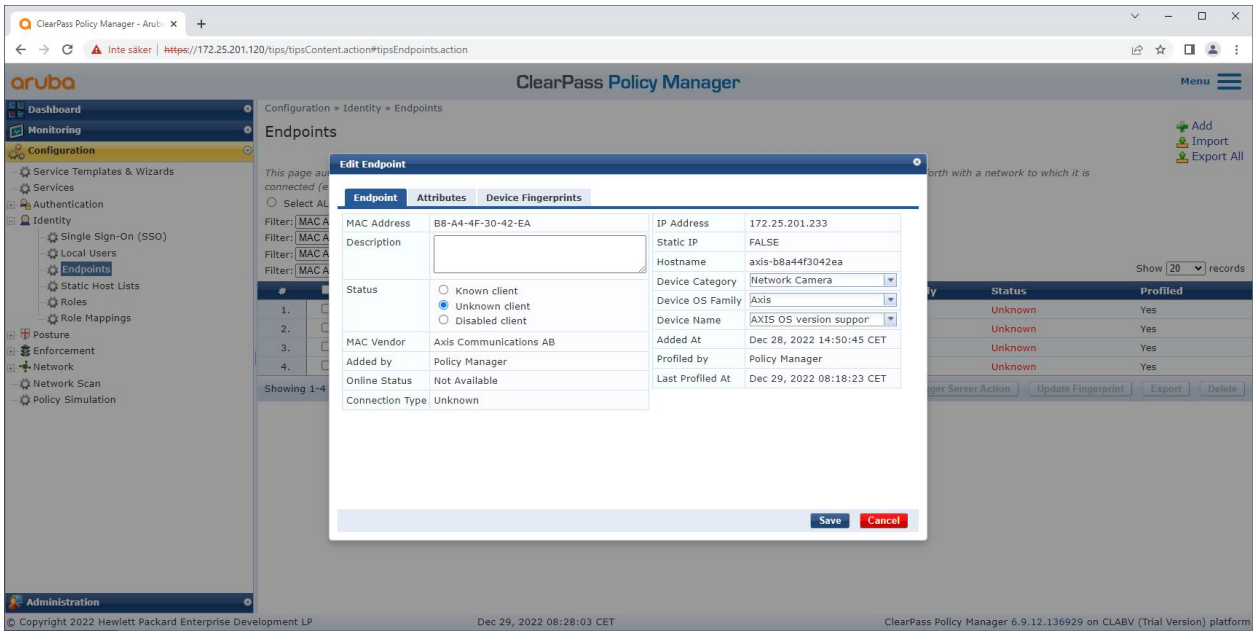
La configurazione dell'impronta digitale del dispositivo in ClearPass Policy Manager. I dispositivi Axis che eseguono AXIS OS 10.12 sono considerati supportati nell'esempio precedente.

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

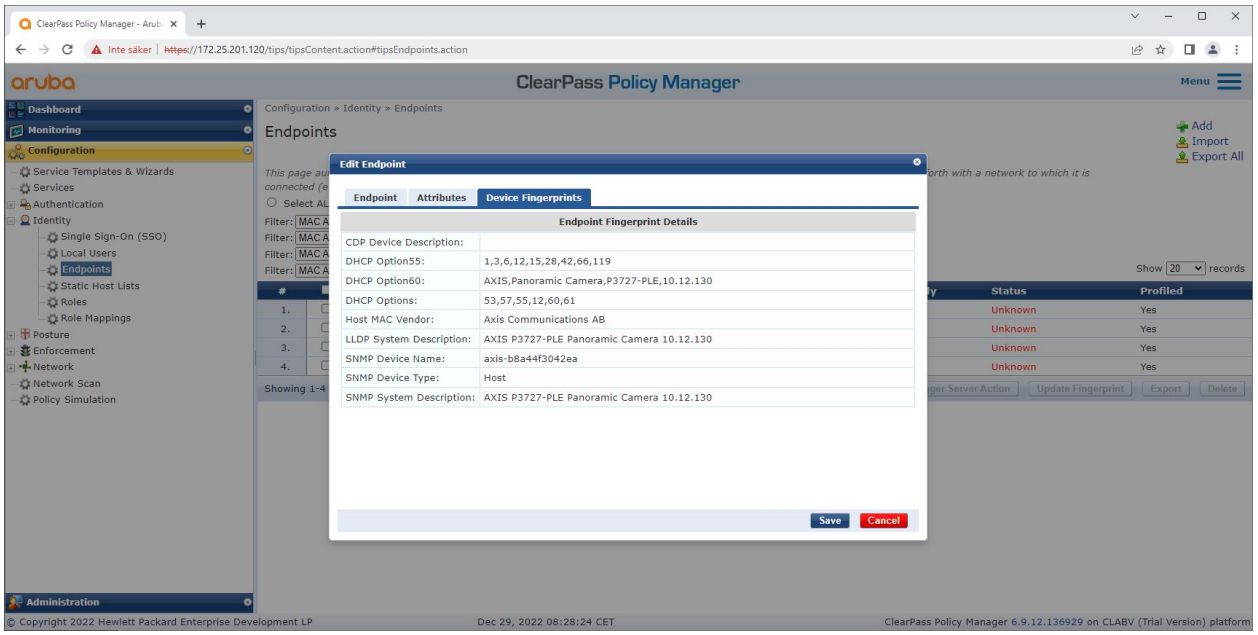
1. Andare a **Configuration > Identity > Endpoints (Configurazione > Identità > Endpoint)**.
2. Selezionare il dispositivo che desideri visualizzare.
3. Fare clic sulla scheda **Device Fingerprints (Impronte digitali)** del dispositivo.

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.

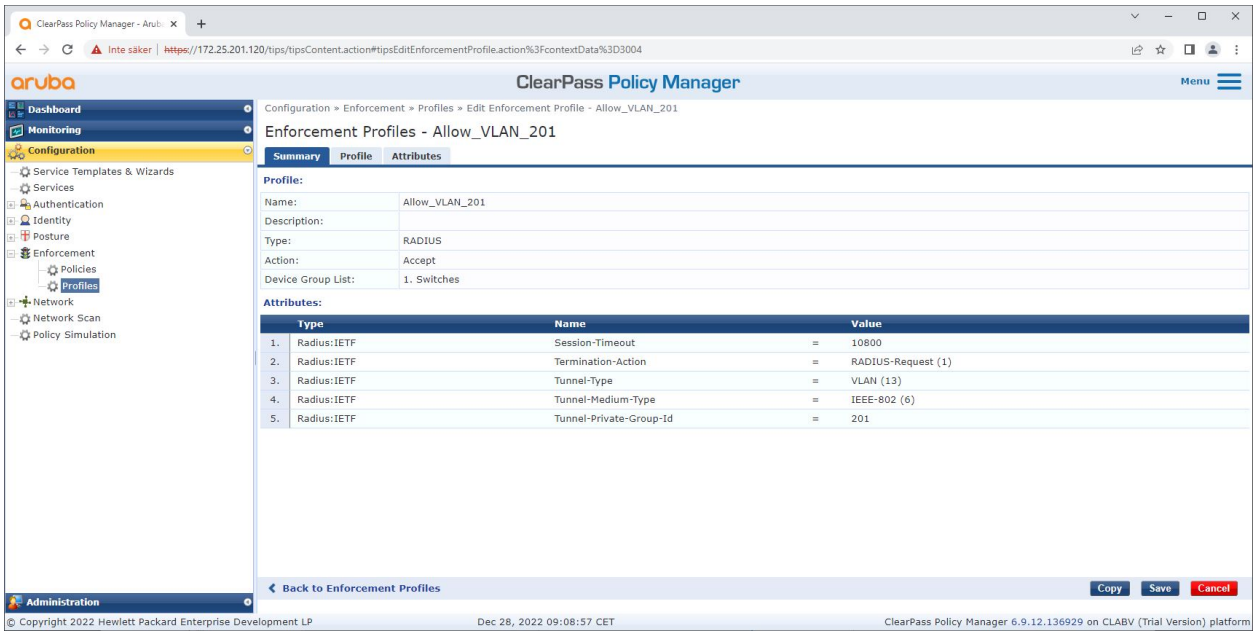


Le Impronte digitali dettagliate di un dispositivo Axis profilato. Tieni presente che SNMP è disabilitato per impostazione predefinita nei dispositivi Axis. Le informazioni di rilevamento specifiche di LLDP, CDP e DHCP vengono condivise dal dispositivo Axis nello stato predefinito di fabbrica e inoltrate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

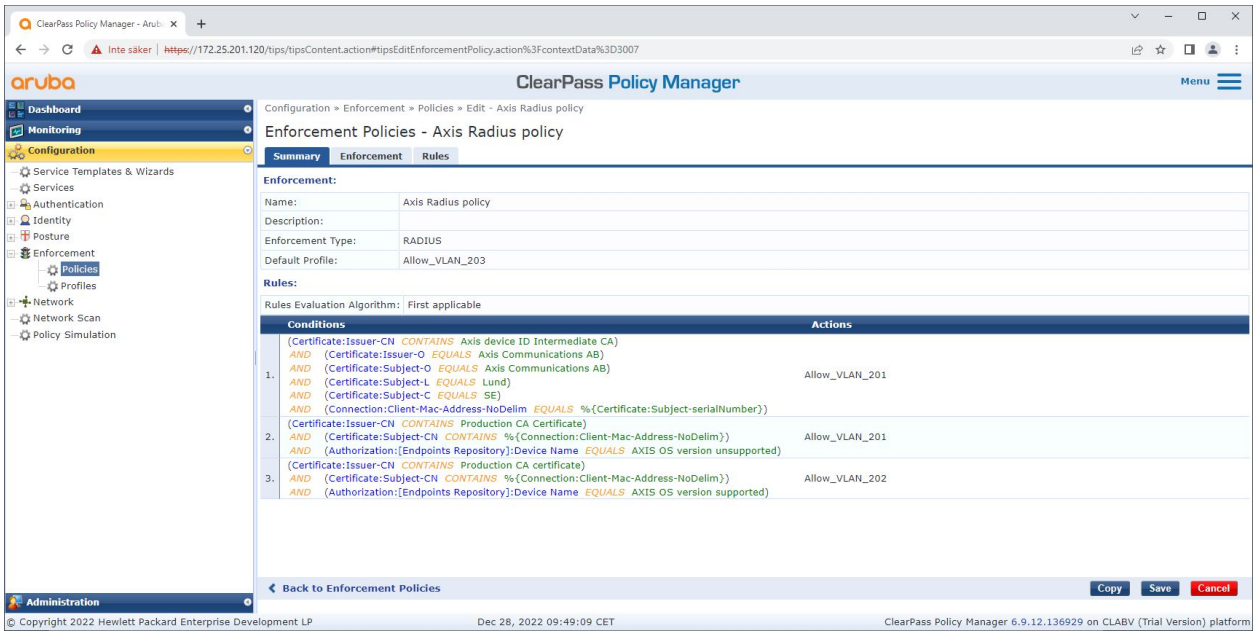
Configurazione del profilo di applicazione

Enforcement Profile (Profilo esecutivo) viene utilizzato per consentire ad Aruba 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 necessario di profili di applicazione dipende dal numero di VLAN utilizzate. Nella nostra configurazione sono presenti un totale di tre VLAN (VLAN 201, 202, 203), correlate a tre profili di applicazione.

Dopo aver configurato i profili di imposizione per la VLAN, è possibile configurare l'effettivo criterio di imposizione. 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 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 elencate di seguito:

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)

Onboarding sicuro: IEEE 802.1AR/802.1X

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 necessaria l'ispezione manuale del dispositivo per intraprendere 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 dell'AXIS OS del dispositivo Axis.
- L'indirizzo MAC del dispositivo corrisponde allo schema Axis 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.

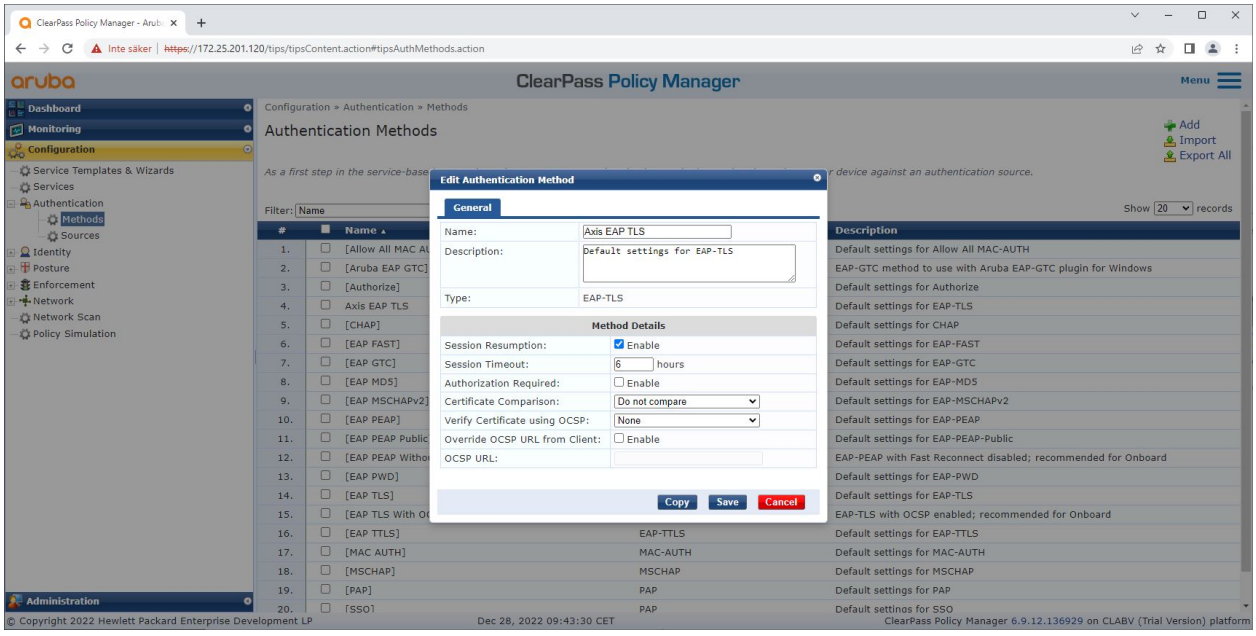
Rete di produzione (VLAN 202)

Al dispositivo Axis è permesso accedere alla rete di produzione dove deve funzionare il dispositivo Axis. 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:

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

Configurazione del metodo di autenticazione

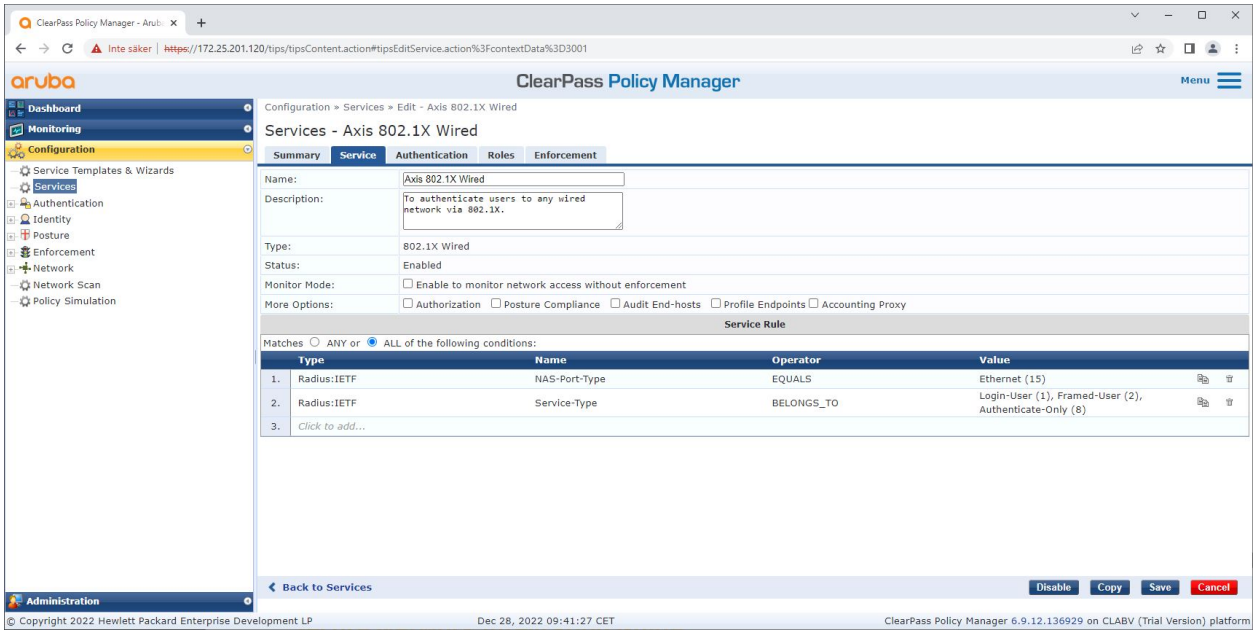
Nel metodo di autenticazione viene definito come un dispositivo Axis tenta di autenticarsi verso la rete. Il metodo di autenticazione preferito dovrebbe essere IEEE 802.1X EAP-TLS poiché i dispositivi Axis con supporto per Axis Edge Vault vengono forniti con IEEE 802.1X EAP-TLS abilitato per impostazione predefinita.



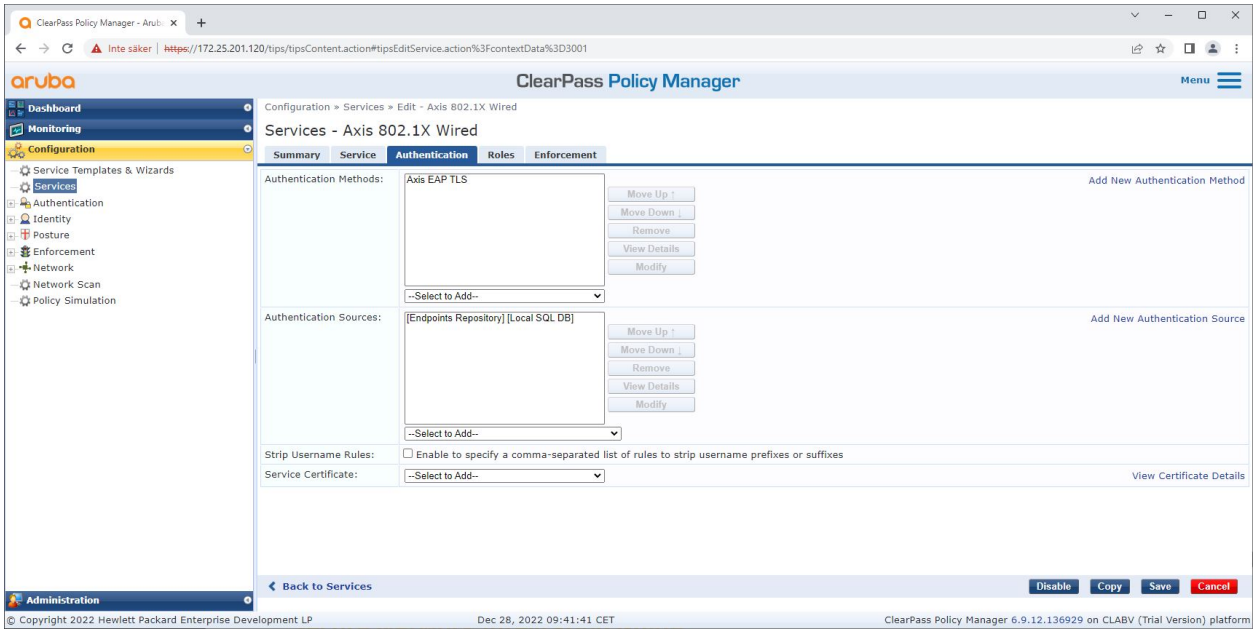
L'interfaccia del metodo di autenticazione di ClearPass Policy Manager in cui viene definito il metodo di autenticazione EAP-TLS per i dispositivi Axis.

Configurazione del servizio

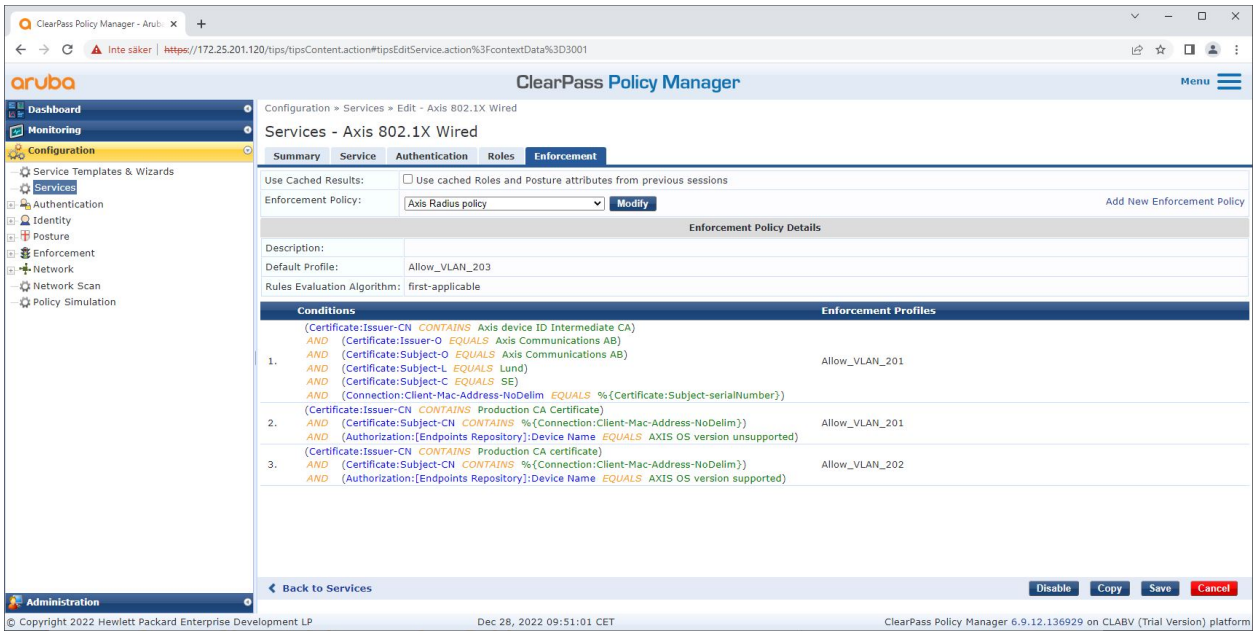
Nella pagina **Services (Servizi)**, i passaggi di configurazione sono riuniti in un unico servizio che gestisce l'autenticazione e l'autorizzazione dei dispositivi Axis nelle reti alimentate da HPE Aruba Networking.



Viene creato un servizio Axis dedicato che definisce IEEE 802.1X come metodo di connessione.



Nel passaggio successivo, il metodo di autenticazione EAP-TLS creato in precedenza viene configurato per il servizio.



Nell'ultimo passaggio, la policy di applicazione creata in precedenza viene configurata per il servizio.

Switch di accesso HPE Aruba Networking

I dispositivi Axis sono collegati direttamente agli switch di accesso compatibili con PoE o tramite midspan PoE Axis compatibili. Per eseguire l'onboarding sicuro dei dispositivi Axis nelle reti alimentate da 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 funge da server RADIUS.

Nota

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

Fare riferimento all'esempio di configurazione globale e delle porte riportato di seguito per gli switch di accesso HPE Aruba Networking.

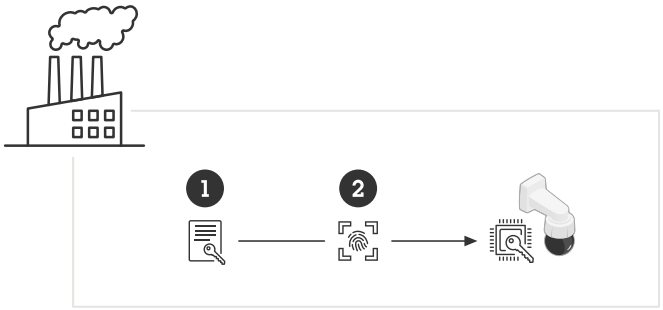
```
radius-server host MyRADIUSIPAddress key "MyRADIUSKey"

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

Axis configurazione

Dispositivo con tecnologia di rete Axis

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

Onboarding sicuro: IEEE 802.1AR/802.1X



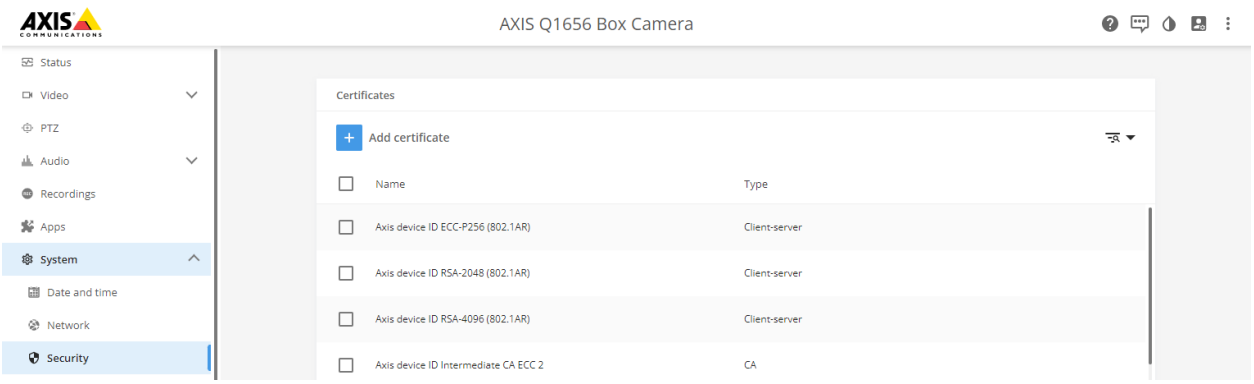
I dispositivi Axis sono prodotti con il certificato ID del dispositivo Axis conforme a IEEE 802.1AR per servizi di identità del dispositivo attendibili

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 scoprire quali dispositivi Axis supportano Axis Edge Vault e Axis Device ID.

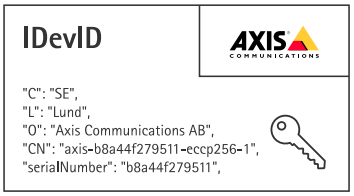
Nota

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.

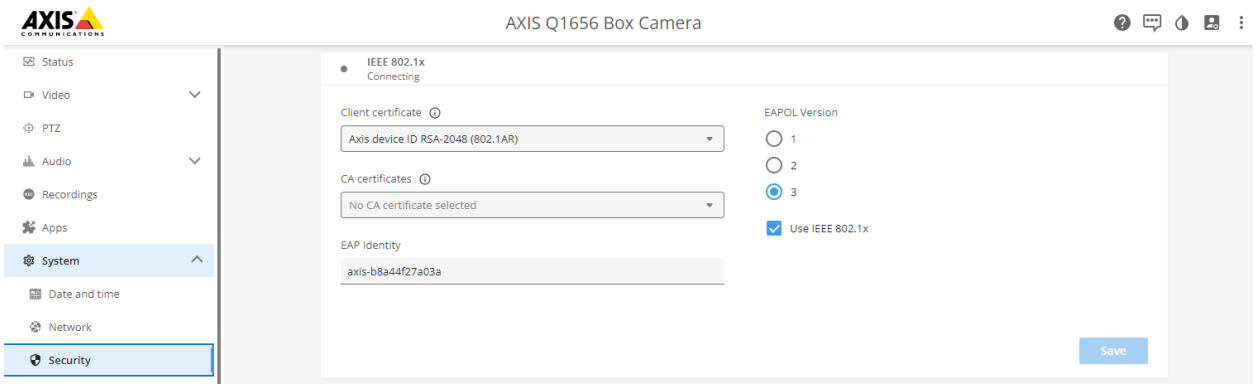
Il certificato ID dispositivo Axis conforme a IEEE 802.1AR include informazioni sul numero di serie e altre informazioni specifiche del fornitore Axis. Le informazioni vengono utilizzate da ClearPass Policy Manager per l'analisi e il processo decisionale per concedere l'accesso alla rete. Fare riferimento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



Country (Paese)	SE
Localizzazione	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 costruito da una combinazione del nome dell'azienda Axis, del numero di serie del dispositivo seguito dall'algoritmo crittografico utilizzato (ECC P256, RSA 2048, RSA 4096). A partire dal sistema operativo AXIS 10.1 (2020-09), IEEE 802.1X è abilitato per impostazione predefinita con l'ID del dispositivo Axis preconfigurato. Ciò consente al dispositivo Axis di autenticarsi sulle 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* può essere utilizzato nella rete per configurare e gestire più dispositivi Axis in modo economico. AXIS Device Manager è un'applicazione basata su Microsoft Windows® che può essere installata localmente su un computer in rete, mentre AXIS Device Manager Extend si affida all'infrastruttura cloud per eseguire la gestione dei dispositivi multisito. Entrambi offrono funzionalità di gestione e configurazione semplici per i dispositivi Axis come:

- Installazione di aggiornamenti AXIS OS.
- Configurazione della sicurezza informatica come i 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, visitare la versione Web di questo documento.

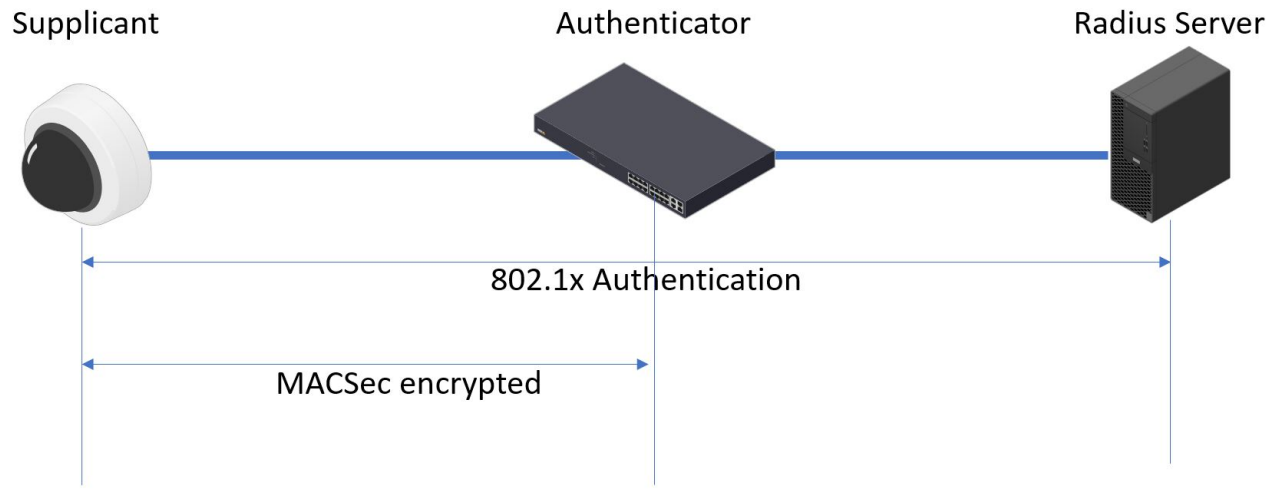
help.axis.com/?&tpiald=&tsection=secure-network-operation-ieee-802-1ae-macsec

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 protegge crittograficamente i collegamenti Ethernet punto a punto sul livello di rete 2. 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 successivi, IEEE 802.1X è abilitato per impostazione predefinita per i dispositivi compatibili con l'ID dispositivo Axis. In AXIS OS 11.8 e versioni successive, supportiamo MACsec con la modalità dinamica automatica utilizzando IEEE 802.1X abilitato per EAP-TLS 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 con IEEE 802.1AR, viene utilizzato per autenticarsi nella rete (4, 5) tramite il controllo degli accessi di rete basati su porta IEEE 802.1X EAP-TLS (2). Attraverso la

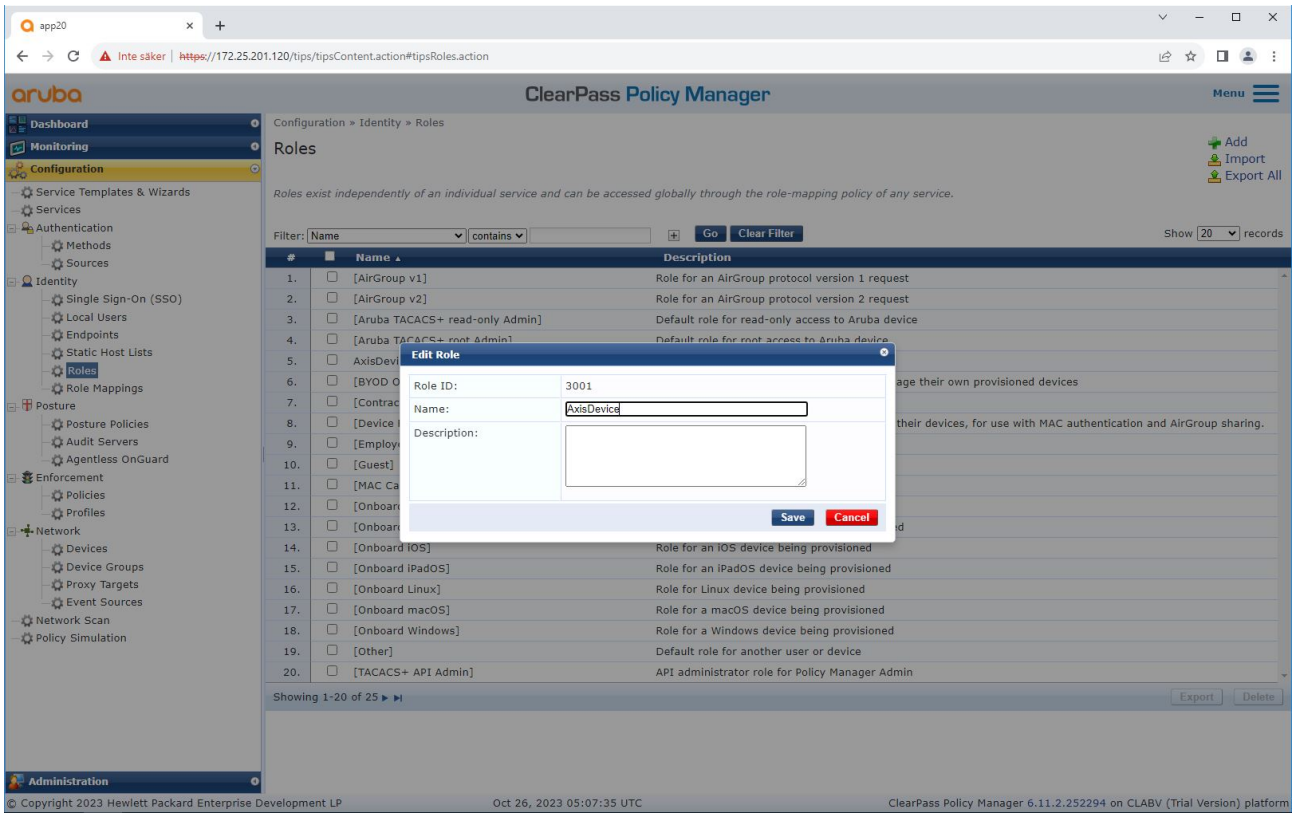
sessione EAP-TLS, le chiavi MACsec vengono scambiate automaticamente per impostare un collegamento sicuro (3), proteggendo tutto il traffico di rete dal dispositivo Axis allo switch di accesso HPE Aruba Networking.

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

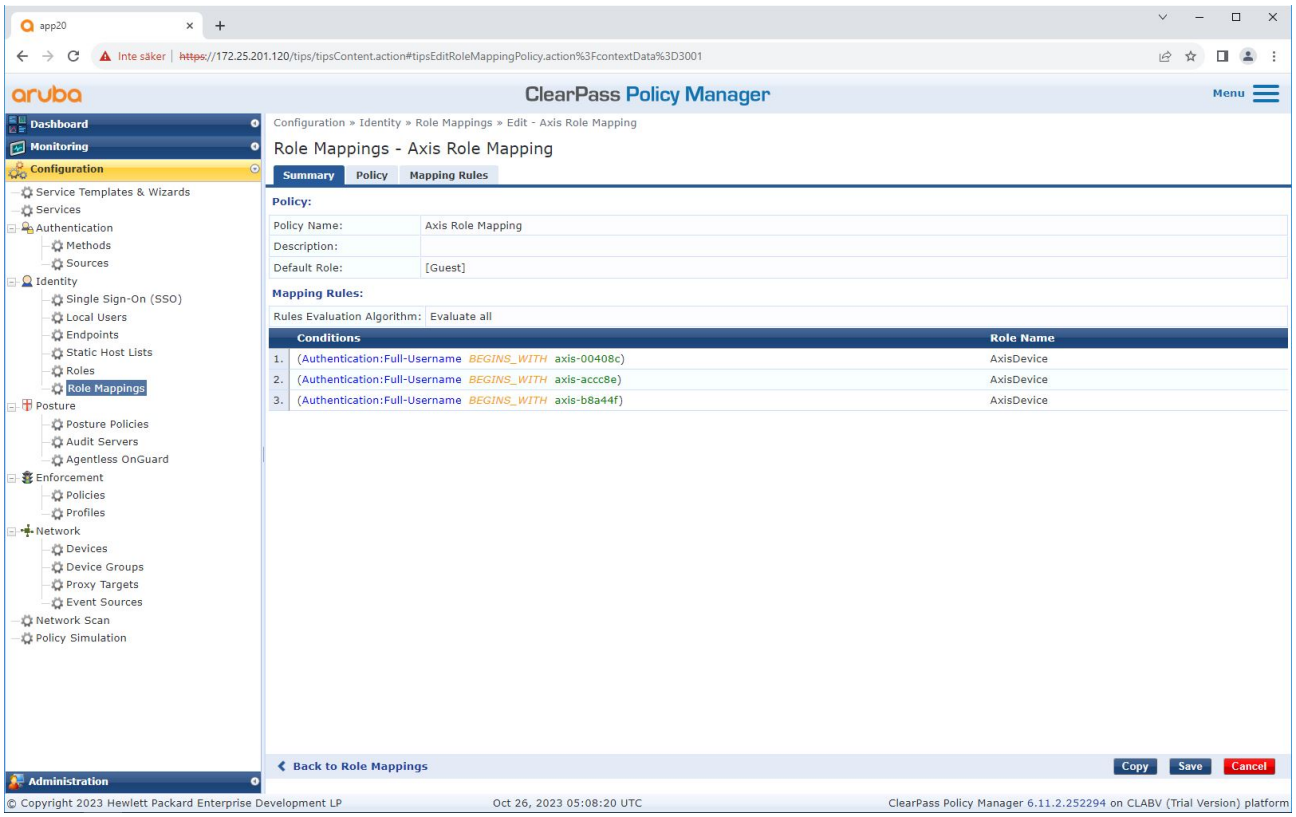
Se lo switch di accesso HPE Aruba Networking non supporta MACsec utilizzando EAP-TLS, è allora possibile utilizzare e configurare manualmente la modalità Pre-Shared Key.

HPE Aruba Networking ClearPass Policy Manager

Ruolo e policy di mappatura del ruolo



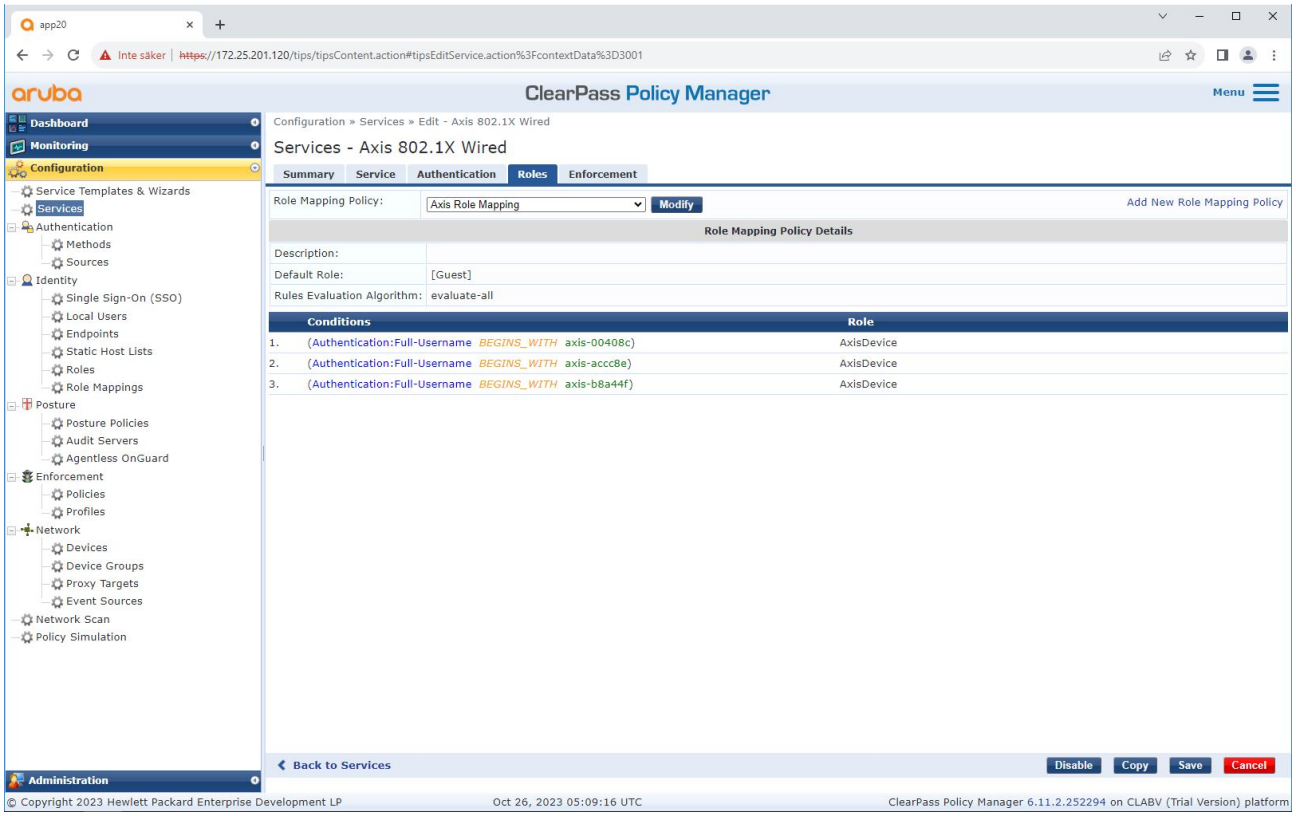
Aggiungere un nome ruolo per i dispositivi Axis. Il nome è quello del ruolo di accesso alla porta nella configurazione dello switch di accesso.



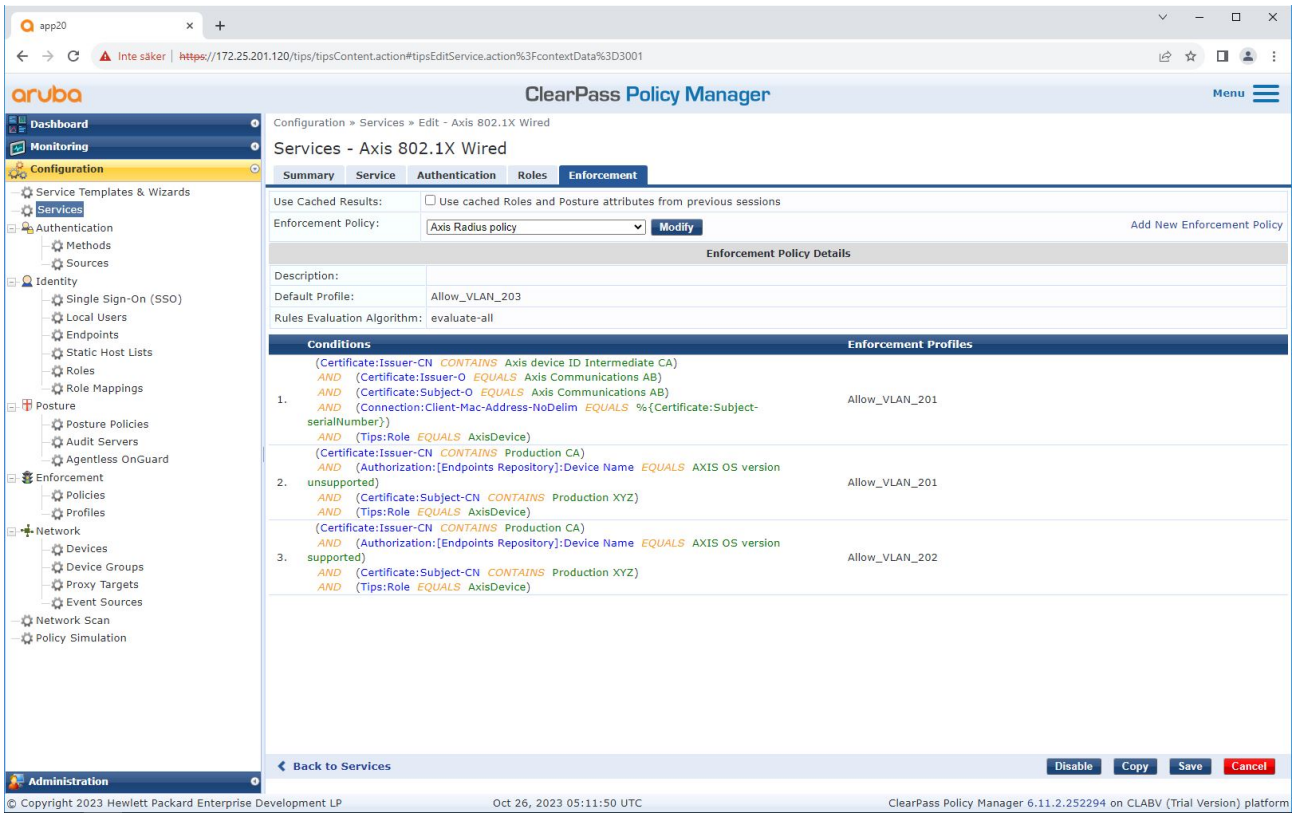
Aggiungere una policy di mappatura dei ruoli Axis per il ruolo del dispositivo Axis creato in precedenza. Le condizioni definite sono necessarie affinché un dispositivo venga mappato al ruolo del dispositivo Axis. Se le condizioni non sono soddisfatte, il dispositivo diventa parte del ruolo [Guest].

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

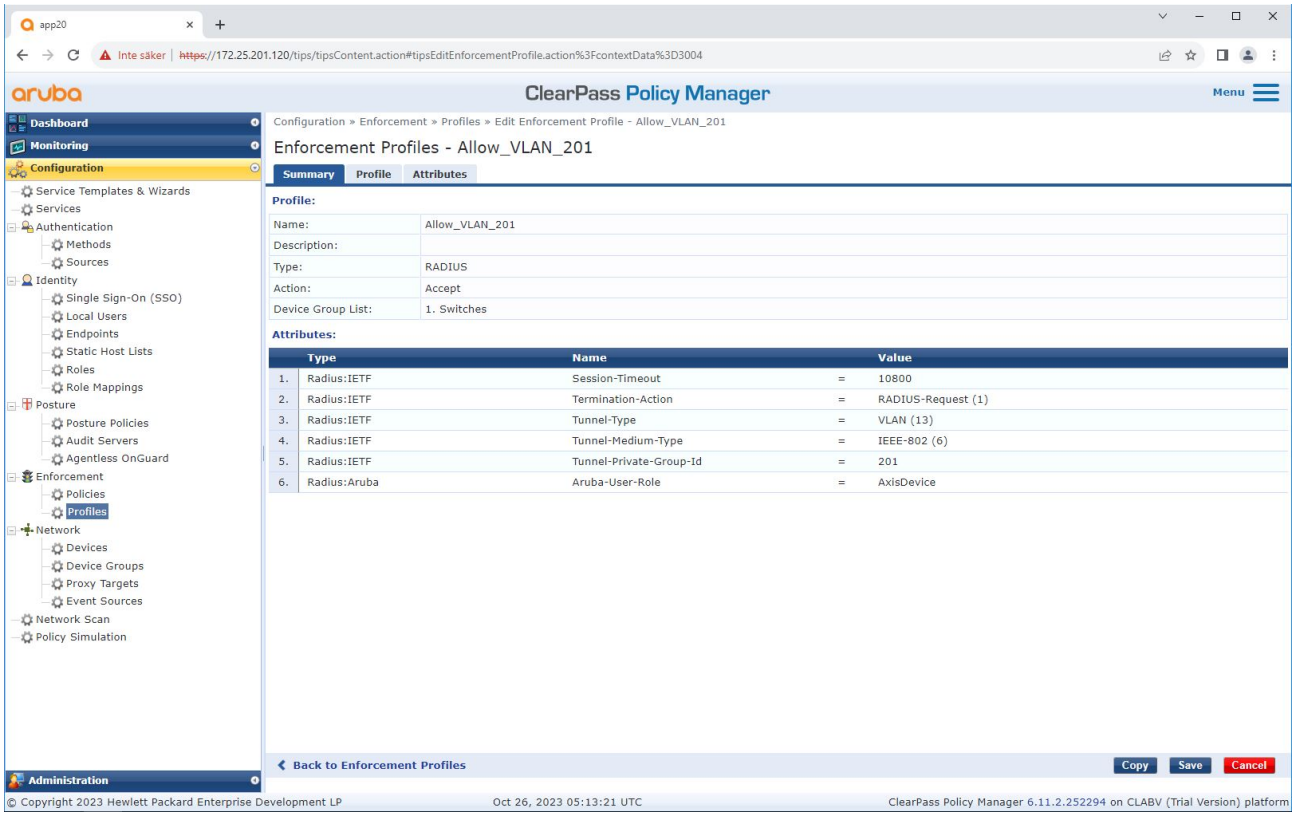


Aggiungere la policy di mappatura dei ruoli Axis creata in precedenza al servizio che definisce IEEE 802.1X come metodo di connessione per l'onboarding dei dispositivi Axis.



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

Profilo esecutivo



Aggiungere il nome del ruolo Axis come 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 alla pagina 16*, fare riferimento all'esempio di configurazione della porta riportato di seguito affinché lo switch di accesso HPE Aruba Networking configuri IEEE 802.1AE MACsec.

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

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

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

Onboarding legacy: autenticazione MAC

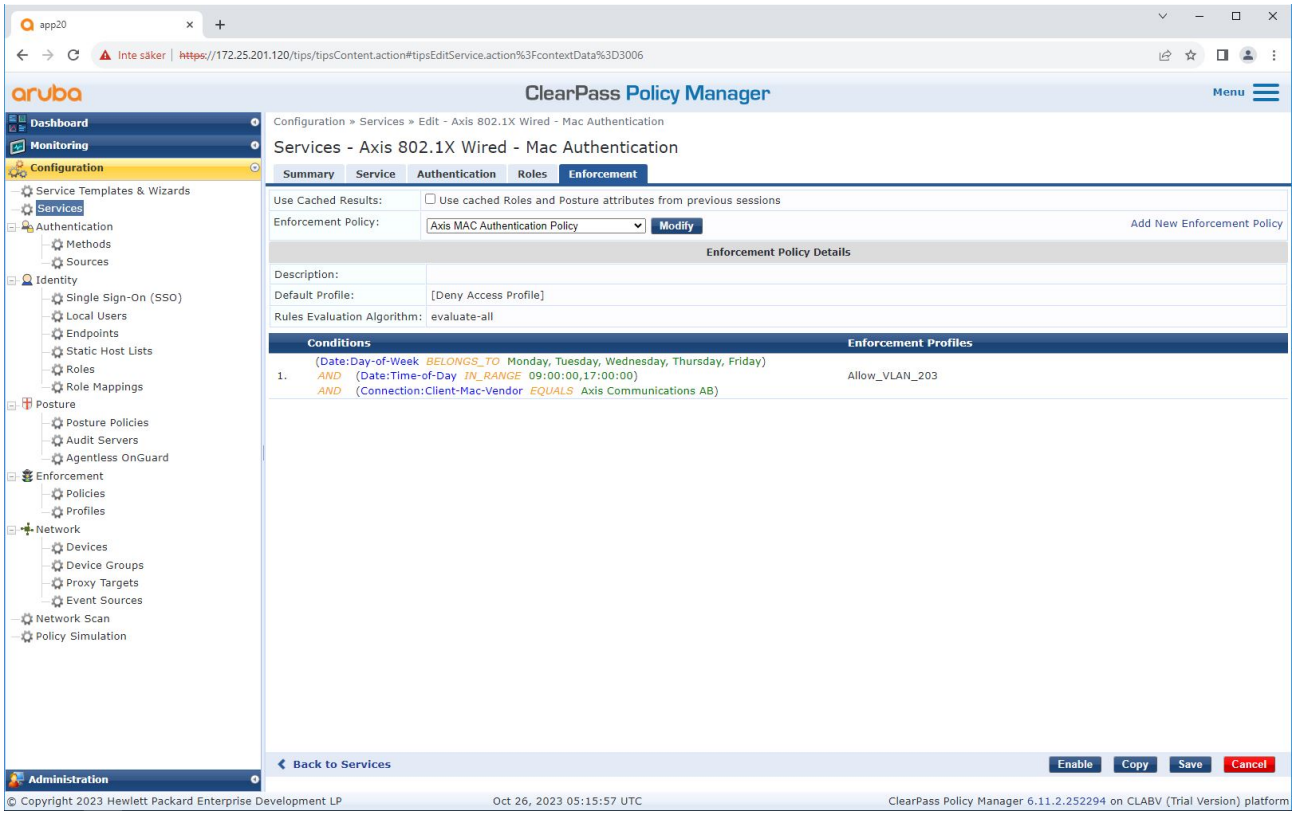
È possibile utilizzare MAC Authentication Bypass (MAB) per integrare dispositivi Axis che non supportano l'onboarding di IEEE 802.1AR con il certificato ID dispositivo Axis e IEEE 802.1X abilitato nello stato predefinito di fabbrica. Se l'onboarding 802.1X fallisce, ClearPass Policy Manager convalida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

MAB richiede sia la preparazione dello switch di accesso che della configurazione di ClearPass Policy Manager. Sul dispositivo Axis non è necessaria alcuna configurazione per consentire l'onboarding di MAB.

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

Quando 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:

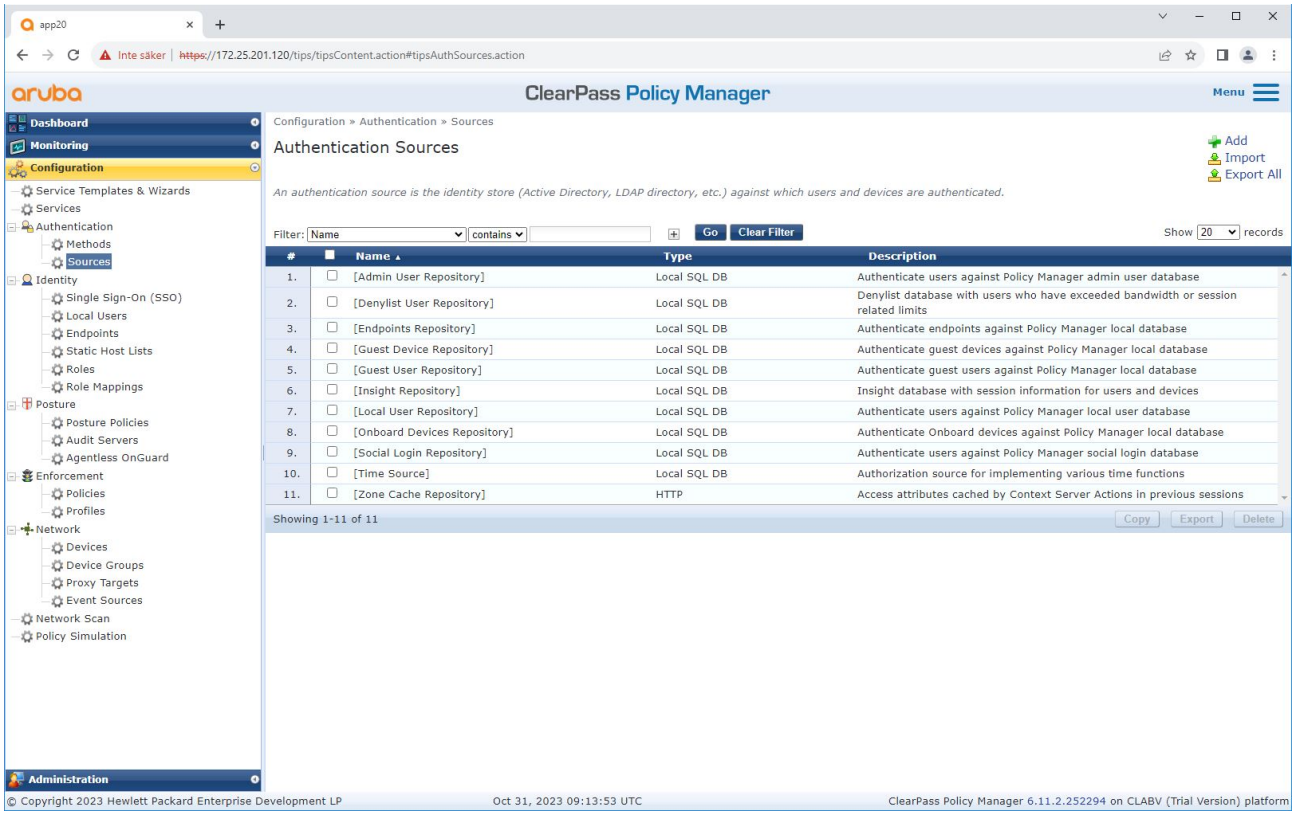
- È un giorno feriale tra lunedì e venerdì
- È un'ora compresa tra le 09:00 e le 17:00

- Il fornitore del MAC address corrisponde ad Axis Communications.

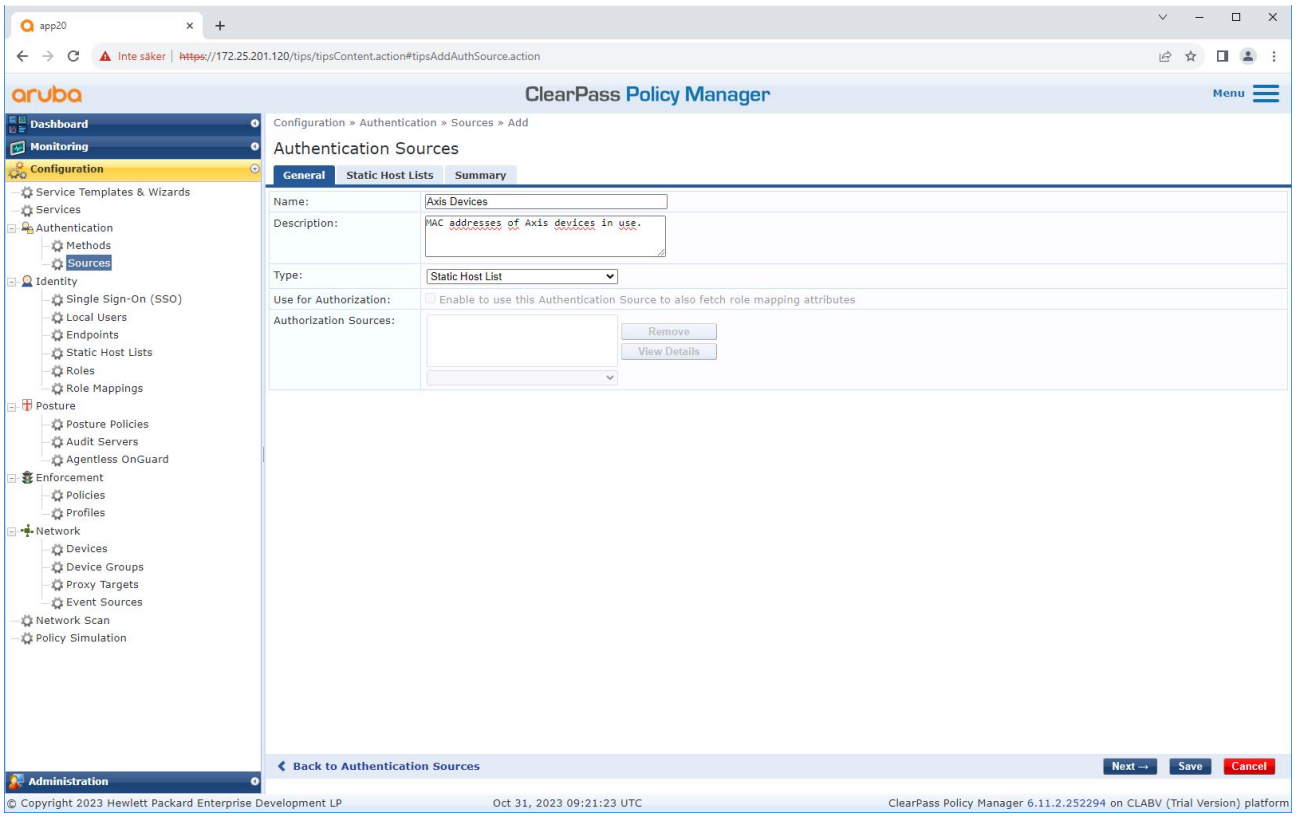
Poiché i MAC address possono essere falsificati, non viene concesso l'accesso alla normale rete di provisioning. Ti consigliamo di utilizzare MAB solo per l'onboarding iniziale e di ispezionare ulteriormente manualmente il dispositivo.

Configurazione di origine

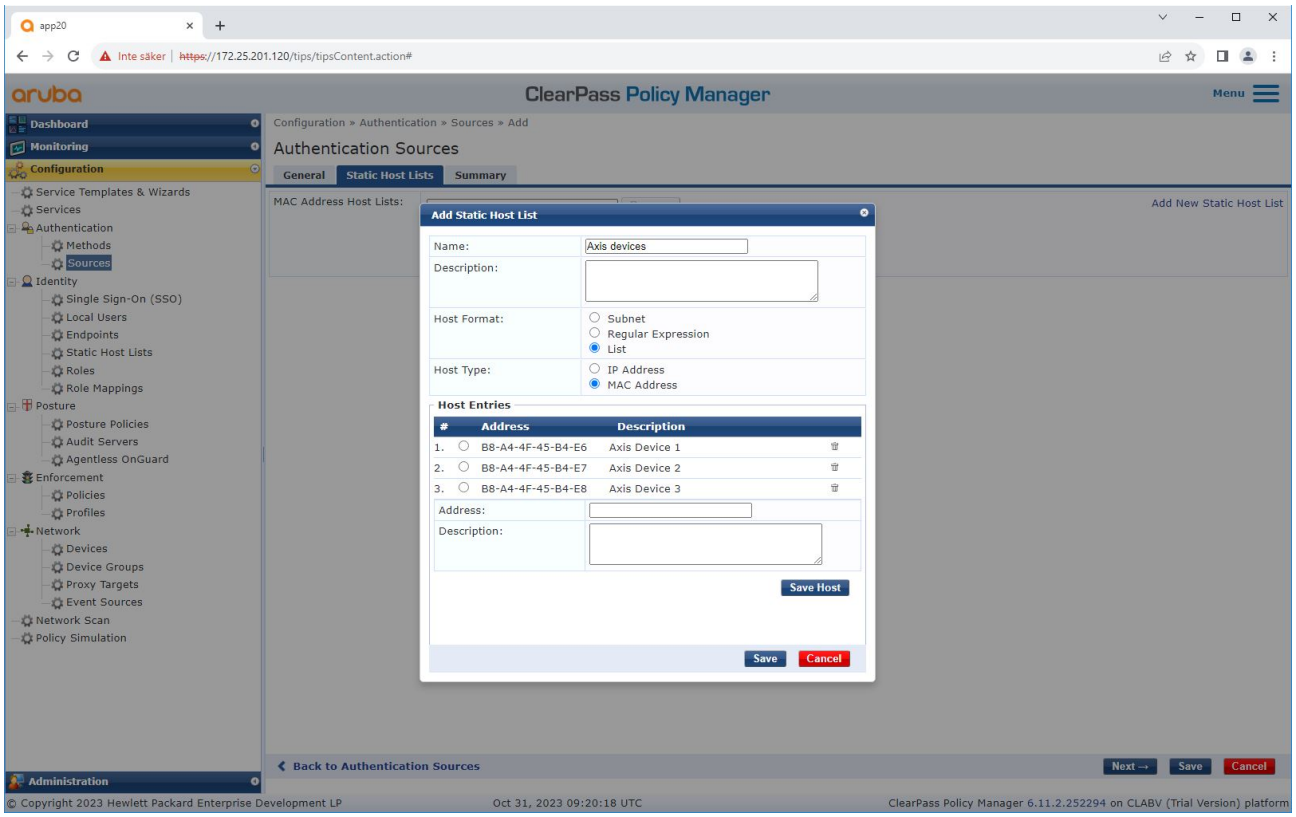
Nella pagina **Sources (Origini)** viene creata una nuova origine di autenticazione per consentire solo MAC address importati manualmente.



Onboarding legacy: autenticazione MAC

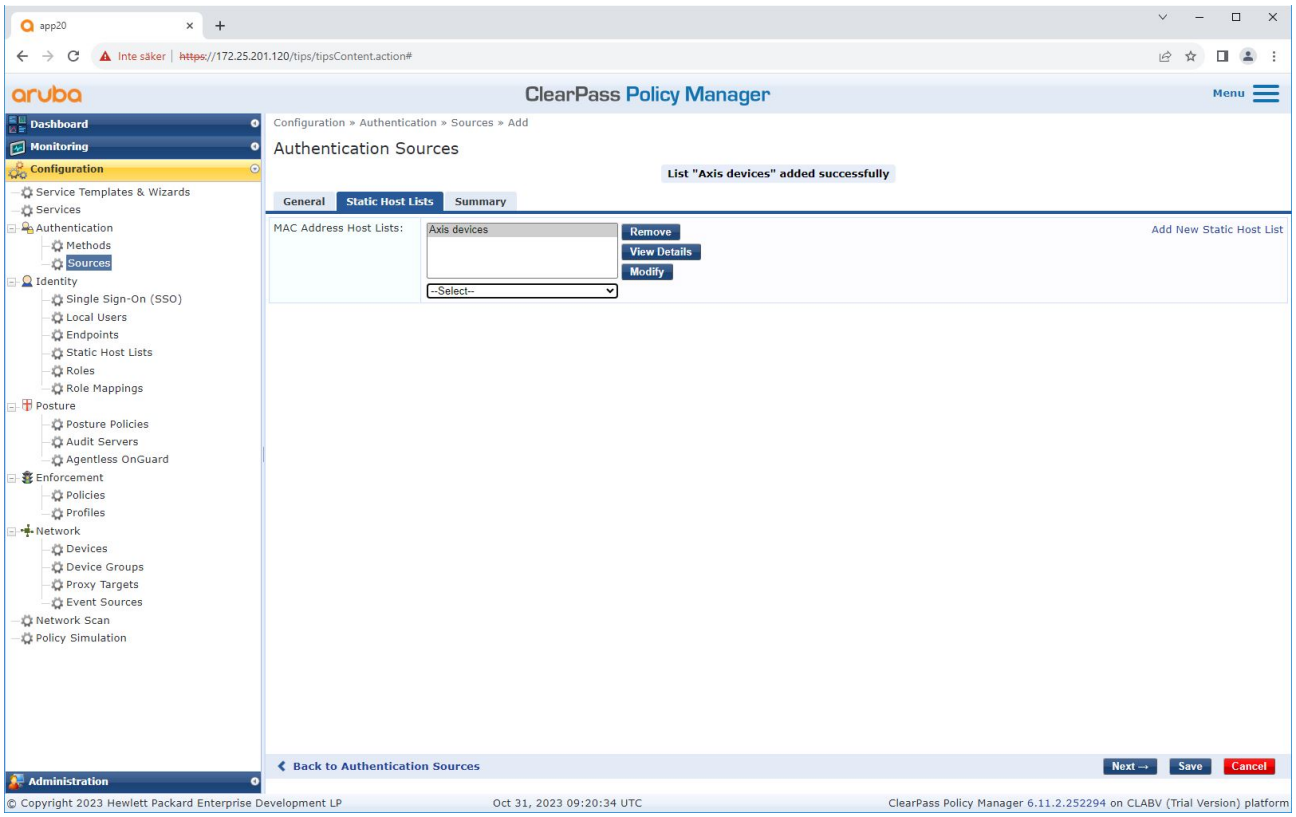


Onboarding legacy: autenticazione MAC



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

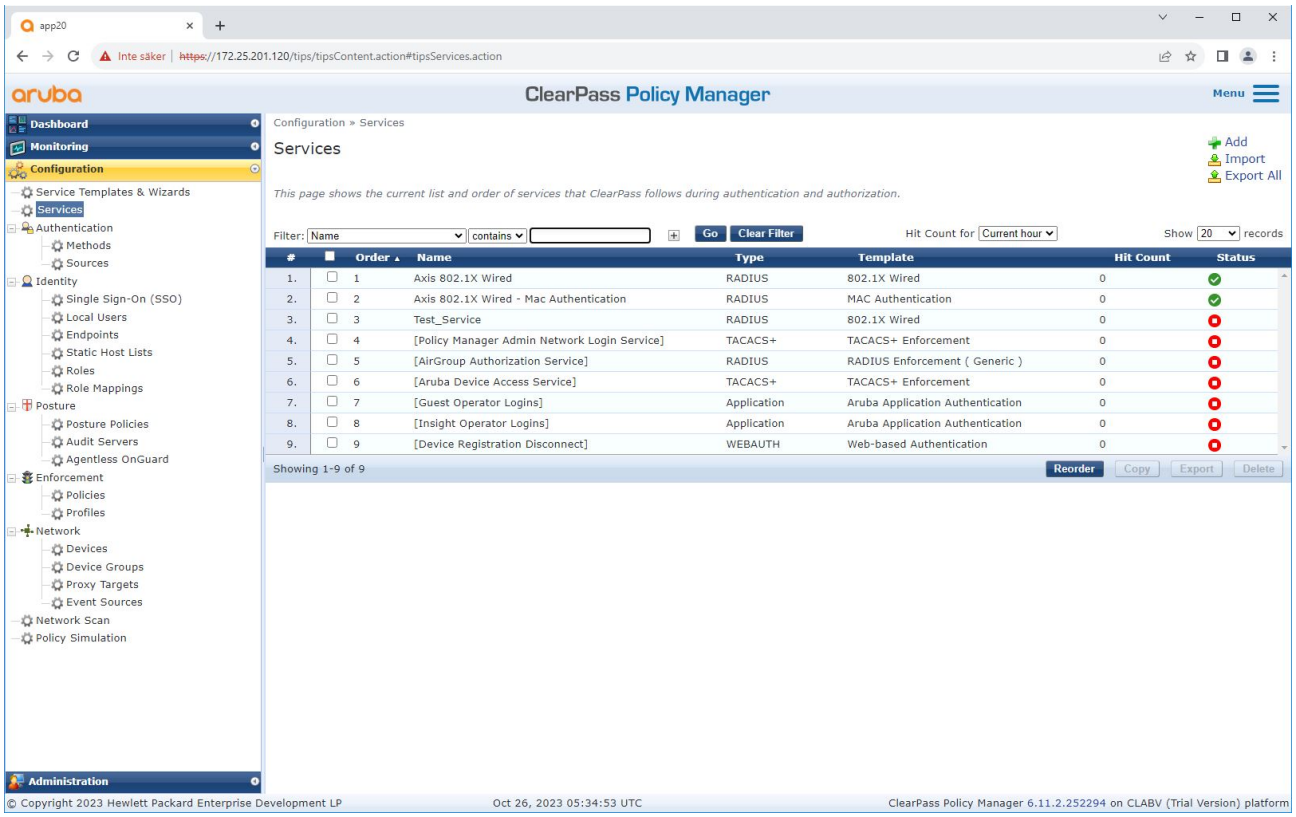
Onboarding legacy: autenticazione MAC



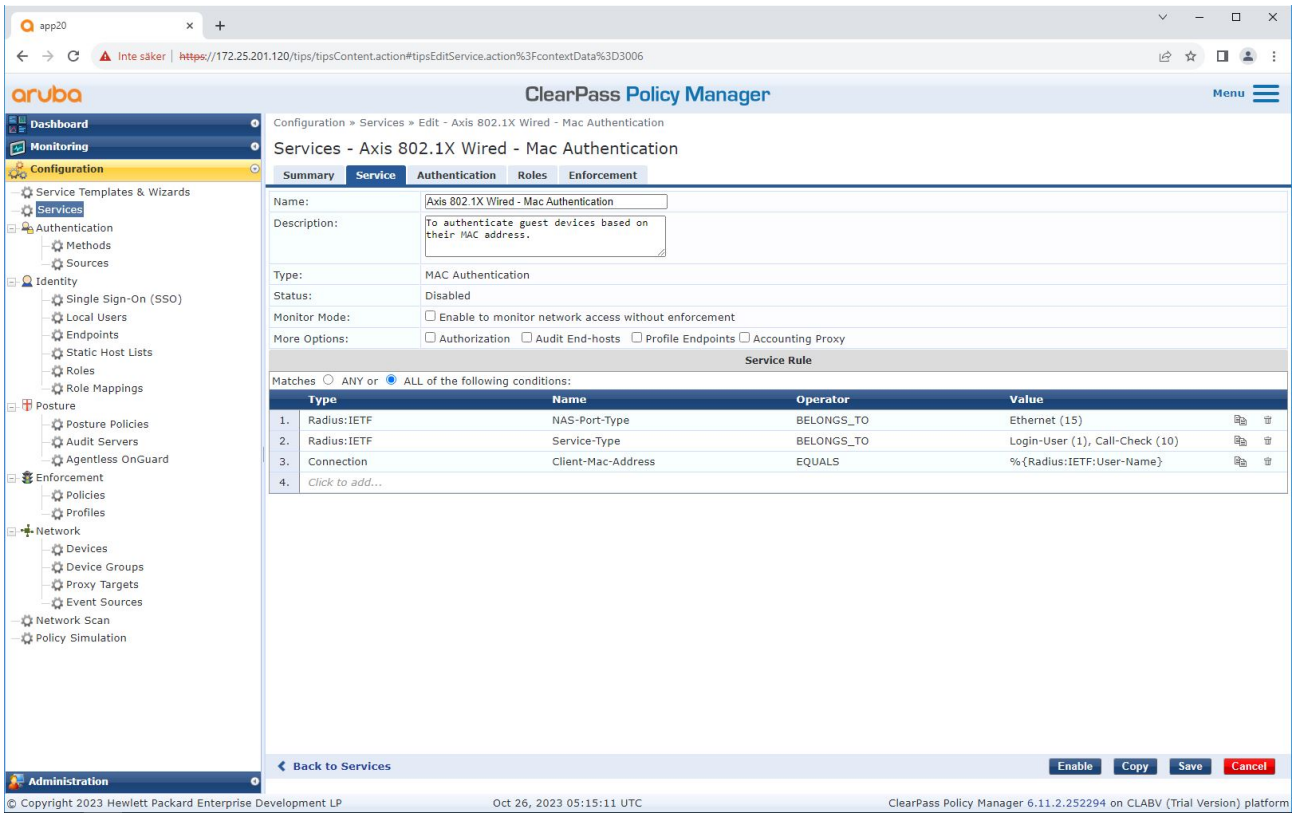
Configurazione del servizio

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

Onboarding legacy: autenticazione MAC

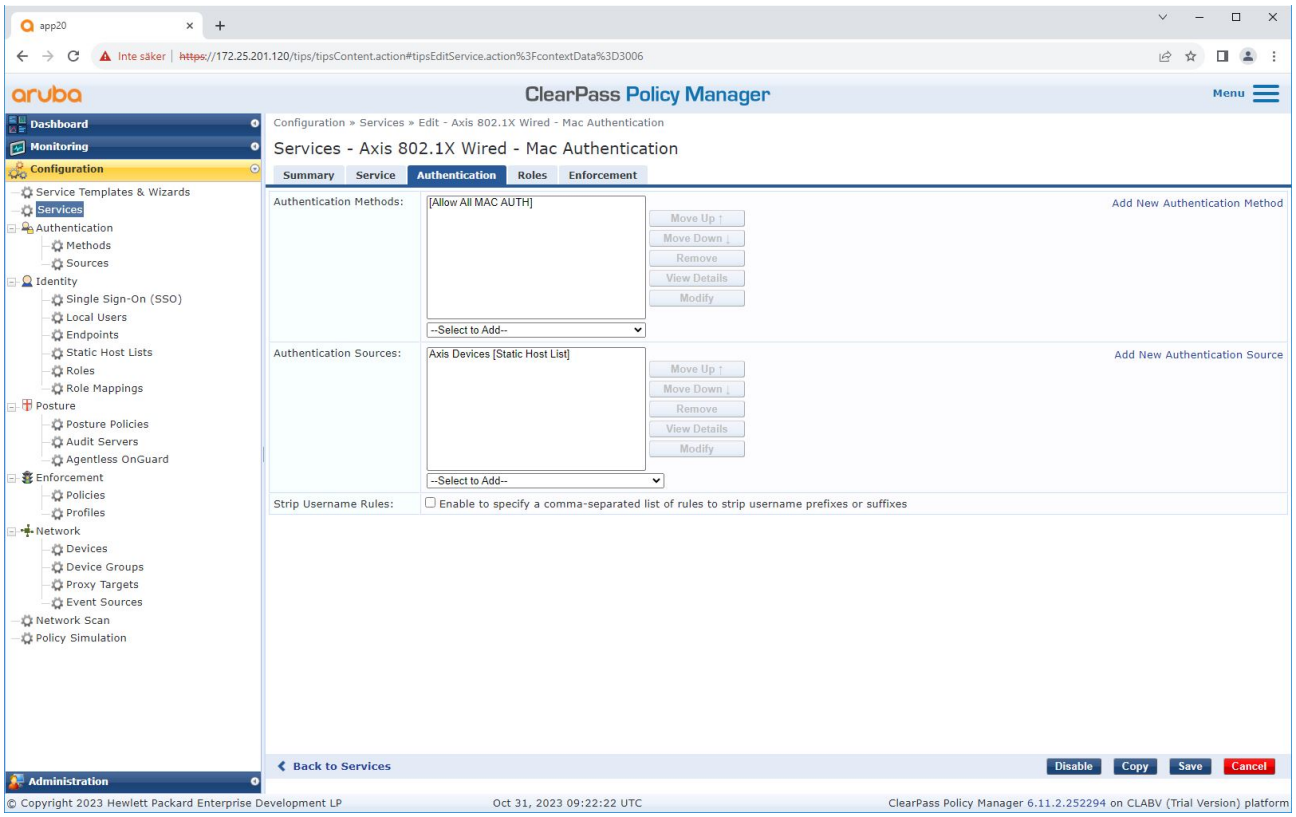


Onboarding legacy: autenticazione MAC



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

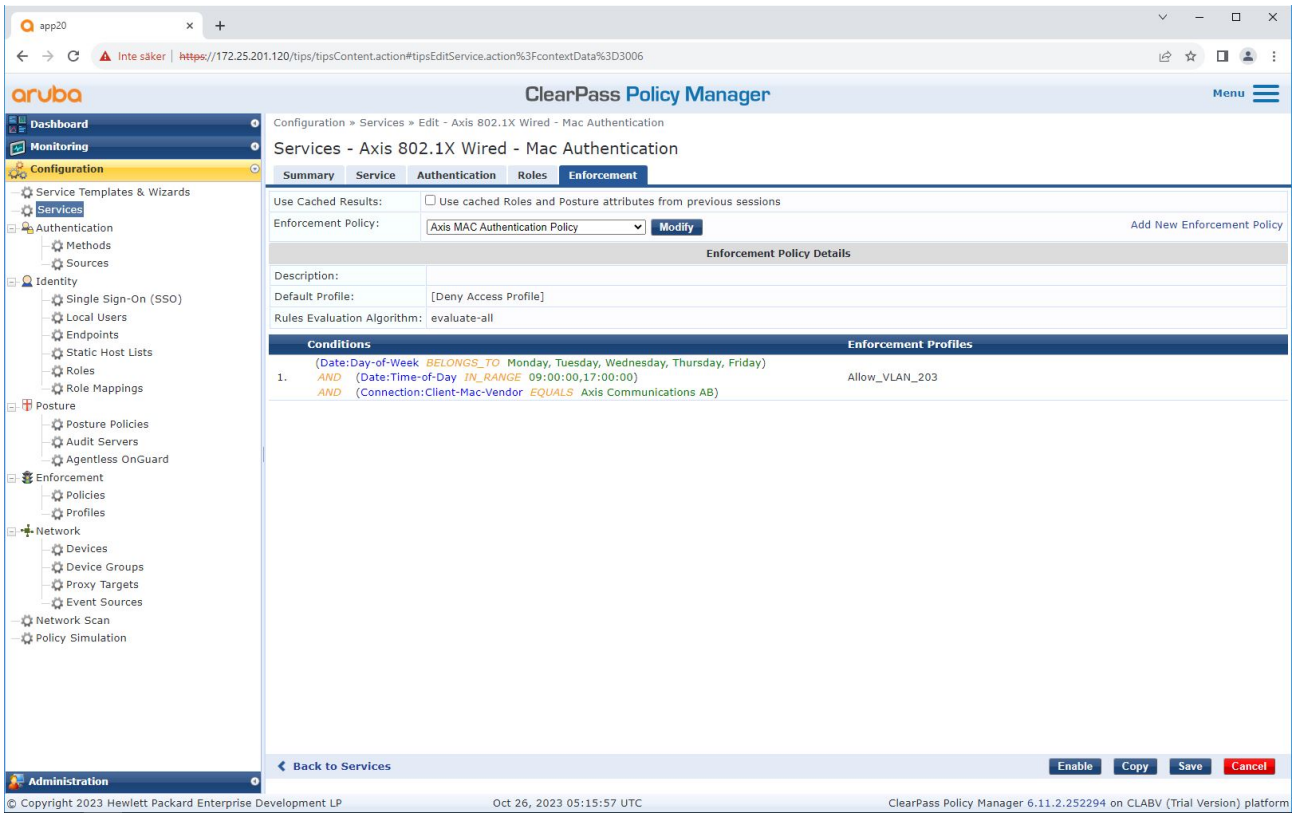
Onboarding legacy: autenticazione MAC



Il metodo di autenticazione MAC preconfigurato viene configurato nel servizio. Inoltre, viene selezionata l'origine di autenticazione creata in precedenza che contiene 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, la policy di applicazione creata in precedenza viene configurata per il servizio.

Switch di accesso HPE Aruba Networking

Oltre alla configurazione di onboarding sicura descritta in *Switch di accesso HPE Aruba Networking alla pagina 16*, fare riferimento all'esempio di configurazione della porta riportato di seguito per lo switch di accesso HPE Aruba Networking da consentire per MAB.

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

Guida all'integrazione
HPE Aruba Networking

Ver. M6.2
Data: Maggio 2024
Codice art. T10197992