

HPE Aruba Networking

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
Onboarding legacy: autenticazione MAC.....	23
HPE Aruba Networking ClearPass Policy Manager	23
Politica di applicazione	23
Configurazione di origine	24
Configurazione del servizio.....	25
Switch di accesso HPE Aruba Networking	28

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



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

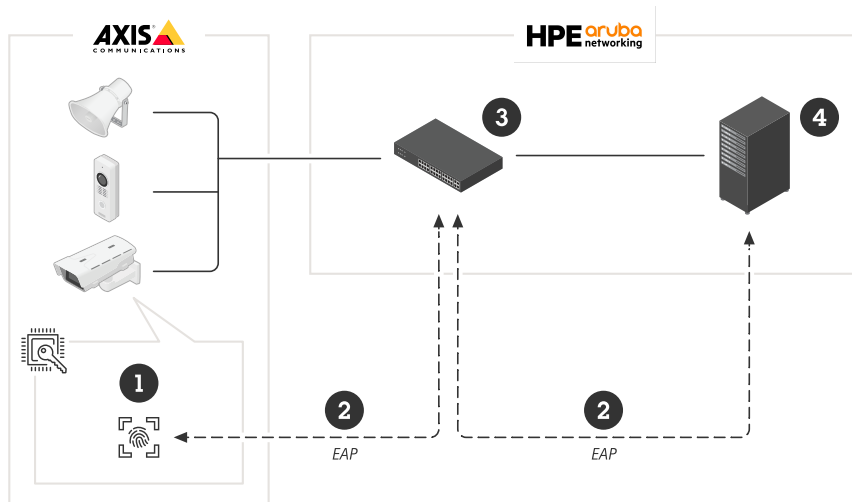
Onboarding sicuro dei dispositivi su reti non attendibili con IEEE 802.1X/802.1AR

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 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.

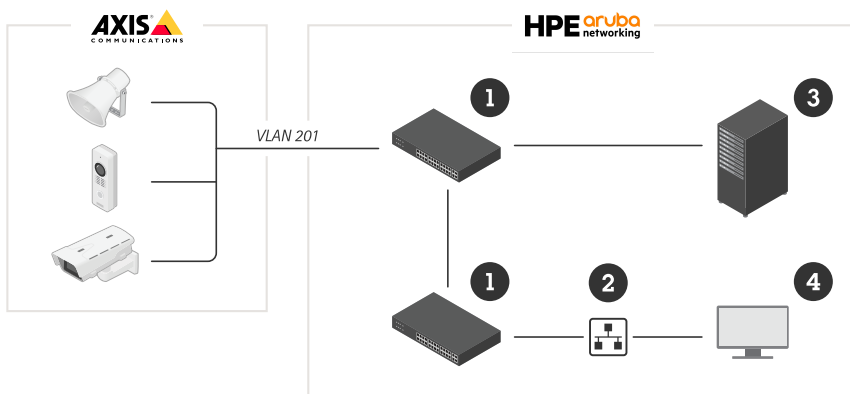


Il dispositivo Axis esegue l'autenticazione sulla rete di HPE Aruba Networking utilizzando il certificato ID dispositivo Axis conforme a IEEE 802.1AR.

- 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. Per completare il provisioning, sul dispositivo vengono caricati nuovi certificati di livello produttivo specifici del cliente per IEEE 802.1X e HTTPS.

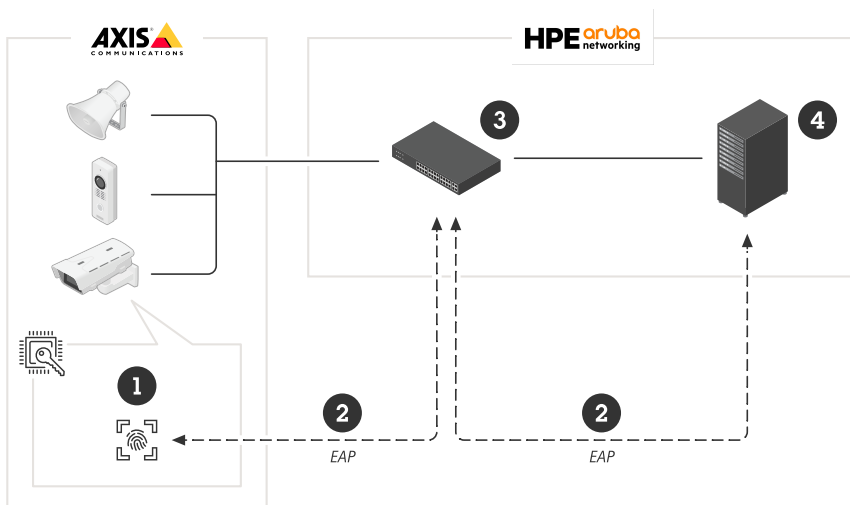


Dopo l'autenticazione, il dispositivo Axis passa a una rete di provisioning per la configurazione.

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

Rete di produzione

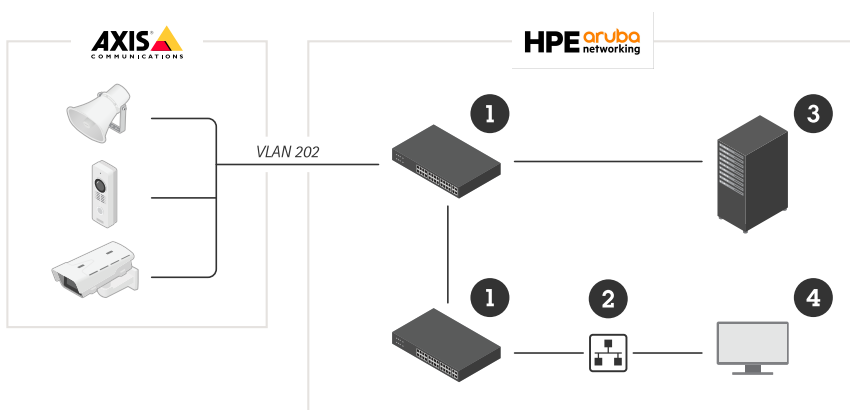
Il provisioning del dispositivo Axis con nuovi certificati IEEE 802.1X attiva un nuovo tentativo di autenticazione. ClearPass Policy Manager verifica i nuovi certificati e decide se spostare o meno il dispositivo Axis nella rete di produzione.



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.

The screenshot shows the ClearPass Policy Manager web interface. The left sidebar contains navigation links: Dashboard, Monitoring, Configuration, and Administration. The main content area is titled 'Certificate Trust List' and displays a table of trusted Certificate Authorities (CA). A dialog box titled 'Add Certificate' is open, showing the 'Certificate File' field with the value 'Axis_device_ID_Int...e_CA_ECC_1.pem' and the 'Usage' field with the value 'EAP'. The dialog also includes a 'Remove' button and an 'Add Certificate' button.

#	Subject	Usage	Validity	Enabled
1.	OU=VeriSign Trust Network,OU=(c) 1998 VeriSign, Inc. - For authorized use only,OU=Class 3 Public Primary Certification Authority - G2,O=VeriSign, Inc.,C=US	Others	Valid	Disabled
2.	OU=Go	AD/LDAP Servers, Endpoint Context Servers, SAML, SMTP, Others	Valid	Enabled
3.	OU=Class	Others	Valid	Disabled
4.	emailAd...	EAP, Others	Valid	Enabled
5.	emailAd...	EAP, Others	Valid	Enabled
6.	C=US,S...	Others	Valid	Disabled
7.	C=US,S...	Others	Valid	Disabled
8.	C=US,S...	Aruba Infrastructure	Valid	Disabled
9.	CN=Wired Phones,OU=PKI Authority,O=Alcatel-Lucent,C=FR	Others	Valid	Disabled
10.	CN=VeriSign Class 3 Public Primary Certification Authority - G5,OU=(c) 2006 VeriSign, Inc. - For authorized use only,OU=VeriSign Trust Network,O=VeriSign, Inc.,C=US	Others	Valid	Disabled
11.	CN=VeriSign Class 3 Public Primary Certification Authority - G3,OU=(c) 1999 VeriSign, Inc. - For authorized use only,OU=VeriSign Trust Network,O=VeriSign, Inc.,C=US	Others	Valid	Disabled
12.	CN=VeriSign Class 1 Public Primary Certification Authority - G3,OU=(c) 1999 VeriSign, Inc. - For authorized use only,OU=VeriSign Trust Network,O=VeriSign, Inc.,C=US	AD/LDAP Servers, Endpoint Context Servers, SAML, SMTP, Others	Valid	Enabled
13.	CN=USERTrust RSA Certification Authority,O=The USERTRUST Network,L=Jersey City,ST=New Jersey,C=US	EAP, Others	Valid	Disabled
14.	CN=thawte Primary Root CA,OU=(c) 2006 thawte, Inc. - For authorized use only,OU=Certification Services Division,O=thawte, Inc.,C=US	Others	Valid	Disabled
15.	CN=TC TrustCenter Universal CA 1,OU=TC TrustCenter Universal CA,O=TC TrustCenter GmbH,C=DE	Others	Valid	Disabled

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

ClearPass Policy Manager - Aruba

Administration » Certificates » Trust List

Certificate Trust List

This page displays a list of trusted Certificate Authorities (CA). You can add, view, or delete a certificate.

Filter: Subject | contains | axis device | Go | Clear Filter

Show 20 records

#	Subject	Usage	Validity	Enabled
1.	CN=Axis device ID Root CA RSA,O=Axis Communications AB	EAP	Valid	Enabled
2.	CN=Axis device ID Root CA ECC,O=Axis Communications AB	EAP	Valid	Enabled
3.	CN=Axis device ID Intermediate CA RSA 2,O=Axis Communications AB	EAP	Valid	Enabled
4.	CN=Axis device ID Intermediate CA RSA 1,O=Axis Communications AB	EAP	Valid	Enabled
5.	CN=Axis device ID Intermediate CA ECC 2,O=Axis Communications AB	EAP	Valid	Enabled
6.	CN=Axis device ID Intermediate CA ECC 1,O=Axis Communications AB	EAP	Valid	Enabled

Showing 1-6 of 6

Copyright 2022 Hewlett Packard Enterprise Development LP Nov 25, 2022 08:48:50 CET ClearPass Policy Manager 6.9.12.136929 on CLABV (Trial Version) platform

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.

ClearPass Policy Manager - Aruba

Configuration » Network » Devices

Network Devices

A Network Access Device (NAD) must belong to the global list of devices in the ClearPass database in order to connect to ClearPass.

Filter: Name | contains | | Go | Clear Filter

Show 20 records

#	Name	IP or Subnet Address	Device Groups	Description
---	------	----------------------	---------------	-------------

Copy Export Delete

Copyright 2022 Hewlett Packard Enterprise Development LP Dec 28, 2022 09:01:17 CET ClearPass Policy Manager 6.9.12.136929 on CLABV (Trial Version) platform

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

ClearPass Policy Manager - Aruba

Configuration » Network » Devices

Network Devices

Add Device

Device | SNMP Read Settings | SNMP Write Settings | CLI Settings | OnConnect Enforcement | Attributes

Name: SW04

IP or Subnet Address: 172.25.200.13
(e.g., 192.168.1.10 or 192.168.1.1/24 or 2001:db8:a0b:12f0::1 or 2001:db8:a0b:12f0::1/64)

Description:

RADIUS Shared Secret: [password field] Verify: [password field]

TACACS+ Shared Secret: [password field] Verify: [password field]

Vendor Name: Aruba

Enable RADIUS Dynamic Authorization: ☐

Enable RadSec: ☐

Add Cancel

Copyright 2022 Hewlett Packard Enterprise Development LP Dec 28, 2022 09:02:18 CET ClearPass Policy Manager 6.9.12.136929 on CLABV (Trial Version) platform

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 - Aruba

Configuration » Network » Devices

Network Devices

Device SW04 added

A Network Access Device (NAD) must belong to the global list of devices in the ClearPass database in order to connect to ClearPass.

Filter: Name contains [] Go Clear Filter

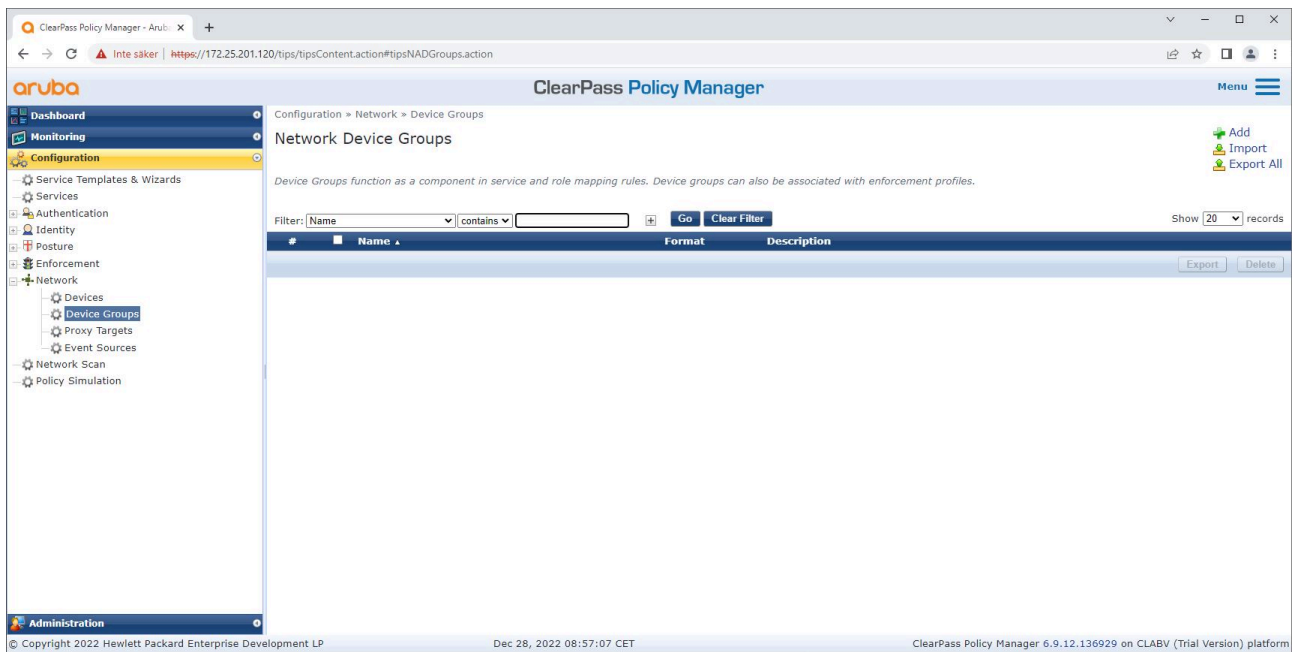
#	Name	IP or Subnet Address	Device Groups	Description
1.	SW04	172.25.200.13	-	

Showing 1-1 of 1

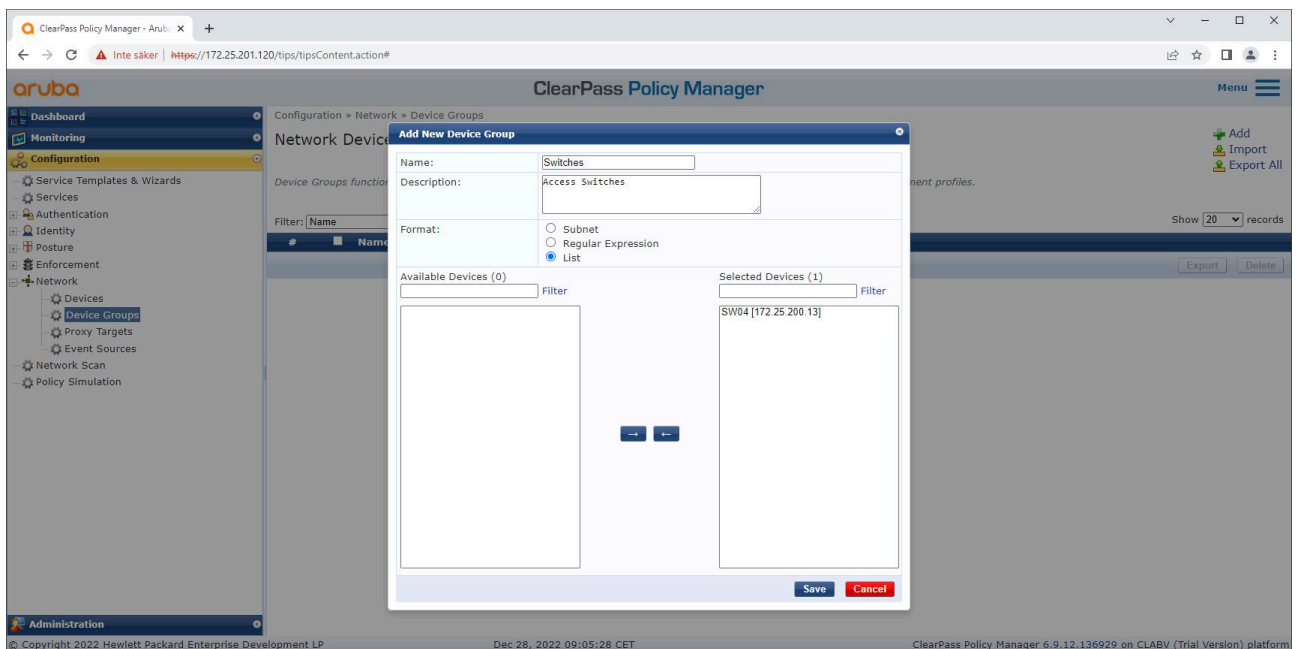
Copy Export Delete

Copyright 2022 Hewlett Packard Enterprise Development LP Dec 28, 2022 09:02:33 CET ClearPass Policy Manager 6.9.12.136929 on CLABV (Trial Version) platform

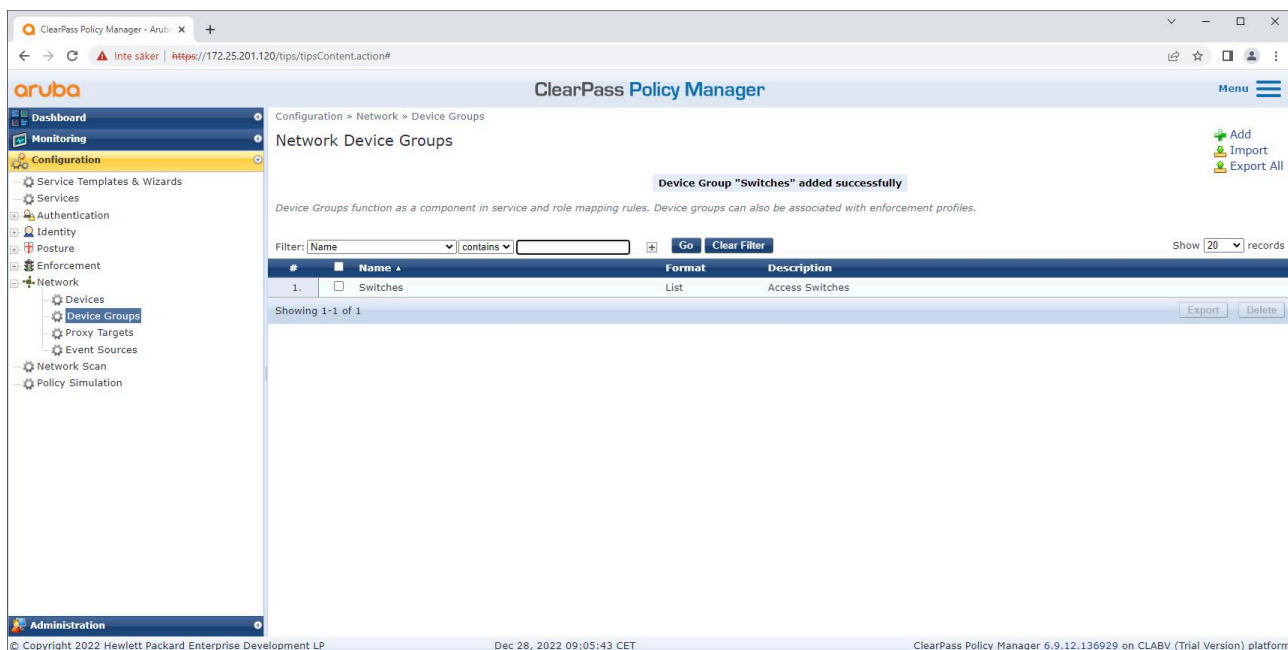
ClearPass Policy Manager con un singolo dispositivo di rete affidabile configurato.



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.

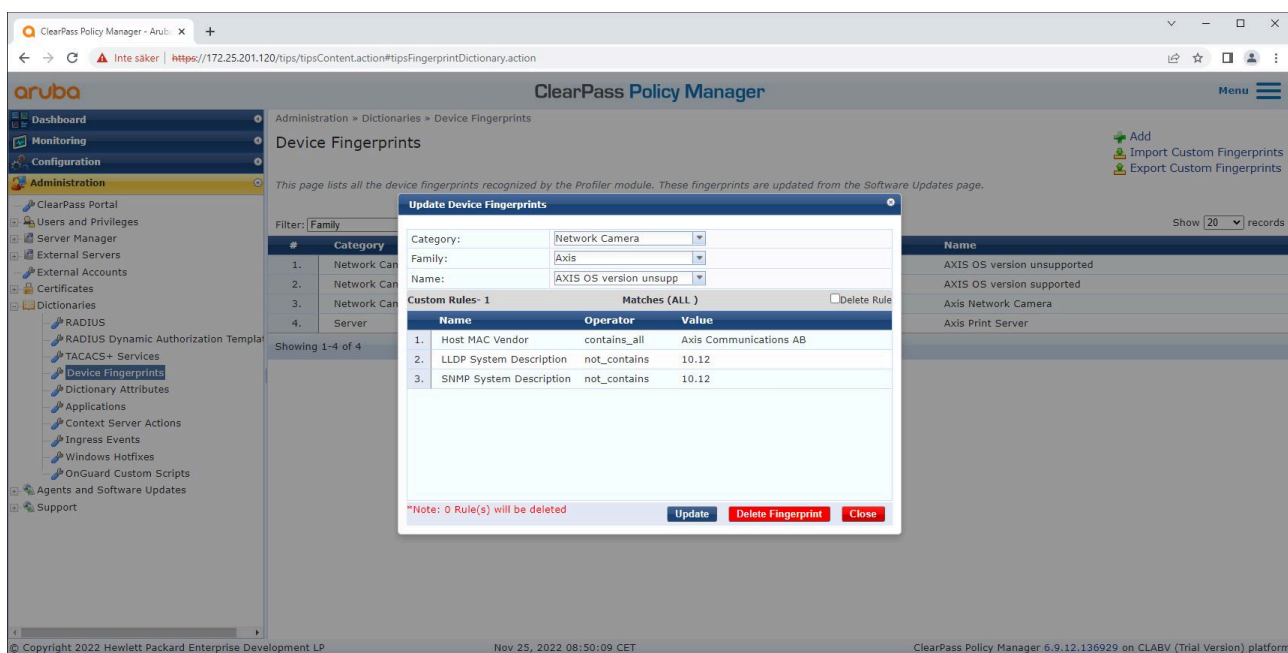


ClearPass Policy Manager con un gruppo di dispositivi di rete configurato che include uno o più dispositivi di rete attendibili.

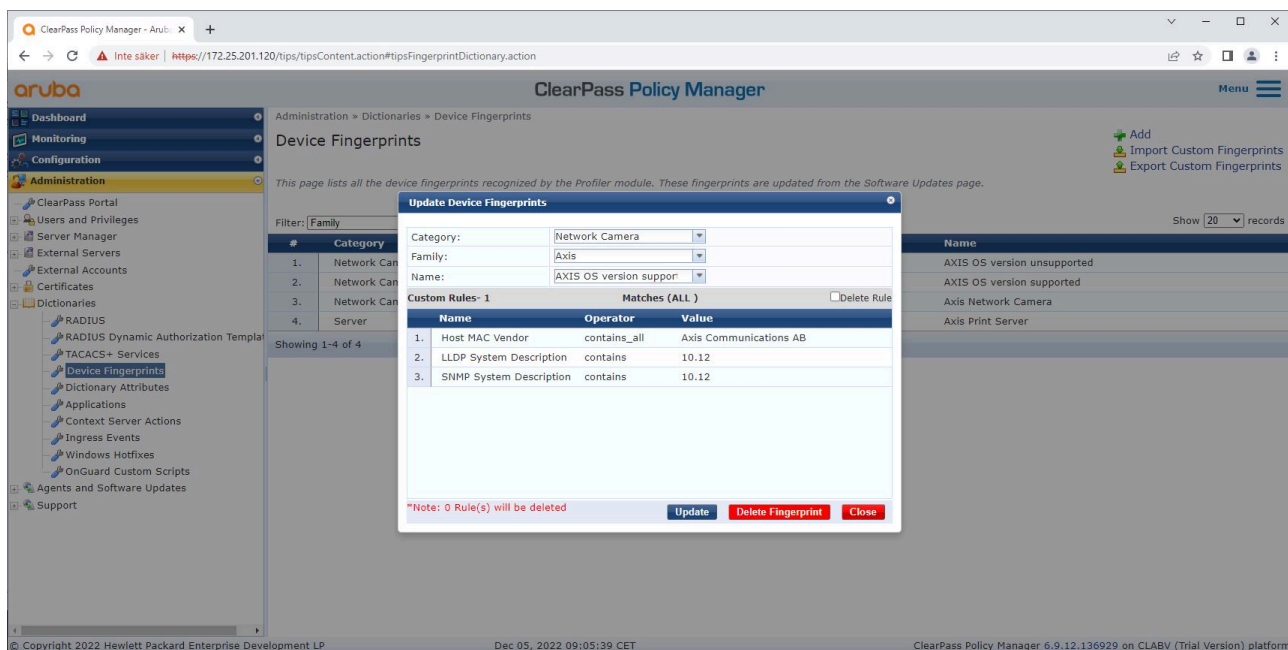
Configurazione dell'impronta digitale del dispositivo

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.



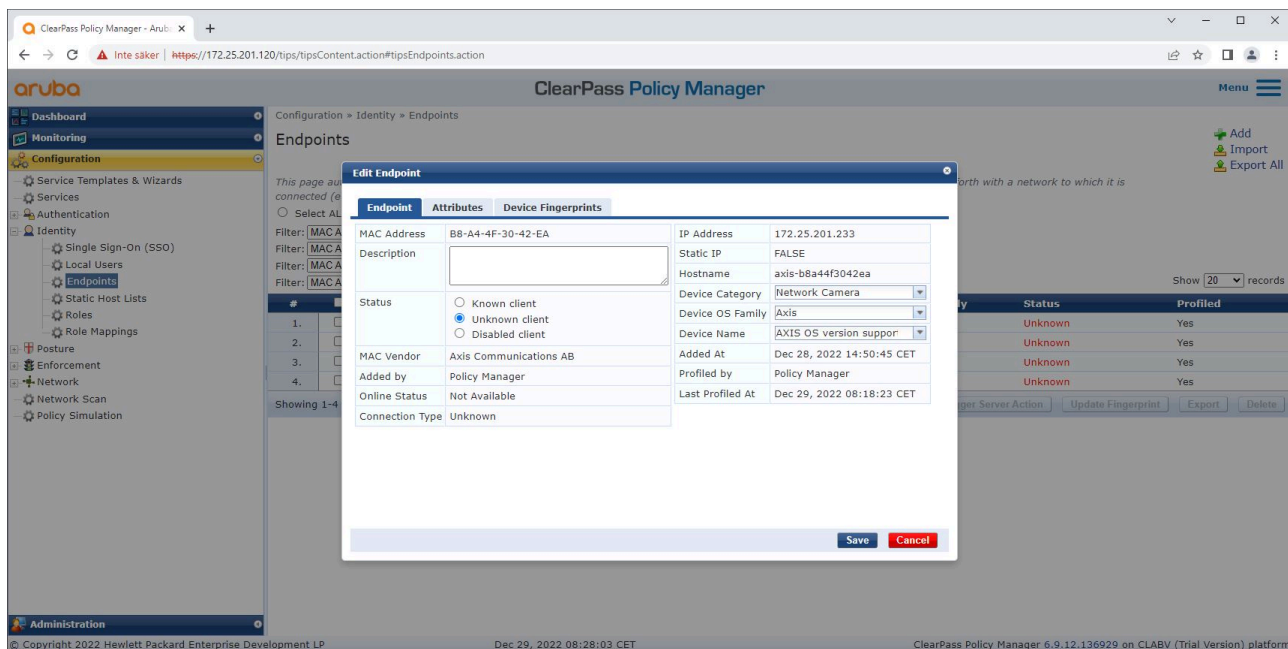
La configurazione dell'impronta digitale del dispositivo in ClearPass Policy Manager. I dispositivi Axis che utilizzano versioni di AXIS OS diverse dalla 10.12 sono contemplati in questo esempio.

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

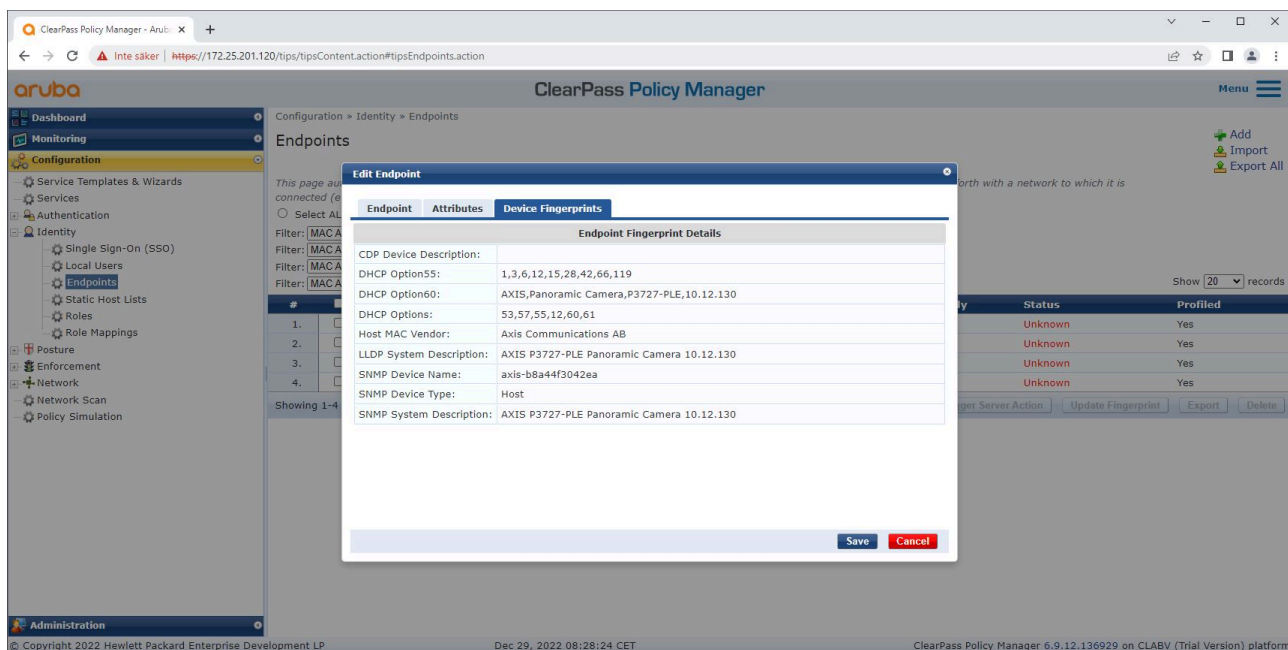
1. Andare a Configuration > Identity > Endpoints (Configurazione > Identità > Endpoint).
2. Selezionare il dispositivo che desideri visualizzare.
3. Fare clic sulla scheda Device Fingerprints (Impronte digitali) del dispositivo.

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.

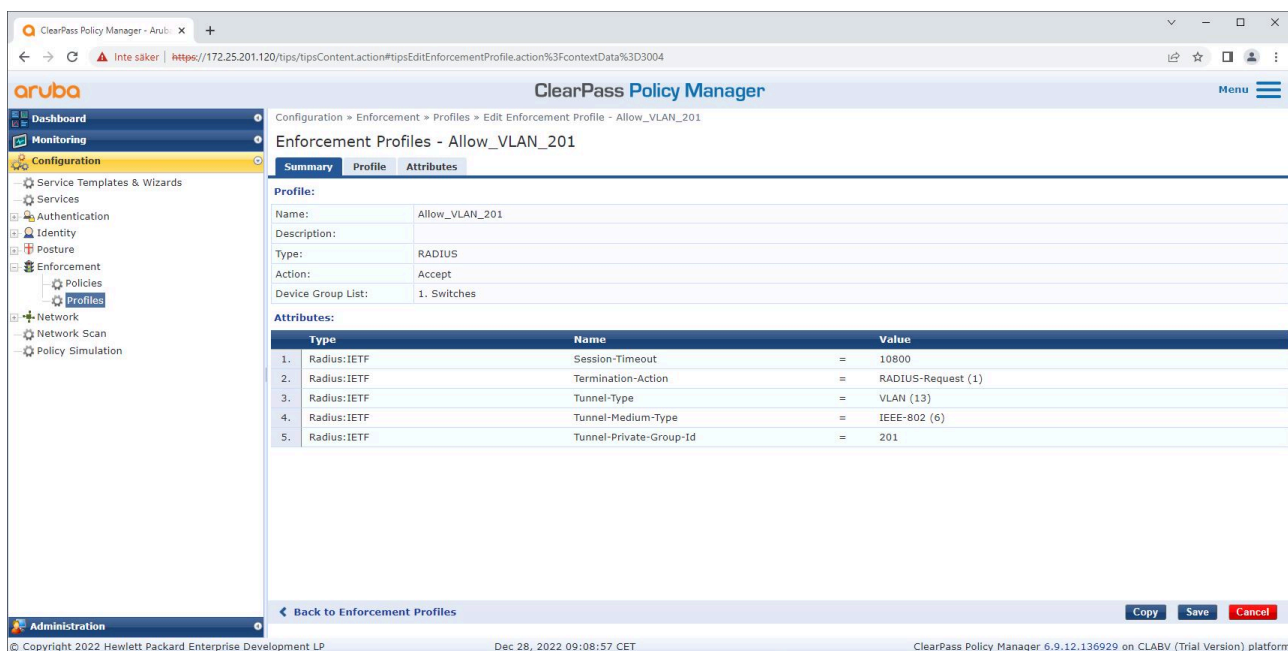


Le Impronte digitali dettagliate di un dispositivo Axis profilato. Si noti che SNMP è disabilitato per impostazione predefinita nei dispositivi Axis. Le informazioni di rilevamento specifiche LLDP, CDP e DHCP sono condivise dal dispositivo Axis nello stato predefinito di fabbrica e vengono inoltrate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

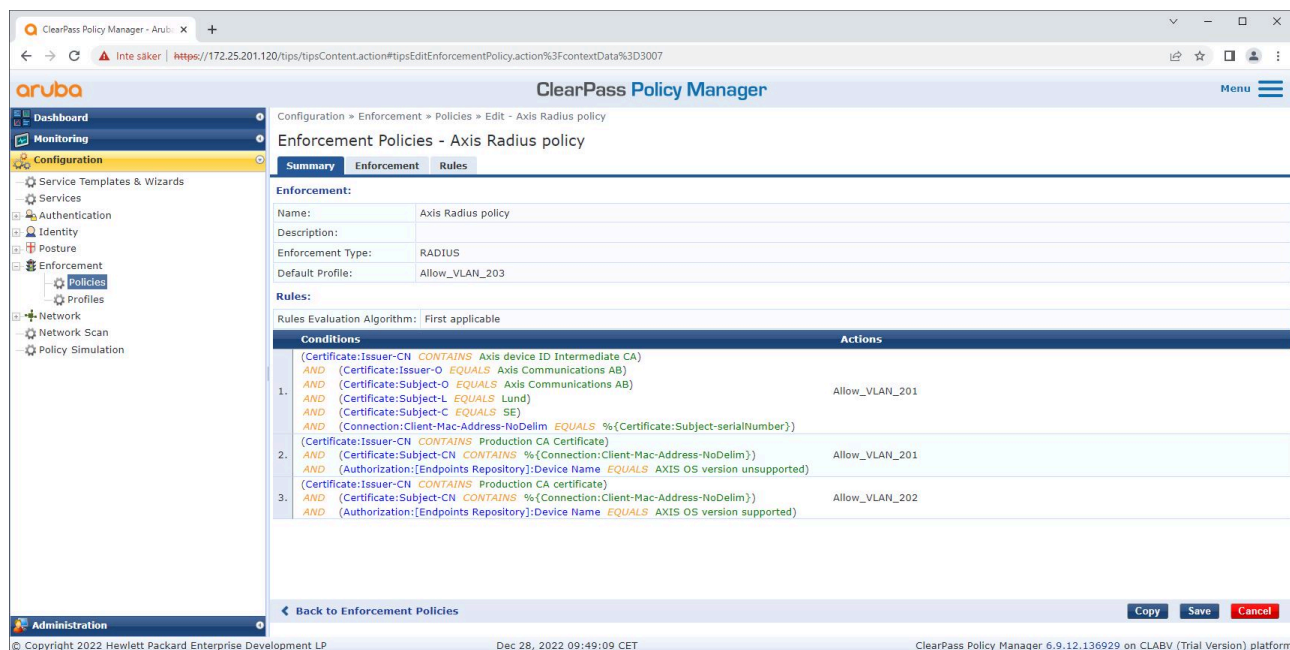
Configurazione del profilo di applicazione

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 politica che si applica ai dispositivi di rete nel gruppo di dispositivi "Interruttori". Il numero richiesto di profili di applicazione 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.

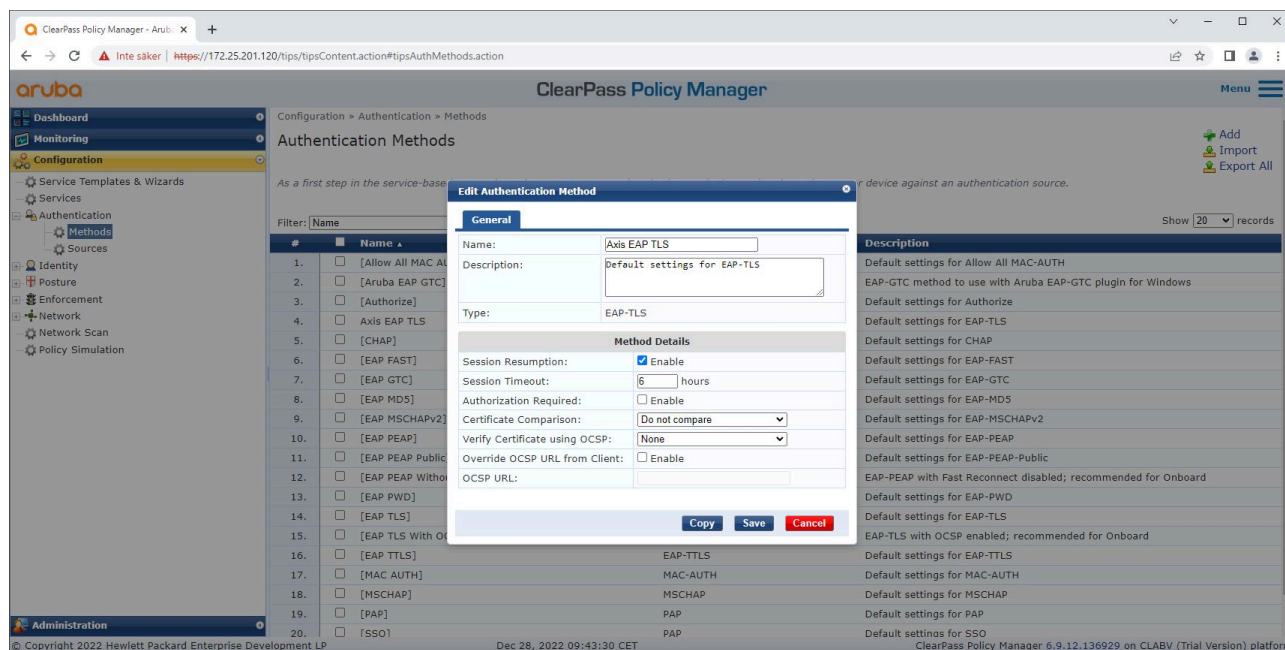
Rete di produzione (VLAN 202)

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

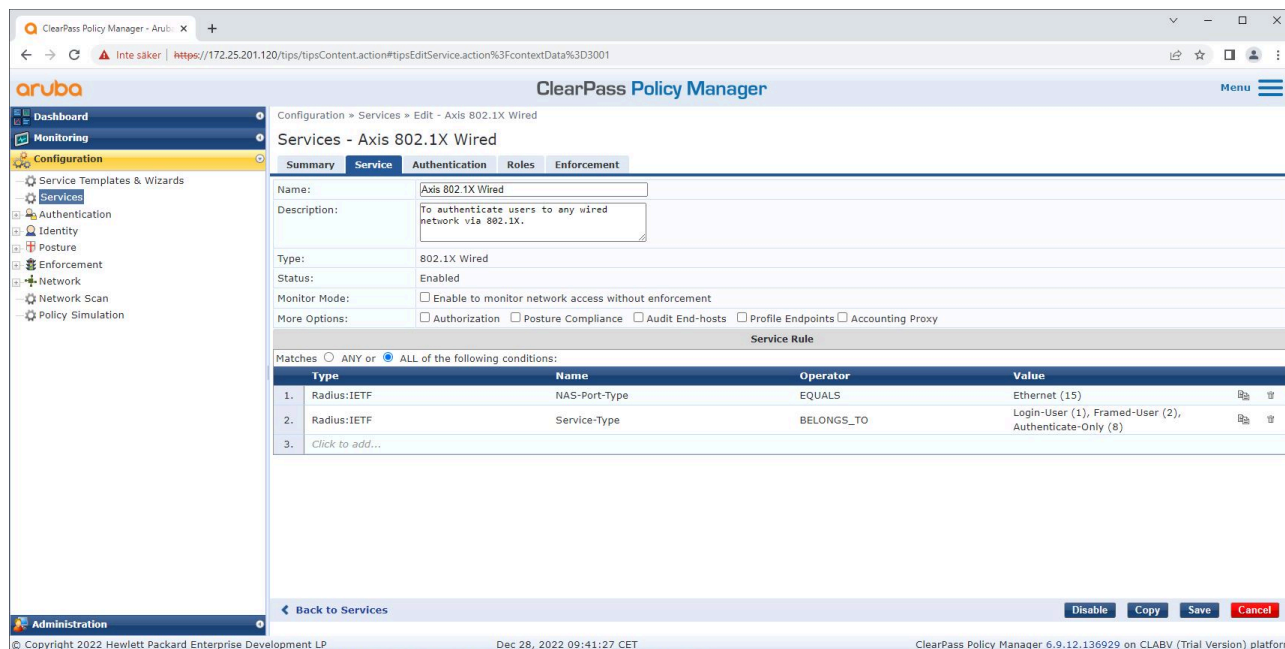
Il metodo di autenticazione definisce il modo in cui un dispositivo Axis tenta di autenticarsi sulla rete. Il metodo preferito è IEEE 802.1X EAP-TLS poiché i dispositivi Axis con Axis Edge Vault vengono forniti con IEEE 802.1X EAP-TLS abilitato per impostazione predefinita.



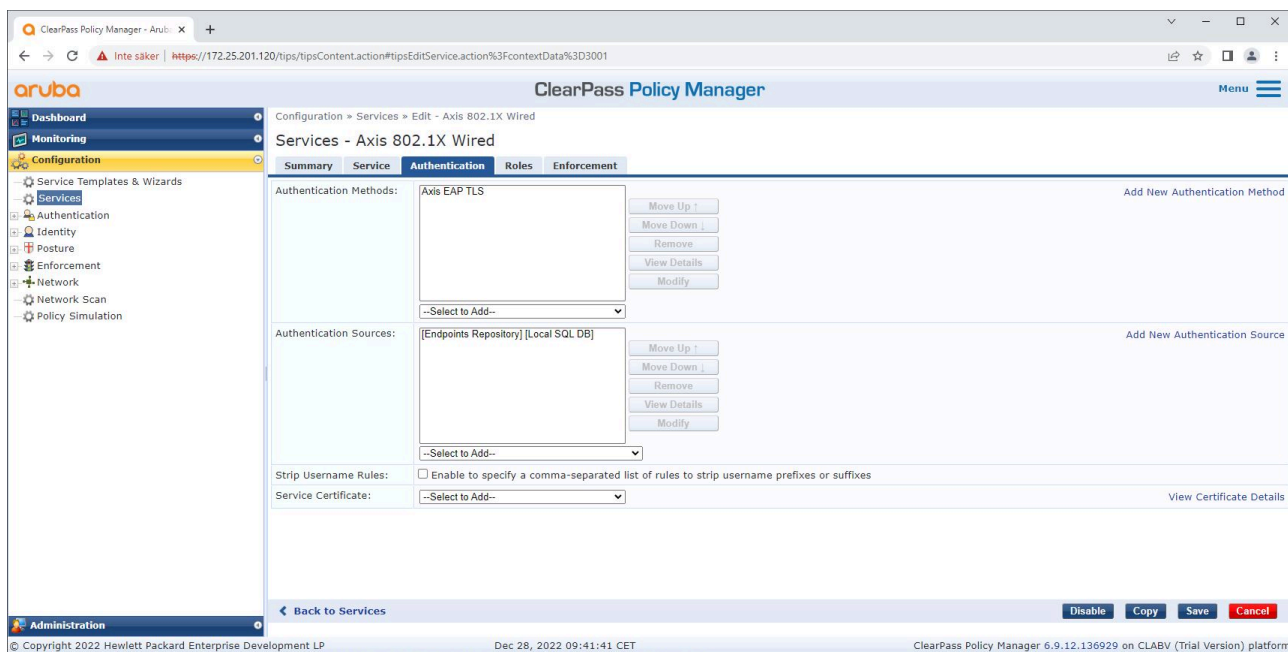
L'interfaccia del metodo di autenticazione di ClearPass Policy Manager, in cui viene definito il metodo di autenticazione EAP-TLS per i dispositivi Axis.

Configurazione del servizio

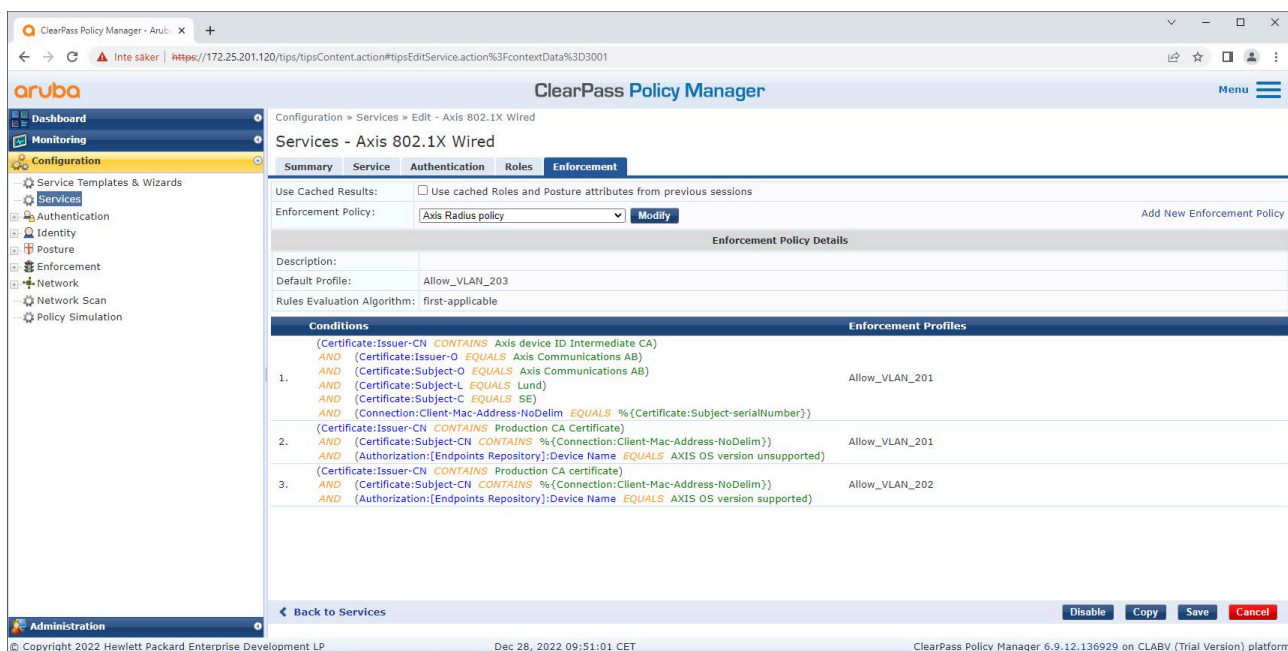
Nella pagina Services (Servizi), i passaggi di configurazione sono riuniti in un singolo servizio che gestisce l'autenticazione e l'autorizzazione dei dispositivi Axis nelle reti HPE Aruba Networking.



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.

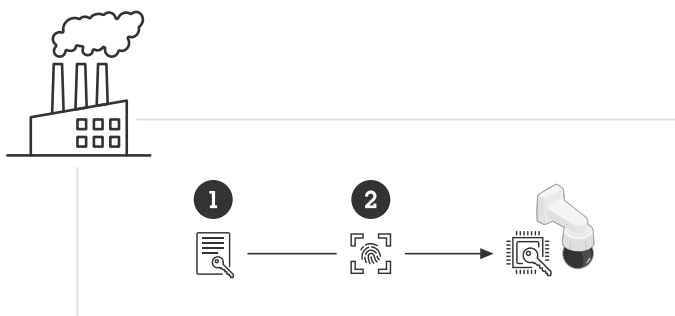
radius-server host MyRADIUSIPAddress key "MyRADIUSKey"

```
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.



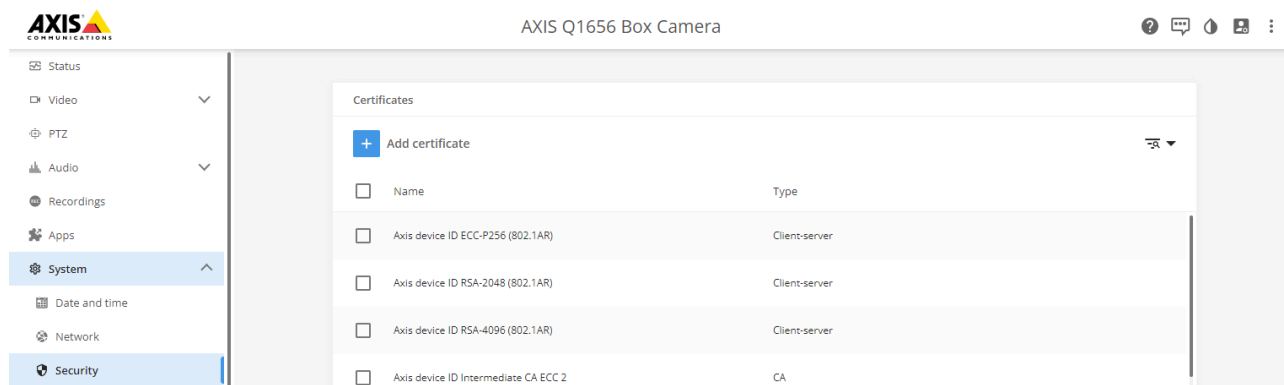
I dispositivi Axis sono prodotti con il certificato ID del dispositivo Axis conforme a IEEE 802.1AR per servizi di identità del dispositivo attendibili

- 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.

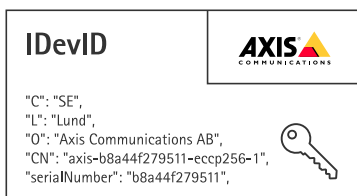
Nota

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



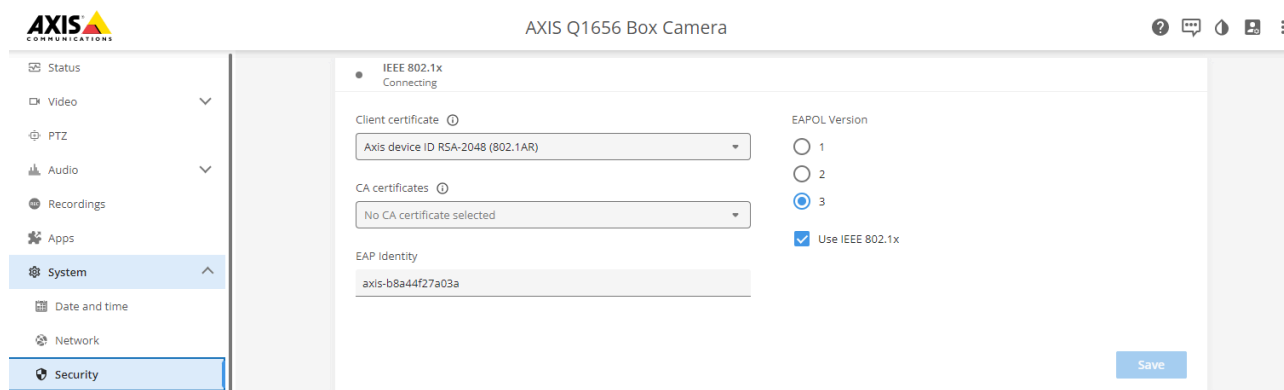
L'archivio certificati del dispositivo Axis nello stato predefinito di fabbrica, con l'ID dispositivo Axis.

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
Location	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 sulla rete per configurare e gestire più dispositivi Axis in modo economicamente vantaggioso. AXIS Device Manager è un'applicazione basata su Microsoft Windows® che viene installata localmente su un computer della rete, mentre AXIS Device Manager Extend si avvale di un'infrastruttura cloud per eseguire la gestione dei dispositivi in più siti. 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



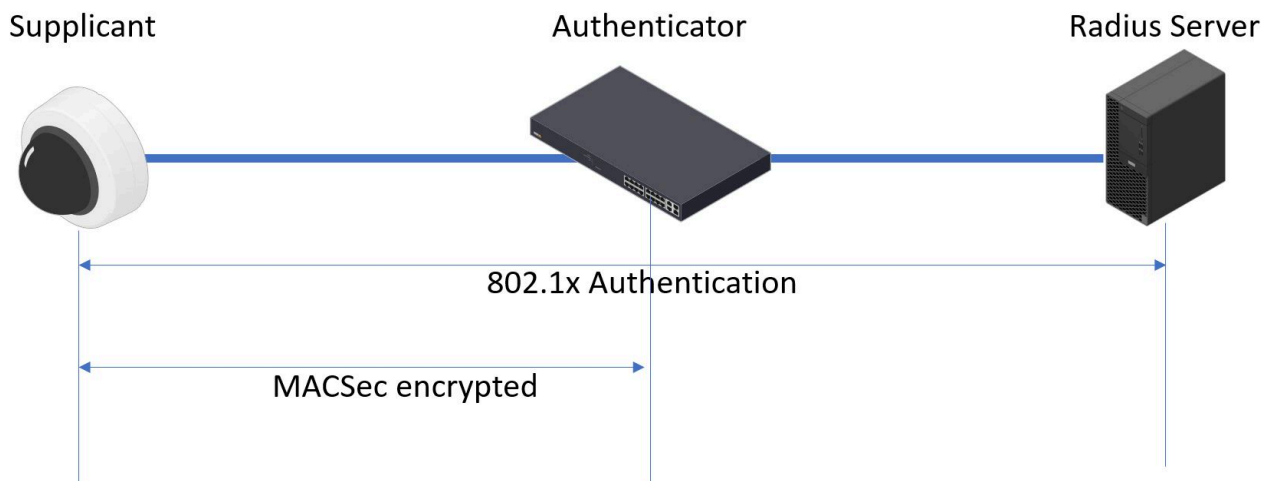
Per guardare questo video, andare alla versione web di questo documento.

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

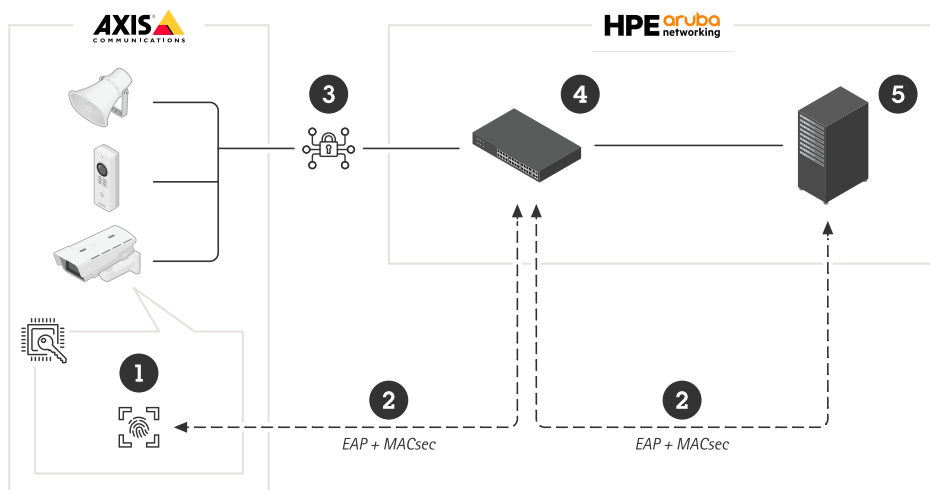
IEEE 802.1AE MACsec (Media Access Control Security) è un protocollo di rete ben definito che protegge crittograficamente i collegamenti Ethernet punto a punto sul livello di rete 2. Garantisce la riservatezza e l'integrità delle trasmissioni di dati tra due host.

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 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

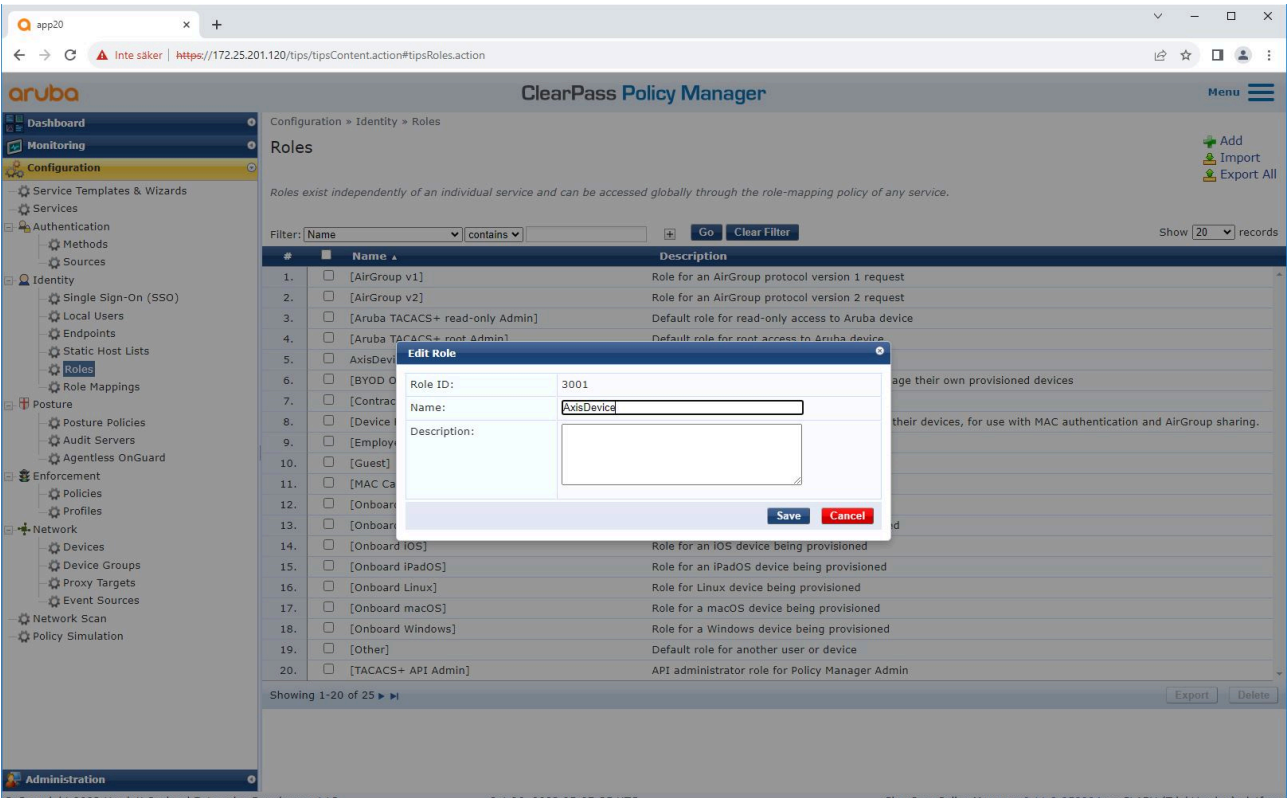
basato su porta IEEE 802.1X EAP-TLS (2). Attraverso la sessione EAP-TLS, le chiavi MACsec vengono scambiate automaticamente per impostare un collegamento sicuro (3), proteggendo tutto il traffico di rete dal dispositivo Axis allo switch di accesso HPE Aruba Networking.

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



The screenshot displays the ClearPass Policy Manager web interface. The left sidebar shows the navigation menu with options like Dashboard, Monitoring, Configuration, Authentication, Identity, Posture, Enforcement, and Network. The main content area is titled 'Roles' and shows a list of roles. An 'Edit Role' dialog box is open, showing the following details:

- Role ID: 3001
- Name: AxisDevice
- Description: (empty field)

The dialog has 'Save' and 'Cancel' buttons. The background list of roles includes entries like [AirGroup v1], [AirGroup v2], [Aruba TACACS+ read-only Admin], [Aruba TACACS+ root Admin], [AxisDevice], [BYOD], [Contract], [Device], [Employee], [Guest], [MAC Ca], [Onboard], [Onboard iOS], [Onboard iPadOS], [Onboard Linux], [Onboard macOS], [Onboard Windows], [Other], and [TACACS+ API Admin].

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

The screenshot shows the Aruba ClearPass Policy Manager web interface. The left sidebar contains navigation menus for Dashboard, Monitoring, Configuration, and Administration. The main content area is titled 'Role Mappings - Axis Role Mapping' and includes tabs for Summary, Policy, and Mapping Rules. The 'Policy' tab is active, showing the following details:

- Policy Name:** Axis Role Mapping
- Description:**
- Default Role:** [Guest]
- Mapping Rules:** Rules Evaluation Algorithm: Evaluate all

Conditions	Role Name
1. (Authentication:Full-Username BEGINS_WITH axis-00408c)	AxisDevice
2. (Authentication:Full-Username BEGINS_WITH axis-acc8e)	AxisDevice
3. (Authentication:Full-Username BEGINS_WITH axis-b8a44f)	AxisDevice

At the bottom of the page, there is a footer with copyright information and the version number: ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform.

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-numero di serie". Il numero di serie di un dispositivo Axis corrisponde al suo MAC address. Ad esempio "axis-b8a44f45b4e6".

Configurazione del servizio

The screenshot shows the Aruba ClearPass Policy Manager web interface. The left sidebar contains navigation menus for Dashboard, Monitoring, Configuration, and Administration. The main content area is titled 'Services - Axis 802.1X Wired' and includes tabs for Summary, Service, Authentication, Roles, and Enforcement. The 'Roles' tab is active, showing the following details:

- Role Mapping Policy:** Axis Role Mapping
- Description:**
- Default Role:** [Guest]
- Rules Evaluation Algorithm:** evaluate-all

Conditions	Role
1. (Authentication:Full-Username BEGINS_WITH axis-00408c)	AxisDevice
2. (Authentication:Full-Username BEGINS_WITH axis-acc8e)	AxisDevice
3. (Authentication:Full-Username BEGINS_WITH axis-b8a44f)	AxisDevice

At the bottom of the page, there is a footer with copyright information and the version number: ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform.

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.

ClearPass Policy Manager

Configuration » Services » Edit - Axis 802.1X Wired

Services - Axis 802.1X Wired

Summary Service Authentication Roles **Enforcement**

Use Cached Results: ☐ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: **Axis Radius policy** [Modify](#) [Add New Enforcement Policy](#)

Enforcement Policy Details

Description:

Default Profile: **Allow_VLAN_203**

Rules Evaluation Algorithm: evaluate-all

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

[Back to Services](#) [Disable](#) [Copy](#) [Save](#) [Cancel](#)

© Copyright 2023 Hewlett Packard Enterprise Development LP Oct 26, 2023 05:11:50 UTC ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform

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

Profilo esecutivo

ClearPass Policy Manager

Configuration » Enforcement » Profiles » Edit Enforcement Profile - Allow_VLAN_201

Enforcement Profiles - Allow_VLAN_201

Summary Profile **Attributes**

Profile:

Name: **Allow_VLAN_201**

Description:

Type: **RADIUS**

Action: **Accept**

Device Group List: **1. Switches**

Attributes:

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

[Back to Enforcement Profiles](#) [Copy](#) [Save](#) [Cancel](#)

© Copyright 2023 Hewlett Packard Enterprise Development LP Oct 26, 2023 05:13:21 UTC ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform

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 , vedere di seguito l'esempio di configurazione della porta riportato di seguito 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
```

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.

The screenshot displays the ClearPass Policy Manager web interface. The main content area is titled 'Services - Axis 802.1X Wired - Mac Authentication'. The 'Enforcement' tab is selected, showing the 'Enforcement Policy Details' section. The 'Conditions' table lists a single rule with three conditions: (Date:Day-of-Week BELONGS_TO Monday, Tuesday, Wednesday, Thursday, Friday), (Date:Time-of-Day IN_RANGE 09:00:00,17:00:00), and (Connection:Client-Mac-Vendor EQUALS Axis Communications AB). The 'Enforcement Profiles' table shows a single profile named 'Allow_VLAN_203'. The interface includes a sidebar with navigation options like Dashboard, Monitoring, Configuration, and Administration. The bottom status bar shows the copyright information and the version of the ClearPass Policy Manager.

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 ferialo, 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.

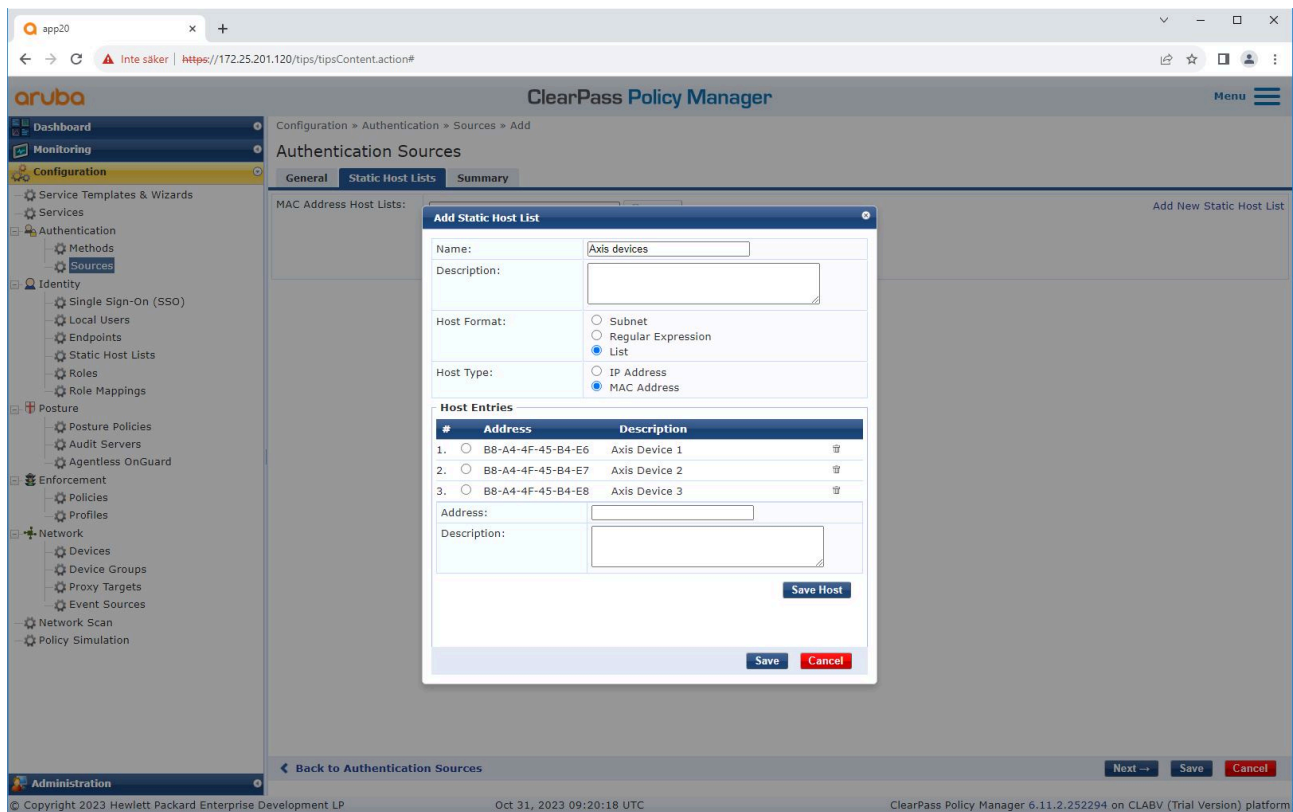
Configurazione di origine

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

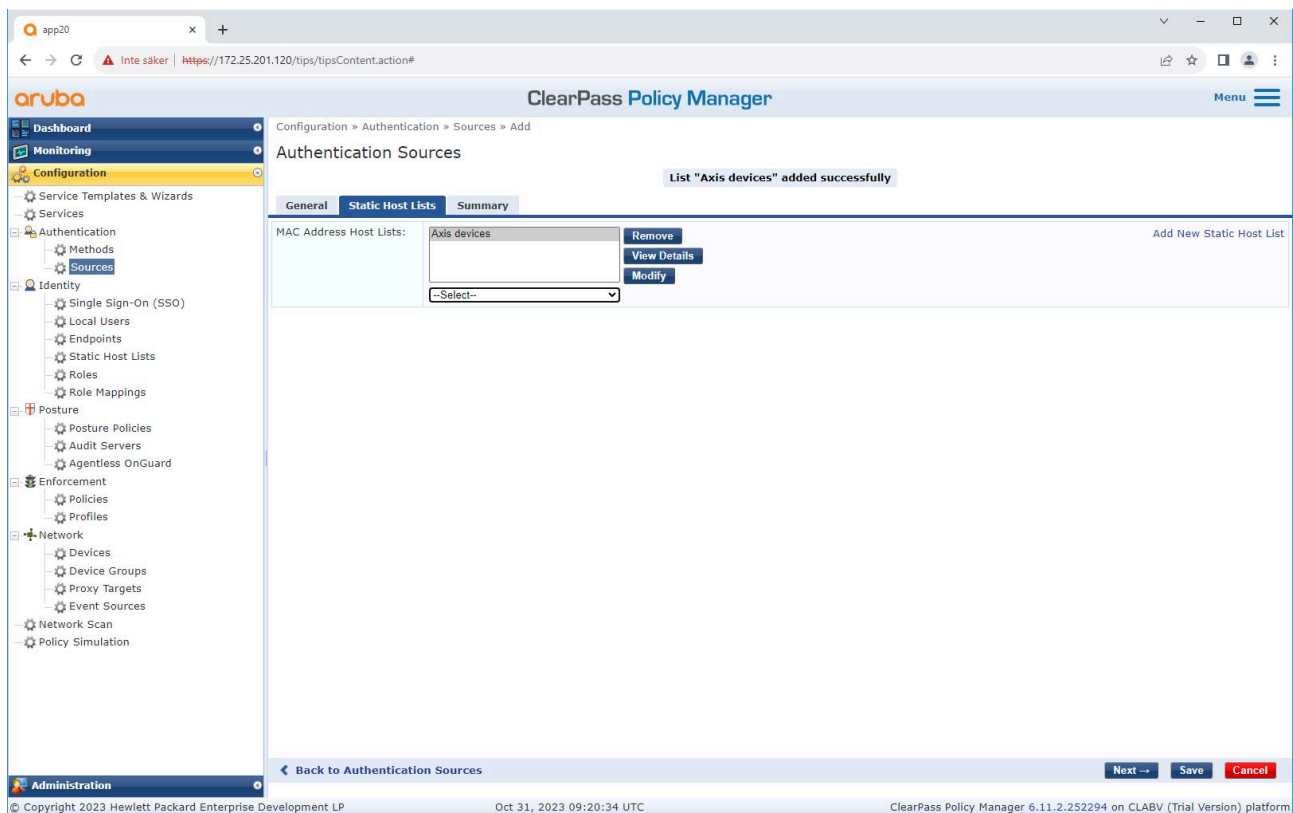
The first screenshot shows the 'Authentication Sources' page in the ClearPass Policy Manager. The left sidebar contains a navigation menu with options like Dashboard, Monitoring, Configuration, and Administration. The main content area displays a table of existing authentication sources. A filter bar at the top allows searching by name. The table lists 11 sources, including various user and device repositories.

#	Name	Type	Description
1.	[Admin User Repository]	Local SQL DB	Authenticate users against Policy Manager admin user database
2.	[Denylist User Repository]	Local SQL DB	Denylist database with users who have exceeded bandwidth or session related limits
3.	[Endpoints Repository]	Local SQL DB	Authenticate endpoints against Policy Manager local database
4.	[Guest Device Repository]	Local SQL DB	Authenticate guest devices against Policy Manager local database
5.	[Guest User Repository]	Local SQL DB	Authenticate guest users against Policy Manager local database
6.	[Insight Repository]	Local SQL DB	Insight database with session information for users and devices
7.	[Local User Repository]	Local SQL DB	Authenticate users against Policy Manager local user database
8.	[Onboard Devices Repository]	Local SQL DB	Authenticate Onboard devices against Policy Manager local database
9.	[Social Login Repository]	Local SQL DB	Authenticate users against Policy Manager social login database
10.	[Time Source]	Local SQL DB	Authorization source for implementing various time functions
11.	[Zone Cache Repository]	HTTP	Access attributes cached by Context Server Actions in previous sessions

The second screenshot shows the 'Add Authentication Source' page. The 'General' tab is active, showing fields for Name, Description, Type, and Use for Authorization. The Name field is set to 'Axis Devices' and the Description field contains 'MAC addresses of Axis devices in use.' The Type is set to 'Static Host List'. There is a checkbox for 'Use for Authorization' and a section for 'Authorization Sources' with a 'Remove' button and a 'View Details' button.



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.

app20 x +

Inte saker | <https://172.25.201.120/tips/tipsContent.action#tipsServices.action>

aruba ClearPass Policy Manager Menu

Configuration » Services

Services

This page shows the current list and order of services that ClearPass follows during authentication and authorization.

Filter: Name contains Go Clear Filter Hit Count for Current hour Show 20 records

#	Order	Name	Type	Template	Hit Count	Status
1.	☐ 1	Axis 802.1X Wired	RADIUS	802.1X Wired	0	✓
2.	☐ 2	Axis 802.1X Wired - Mac Authentication	RADIUS	MAC Authentication	0	✓
3.	☐ 3	Test_Service	RADIUS	802.1X Wired	0	✗
4.	☐ 4	[Policy Manager Admin Network Login Service]	TACACS+	TACACS+ Enforcement	0	✗
5.	☐ 5	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	0	✗
6.	☐ 6	[Aruba Device Access Service]	TACACS+	TACACS+ Enforcement	0	✗
7.	☐ 7	[Guest Operator Logins]	Application	Aruba Application Authentication	0	✗
8.	☐ 8	[Insight Operator Logins]	Application	Aruba Application Authentication	0	✗
9.	☐ 9	[Device Registration Disconnect]	WEBAUTH	Web-based Authentication	0	✗

Showing 1-9 of 9 Reorder Copy Export Delete

Copyright 2023 Hewlett Packard Enterprise Development LP Oct 26, 2023 05:34:53 UTC ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform

app20 x +

Inte saker | <https://172.25.201.120/tips/tipsContent.action#tipsEditService.action%3FcontextData%3D3006>

aruba ClearPass Policy Manager Menu

Configuration » Services » Edit - Axis 802.1X Wired - Mac Authentication

Services - Axis 802.1X Wired - Mac Authentication

Summary Service Authentication Roles Enforcement

Name: Axis 802.1X Wired - Mac Authentication

Description: To authenticate guest devices based on their MAC address.

Type: MAC Authentication

Status: Disabled

Monitor Mode: ☐ Enable to monitor network access without enforcement

More Options: ☐ Authorization ☐ Audit End-hosts ☐ Profile Endpoints ☐ Accounting Proxy

Service Rule

Matches ANY or ALL of the following conditions:

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

Back to Services Enable Copy Save Cancel

Copyright 2023 Hewlett Packard Enterprise Development LP Oct 26, 2023 05:15:11 UTC ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform

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

Configuration » Services » Edit - Axis 802.1X Wired - Mac Authentication

Services - Axis 802.1X Wired - Mac Authentication

Summary Service Authentication Roles Enforcement

Authentication Methods: [Allow All MAC AUTH] Add New Authentication Method

Authentication Sources: Axis Devices [Static Host List] Add New Authentication Source

Strip Username Rules: ☐ Enable to specify a comma-separated list of rules to strip username prefixes or suffixes

Back to Services Disable Copy Save Cancel

Copyright 2023 Hewlett Packard Enterprise Development LP Oct 31, 2023 09:22:22 UTC ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform

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

Configuration » Services » Edit - Axis 802.1X Wired - Mac Authentication

Services - Axis 802.1X Wired - Mac Authentication

Summary Service Authentication Roles Enforcement

Use Cached Results: ☐ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: Axis MAC Authentication Policy Modify Add New Enforcement Policy

Enforcement Policy Details

Description:

Default Profile: [Deny Access Profile]

Rules Evaluation Algorithm: evaluate-all

Conditions	Enforcement Profiles
1. (Date:Day-of-Week BELONGS_TO Monday, Tuesday, Wednesday, Thursday, Friday) AND (Date:Time-of-Day IN_RANGE 09:00:00,17:00:00) AND (Connection:Client-Mac-Vendor EQUALS Axis Communications AB)	Allow_VLAN_203

Back to Services Enable Copy Save Cancel

Copyright 2023 Hewlett Packard Enterprise Development LP Oct 26, 2023 05:15:57 UTC ClearPass Policy Manager 6.11.2.252294 on CLABV (Trial Version) platform

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 , vedere l'esempio di configurazione della porta riportato di seguito 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

2025-11 (M7.2)

© 2023 – 2025 Axis Communications AB