



HPE Aruba Networking

ユーザーマニュアル

目次

はじめに	3
安全なオンボーディング - IEEE 802.1AR/802.1X	4
初期認証	4
プロビジョニング	4
運用ネットワーク	5
HPE Aruba Networkingの設定	6
HPE Aruba Networking ClearPass Policy Manager	6
HPE Aruba Networkingアクセススイッチ	15
Axisの設定	16
Axisネットワーク装置	16
AXIS Device Manager	17
安全なネットワーク運用 - IEEE 802.1AE MACsec	18
HPE Aruba Networking ClearPass Policy Manager	19
ロールとロールマッピングポリシー	19
サービスの設定	20
強制プロファイル	21
HPE Aruba Networkingアクセススイッチ	22
レガシーオンボーディング - MAC認証	23
HPE Aruba Networking ClearPass Policy Manager	23
強制ポリシー	23
ソースの設定	24
サービスの設定	25
HPE Aruba Networkingアクセススイッチ	28

はじめに

この統合ガイドでは、HPE Aruba NetworkingネットワークへのAxisデバイスのオンボーディングと操作における最適な設定について説明しています。この設定では、IEEE 802.1X、IEEE 802.1AR、IEEE 802.1AE、HTTPSなどの最新のセキュリティ標準とプロトコルを使用します。

ネットワーク統合の適切な自動化を確立することにより、時間とコストを節約できます。これにより、Axisデバイス管理アプリケーションをHPE Aruba Networkingインフラストラクチャーとアプリケーションと合わせて使用する際に、システムの不必要的複雑化を回避できます。HPE Aruba NetworkingインフラストラクチャーとAxisデバイスおよびソフトウェアを組み合わせることで、以下のメリットが得られます。

- デバイスのステージングネットワークの削除によって、システムの複雑性を最小限に抑えられる。
- オンボーディングプロセスの自動化とデバイス管理の追加によって、コストを削減できる。
- Axisデバイスは、ゼロタッチのネットワークセキュリティ管理を提供する。
- HPEとAxisの専門性によって、ネットワーク全体のセキュリティが強化される。



オンボーディングプロセス全体を通じて論理ネットワーク間のソフトウェア定義による円滑な移行を実現するためには、設定を開始する前に、Axisデバイスの完全性を安全に検証できるようにネットワークインフラストラクチャーを準備する必要があります。設定を行う前に以下が必要です。

- HPE Aruba NetworkingアクセススイッチやHPE Aruba Networking ClearPass Policy Managerなど、HPE Aruba NetworkingのエンタープライズネットワークITインフラストラクチャーの管理の経験。
- 最新のネットワークアクセス制御技術とネットワークセキュリティポリシーに関する専門知識。
- できればAxis製品に関する事前の基本知識(ただし、これはガイドでも提供される)。

安全なオンボーディング - IEEE 802.1AR/802.1X



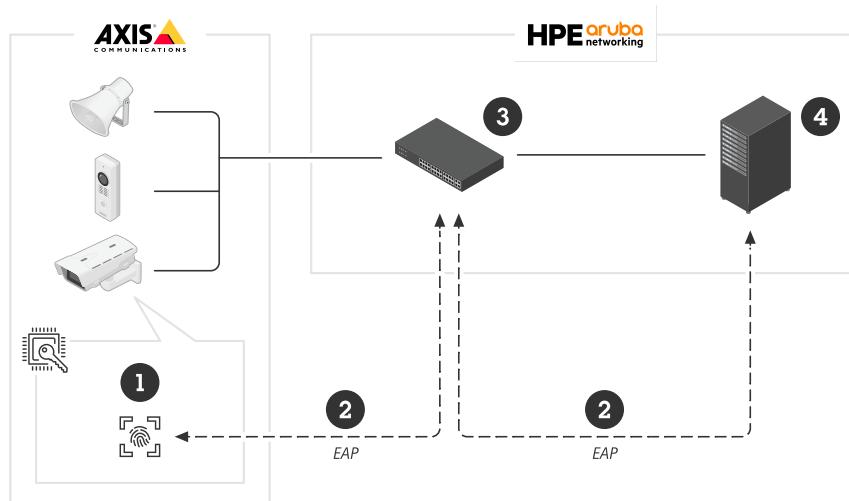
IEEE 802.1X/802.1ARによるゼロトラストネットワークへの安全な装置オンボーディング

初期認証

Axis Edge Vaultに対応するAxisデバイスがネットワークに接続されると、デバイスはIEEE 802.1Xネットワークアクセスコントロールを通じてIEEE 802.1AR AxisデバイスID証明書を使用し、自己認証を行います。

ネットワークへのアクセスの付与に際し、ClearPass Policy ManagerはAxisデバイスIDとデバイス固有の他のフィンガープリントを検証します。この情報 (MACアドレスやデバイスのAXIS OSバージョンなど) は、ポリシーに基づく決定に使用されます。

Axisデバイスは、ネットワーク上での自己認証に、IEEE 802.1AR準拠のAxisデバイスID証明書を使用します。

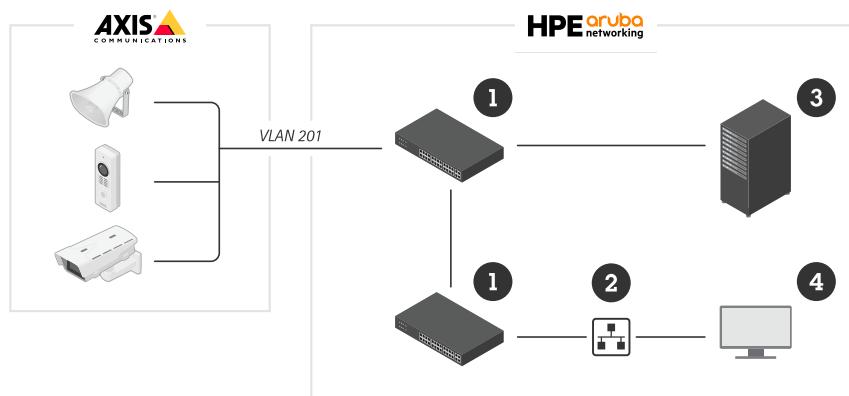


AxisデバイスはHPE Aruba Networkingネットワークに対する認証に、IEEE 802.1AR準拠のAxisデバイスID証明書を使用します。

- 1 AxisデバイスID
- 2 IEEE 802.1x EAP-TLSネットワーク認証
- 3 アクセススイッチ (認証者)
- 4 ClearPass Policy Manager

プロビジョニング

認証後、Axisデバイスはプロビジョニングネットワーク (VLAN201) に移行します。このネットワークには、AXIS Device Managerが含まれています。これは、デバイス設定、セキュリティ強化、AXIS OSの更新を実行します。デバイスのプロビジョニングを完了するには、IEEE 802.1XおよびHTTPSに対応する、新規顧客固有の運用グレード証明書をデバイスにアップロードします。

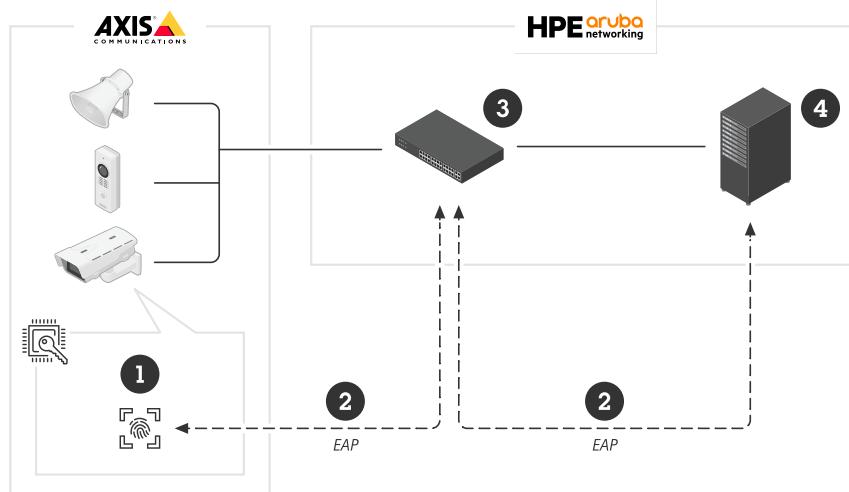


認証が成功すると、Axis装置は構成のためにプロビジョニングネットワークに移行します。

- 1 アクセススイッチ
- 2 プロビジョニングネットワーク
- 3 ClearPass Policy Manager
- 4 装置管理アプリケーション

運用ネットワーク

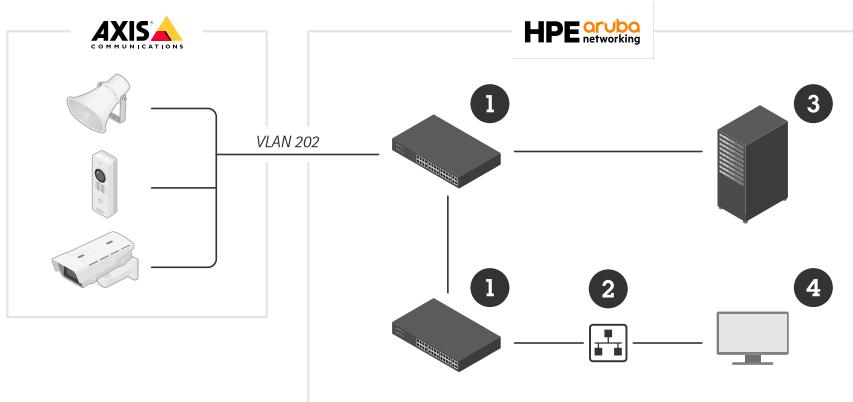
新規のIEEE 802.1X証明書を使用してAxis装置をプロビジョニングすると、新規認証の試行がトリガーされます。ClearPass Policy Managerは、新規の証明書を検証し、Axisデバイスを運用ネットワークに移行するかどうかを決定します。



設定が完了した後、Axisデバイスはプロビジョニングネットワークを離れ、ネットワーク上で再認証を試みます。

- 1 AxisデバイスID
- 2 IEEE 802.1x EAP-TLSネットワーク認証
- 3 アクセススイッチ(認証者)
- 4 ClearPass Policy Manager

再認証後、Axisデバイスは運用ネットワーク (VLAN 202) に移行し、そこでビデオ管理ソフトウェア (VMS) がデバイスに接続し、動作を開始します。



Axis装置には、運用ネットワークへのアクセスが付与されています。

- 1 アクセススイッチ
- 2 運用ネットワーク
- 3 ClearPass Policy Manager
- 4 ビデオ管理システム

HPE Aruba Networkingの設定

HPE Aruba Networking ClearPass Policy Manager

ClearPass Policy Managerは、マルチベンダーの有線、ワイヤレス、VPNインフラストラクチャー全体でIoT、BYOD、コーポレートデバイス、従業員、請負業者、ゲストを対象とする役割ベースとデバイスベースの安全なネットワークアクセスコントロールを提供します。

信頼できる証明書ストアの構成

1. axis.comで、Axis固有のIEEE 802.1AR証明書チェーンをダウンロードします。
2. Axis固有のIEEE 802.1AR Root CAおよび中間CA証明書チェーンを、信頼できる証明書ストアにアップロードします。
3. ClearPass Policy Managerを有効化し、IEEE 802.1X EAP-TLS経由でAxis装置を認証します。
4. 使用フィールドでEAPを選択します。証明書はIEEE 802.1X EAP-TLS認証に使用されます。

#	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=GlobalSign Root CA 2024, O=GlobalSign, Inc., C=US	AD/LDAP Servers, Endpoint Context Servers, SAML, SMTP, Others	Valid	Enabled
3.	OU=Class 3 Public Primary Certification Authority - G5,O=(c) 2006 VeriSign, Inc. - For authorized use only,OU=VeriSign Trust Network,O=VeriSign, Inc.,C=US	Others	Valid	Disabled
4.	OU=Class 3 Public Primary Certification Authority - G3,O=(c) 1999 VeriSign, Inc. - For authorized use only,OU=VeriSign Trust Network,O=VeriSign, Inc.,C=US	EAP, Others	Valid	Enabled
5.	OU=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	EAP, Others	Valid	Enabled
6.	OU=VeriSign Class 1 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
7.	OU=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	Aruba Infrastructure	Valid	Disabled
8.	OU=VeriSign Class 1 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
9.	OU=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	Others	Valid	Disabled
10.	OU=VeriSign Class 1 Public Primary Certification Authority - G5,OU=(c) 2006 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
11.	OU=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	EAP, Others	Valid	Disabled
12.	OU=VeriSign Class 1 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
13.	OU=USERTrust RSA Certification Authority,O=The USERTRUST Network,L=Jersey City,ST=New Jersey,C=US	EAP, Others	Valid	Disabled
14.	OU=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.	OU=TC TrustCenter Universal CA 1,OU=TC TrustCenter Universal CA,O=TC TrustCenter GmbH,C=DE	Others	Valid	Disabled

Axis固有のIEEE 802.1AR証明書を、Aruba ClearPass Policy Managerの信頼できる証明書ストアにアップロードします。

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.

#	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

Show [20] records

Showing 1-6 of 6

Add

Delete

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

Axis固有のIEEE 802.1AR証明書チェーンを含む、ClearPass Policy Manager内の信頼された証明書ストア。

ネットワーク装置/グループの構成

1. HPE Aruba Networkingアクセススイッチなどの信頼できるネットワークアクセス装置をClearPass Policy Managerに追加します。ClearPass Policy Managerは、ネットワーク内でIEEE 802.1X通信に使用されるアクセススイッチを把握する必要があります。RADIUS共有秘密は、特定のスイッチのIEEE 802.1X設定と一致させる必要があることに注意してください。
2. ネットワークデバイスグループ設定を使用して、複数の信頼できるネットワークアクセスデバイスをグループ化します。デバイスをグループ化することで、ポリシー設定が容易になります。

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.

#	Name	IP or Subnet Address	Device Groups	Description

Show [20] records

Add Import Export All Discovered Devices

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

ClearPass Policy Managerの信頼されたネットワーク装置インターフェース。

The screenshot shows the 'Add Device' dialog in the ClearPass Policy Manager interface. The device is named 'SW04' and has the IP address '172.25.200.13'. The 'Vendor Name' is set to 'Aruba'. The 'Description' field is empty. The 'RADIUS Shared Secret' and 'TACACS+ Shared Secret' fields both contain '*****'. The 'Verify' fields next to them also contain '*****'. There are checkboxes for 'Enable RADIUS Dynamic Authorization' and 'Enable RadSec', both of which are unchecked.

信頼できるデバイスとしてHPE Aruba NetworkingアクセススイッチをClearPass Policy Managerに追加します。RADIUS共有秘密は、特定のスイッチのIEEE 802.1X設定と一致させる必要があることに注意してください。

The screenshot shows the 'Network Devices' list in the ClearPass Policy Manager. A message at the top says 'Device SW04 added'. Below it, a note states: 'A Network Access Device (NAD) must belong to the global list of devices in the ClearPass database in order to connect to ClearPass.' The table lists one device:

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

1つの信頼できるネットワークデバイスが設定されたClearPass Policy Manager。

The screenshot shows the ClearPass Policy Manager interface. The left sidebar is titled 'aruba' and includes sections for Dashboard, Monitoring, Configuration, and Network. Under Configuration, there are Service Templates & Wizards, Services, Authentication, Identity, Posture, Enforcement, and Network. The Network section is expanded, showing Devices, Device Groups (which is selected), Proxy Targets, and Event Sources. The main content area is titled 'Network Device Groups' and contains a table with columns for #, Name, Format, and Description. A filter bar at the top allows searching by Name. On the right, there are buttons for Add, Import, and Export All. The status bar at the bottom indicates the date and time as Dec 28, 2022 08:57:07 CET, and the software version as ClearPass Policy Manager 6.9.12.136929 on CLABV (Trial Version) platform.

ClearPass Policy Managerの信頼されたネットワーク装置グループインターフェース。

The screenshot shows the 'Add New Device Group' dialog box overlaid on the main interface. The dialog has fields for Name (filled with 'Switches') and Description (filled with 'Access Switches'). The Format section has three radio buttons: Subnet, Regular Expression, and List, with List selected. Below these are two lists: 'Available Devices (0)' and 'Selected Devices (1)'. The 'Selected Devices' list contains one item: 'SW04 [172.25.200.13]'. At the bottom of the dialog are 'Save' and 'Cancel' buttons. The background shows the same network configuration interface as the first screenshot.

ClearPass Policy Managerの新規デバイスグループに、信頼されたネットワークアクセスデバイスを追加します。

The screenshot shows the 'Device Groups' page in ClearPass Policy Manager. A success message at the top states 'Device Group "Switches" added successfully'. The table lists one device group named 'Switches' with the description 'Access Switches'. The left sidebar shows the navigation menu, and the bottom status bar indicates the date and time as Dec 28, 2022 09:05:43 CET.

ClearPass Policy Managerで、1つまたは複数の信頼できるネットワークデバイスを含むネットワークデバイスグループが設定された状態。

装置のフィンガープリントの構成

Axisデバイスは、ネットワーク検出を通じて、MACアドレスやデバイスソフトウェアのバージョンなど、デバイス固有の情報を配布することができます。この情報を使用して、ClearPass Policy Managerでデバイスフィンガープリントを作成、更新、管理します。また、AXIS OSバージョンに基づいてアクセスを許可または拒否することもできます。

- [Administration (管理者)] > [Dictionaries (辞書)] > [Device Fingerprints (装置のフィンガープリント)] に進みます。
- 既存の装置フィンガープリントを選択するか、新規の装置フィンガープリントを作成します。
- デバイスフィンガープリントの設定を行います。

The screenshot shows the 'Device Fingerprints' page in ClearPass Policy Manager. A modal window titled 'Update Device Fingerprints' is open, showing a table of custom rules. One rule is selected, showing the conditions: 'Category: Network Camera', 'Family: Axis', and 'Name: AXIS OS version unsupp'. The table also lists other rules: 'Host MAC Vendor contains_all Axis Communications AB', 'LLDP System Description not_contains 10.12', and 'SNMP System Description not_contains 10.12'. The right side of the screen shows a list of device fingerprints with names like 'AXIS OS version unsupported', 'AXIS OS version supported', 'Axis Network Camera', and 'Axis Print Server'. The bottom status bar indicates the date and time as Nov 25, 2022 08:50:09 CET.

ClearPass Policy Managerでの装置のフィンガープリント設定。この例では、AXIS OSバージョン 10.12以外のバージョンを実行しているAxisデバイスはサポートされていません。

The screenshot shows the 'Device Fingerprints' configuration page in ClearPass Policy Manager. A modal window titled 'Update Device Fingerprints' is open, showing a table of custom rules. The rules are:

Name	Operator	Value
Host MAC Vendor	contains_all	Axis Communications AB
LLDP System Description	contains	10.12
SNMP System Description	contains	10.12

Note: 0 Rule(s) will be deleted.

Buttons at the bottom: Update, Delete Fingerprint, Close.

ClearPass Policy Managerでの装置のフィンガープリント設定。この例では、AXIS OSバージョン 10.12以外のバージョンを実行しているAxisデバイスはサポートされています。

ClearPass Policy Managerによって収集された装置のフィンガープリントに関する情報は、エンドポイントセクションにあります。

- [Configuration (設定)] > [Identity (ID)] > [Endpoints (エンドポイント)] に移動します。
- 表示する装置を選択します。
- [Device Fingerprints (装置のフィンガープリント)] タブをクリックします。

注

SNMPは、Axis装置ではデフォルトで無効になっており、HPE Aruba Networkingのアクセススイッチから収集されます。

The screenshot shows the 'Edit Endpoint' configuration page in ClearPass Policy Manager. The endpoint details are:

MAC Address	B8-A4-4F-30-42-EA	IP Address	172.25.201.233
Description		Static IP	FALSE
Status	<input checked="" type="radio"/> Unknown client	Hostname	axis-b8a44f3042ea
MAC Vendor	Axis Communications AB	Device Category	Network Camera
Added by	Policy Manager	Device Name	AXIS OS version support
Online Status	Not Available	Added At	Dec 28, 2022 14:50:45 CET
Connection Type	Unknown	Profiled by	Policy Manager
		Last Profiled At	Dec 29, 2022 08:18:23 CET

Buttons at the bottom: Save, Cancel.

ClearPass Policy ManagerによってプロファイルされたAxis装置。

The screenshot shows the 'Edit Endpoint' dialog for an Axis camera. The dialog has tabs for 'Endpoint', 'Attributes', and 'Device Fingerprints'. Under 'Device Fingerprints', there is a table with the following data:

	CDP Device Description:	DHCP Option55:	DHCP Option60:	DHCP Options:	Host MAC Vendor:	LLDP System Description:	SNMP Device Name:	SNMP Device Type:	SNMP System Description:
1.		1,3,6,12,15,28,42,66,119	AXIS,Panoramic Camera,P3727-PLE,10.12.130	53,57,55,12,60,61	Axis Communications AB	AXIS P3727-PLE Panoramic Camera 10.12.130	axis-b8a4f3042ea	Host	AXIS P3727-PLE Panoramic Camera 10.12.130

Below the table are buttons for 'Save' and 'Cancel'. The main interface shows a list of endpoints with the following columns:

V	Status	Profiled
1.	Unknown	Yes
2.	Unknown	Yes
3.	Unknown	Yes
4.	Unknown	Yes

Buttons at the bottom include 'Get Server Action', 'Update Fingerprint', 'Export', and 'Delete'.

プロファイルされたAxis装置の詳細な装置フィンガープリント。Axisデバイスでは、SNMPがデフォルトで無効になっています。LLDP、CDP、DHCP固有の検出情報は、工場出荷時状態のAxisデバイスによって共有され、HPE Aruba Networkingアクセススイッチを経由してClearPass Policy Managerへ中継されます。

強制プロファイルの構成

強制プロファイルによって、ClearPass Policy Managerはスイッチ上のアクセスポートに特定のVLAN IDを割り当てることが可能になります。これはポリシーに基づく決定であり、デバイスグループ「スイッチ」内のネットワークデバイスに適用されます。必要な強制プロファイル数は、使用しているVLANの数によって異なります。設定には3つのVLAN (VLAN 201、202、203) があります。これらは3つの強制プロファイルに対応しています。

VLANの強制プロファイル設定を完了すると強制ポリシー自体を設定できます。ClearPass Policy Managerの強制ポリシー設定は、4つのサンプルレポリシープロファイルに基づき、HPE Aruba NetworkingネットワークへのアクセスをAxisデバイスに付与するかどうかを判断します。

The screenshot shows the 'Edit Enforcement Profile' dialog for 'Allow_VLAN_201'. The dialog has tabs for 'Summary', 'Profile', and '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

Buttons at the bottom include 'Back to Enforcement Profiles', 'Copy', 'Save', and 'Cancel'.

VLAN 201へのアクセスを許可する強制プロファイルの例。

The screenshot shows the ClearPass Policy Manager interface for managing enforcement policies. The specific policy shown is 'Axis Radius policy' with 'RADiUS' as the enforcement type and 'Allow_VLAN_203' as the default profile. The 'Rules' tab is selected, displaying four rules. Rule 1 allows VLAN 201 for certificates issued by Axis device ID Intermediate CA and subject O=Lund. Rule 2 allows VLAN 201 for Production CA certificates from endpoints with unsupported Axis OS versions. Rule 3 allows VLAN 202 for Production CA certificates from endpoints with supported Axis OS versions.

ClearPass Policy Managerの強制ポリシー構成。

4つの強制ポリシーとそのアクションは以下の通りです。

ネットワークアクセスの拒否

IEEE 802.1Xネットワークアクセスコントロール認証が実行されない場合、ネットワークへのアクセスは拒否されます。

ゲストネットワーク (VLAN 203)

IEEE 802.1Xネットワークアクセスコントロール認証が失敗した場合、Axis装置には限定的な隔離ネットワークへのアクセスが付与されます。その後、適切なアクションを決定するために、デバイスの手動検査が必要になります。

プロビジョニングネットワーク (VLAN 201)

Axis装置に、プロビジョニングネットワークへのアクセスが付与されます。これにより、AXIS Device ManagerとAXIS Device Manager Extendを通じてAxis装置の管理機能が提供されます。また、AXIS OSの更新、運用グレードの証明書、その他の設定を使用してAxis装置を設定することも可能になります。ClearPass Policy Managerは、以下の状態を検証します:

- デバイスのAXIS OSバージョン。
- デバイスのMACアドレスが、AxisデバイスID証明書のシリアル番号属性を持つベンダー固有のMACアドレススキームと一致すること。
- AxisデバイスID証明書が検証可能であり、発行者、組織、場所、国などのAxis固有の属性が一致すること。

運用ネットワーク (VLAN 202)

Axisデバイスには、動作する運用ネットワークへのアクセスが付与されます。アクセスは、プロビジョニングネットワーク (VLAN 201) 内からデバイスのプロビジョニングが完了した後に許可されます。ClearPass Policy Managerは、以下の状態を検証します:

- デバイスのAXIS OSバージョン。
- デバイスのMACアドレスが、AxisデバイスID証明書のシリアル番号属性を持つベンダー固有のMACアドレススキームと一致すること。
- 運用グレードの証明書が、信頼できる証明書ストアによって検証できること。

認証方式の構成

認証方式は、Axisデバイスがネットワーク上で自己認証を試みる方法を定義します。Axis Edge Vaultを搭載するAxisデバイスは、デフォルトでIEEE 802.1X EAP-TLSが有効になっているため、望ましい方式はIEEE 802.1X EAP-TLSです。

The screenshot shows the 'Edit Authentication Method' dialog in the ClearPass Policy Manager. The 'General' tab is selected, displaying the following details:

- Name:** Axis EAP TLS
- Description:** Default settings for EAP-TLS
- Type:** EAP-TLS
- Method Details:**
 - Session Resumption: Enable
 - Session Timeout: 6 hours
 - Authorization Required:
 - Certificate Comparison: Do not compare
 - Verify Certificate using OCSP: None
 - Override OCSP URL from Client:
 - OCSP URL: [empty]

Below the dialog, a list of other authentication methods is shown, including EAP-TTLS, MAC-AUTH, MSCHAP, PAP, and PWD. The status bar at the bottom indicates the date and time: Dec 28, 2022 09:43:30 CET.

AxisデバイスのEAP-TLS認証方式が定義されているClearPass Policy Managerの認証方式インターフェース。

サービスの設定

[Services (サービス)] ページでは、設定手順がHPE Aruba Networkingネットワーク内のAxisデバイスの認証と承認を処理する1つのサービスに統合されています。

The screenshot shows the 'Edit - Axis 802.1X Wired' page in the ClearPass Policy Manager. The 'Service' tab is selected, displaying the following details:

- Name:** Axis 802.1X Wired
- Description:** To authenticate users to any wired network via 802.1X.
- Type:** 802.1X Wired
- Status:** Enabled
- Monitor Mode:** Enable to monitor network access without enforcement
- More Options:** Authorization, Posture Compliance, Audit End-hosts, Profile Endpoints, Accounting Proxy

Below the service details, a 'Service Rule' section is shown with the following conditions:

Type	Name	Operator	Value
1. Radius:IETF	NAS-Port-Type	EQUALS	Ethernet (15)
2. Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)
Click to add...			

At the bottom of the page, there are buttons for Disable, Copy, Save, and Cancel. The status bar at the bottom indicates the date and time: Dec 28, 2022 09:41:27 CET.

専用Axisサービスが作成され、接続方式としてIEEE 802.1Xが採用されます。

ClearPass Policy Manager - Aruba

Configuration > Services > Edit - Axis 802.1X Wired

Services - Axis 802.1X Wired

Authentication (Selected)

Summary Service Roles Enforcement

Authentication Methods: Axis EAP TLS

Authentication Sources: [Endpoints Repository] [Local SQL DB]

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

Service Certificate: [-Select to Add-]

Add New Authentication Method

Add New Authentication Source

View Certificate Details

Move Up ↑ Move Down ↓ Remove View Details Modify

--Select to Add--

Back to Services

Disable Copy Save Cancel

Administration

Copyright 2022 Hewlett Packard Enterprise Development LP Dec 28, 2022 09:41:41 CET ClearPass Policy Manager 6.9.12.136929 on CLABV (Trial Version) platform

先に作成したEAP-TLS認証方式が、サービスに設定されます。

ClearPass Policy Manager - Aruba

Configuration > Services > Edit - Axis 802.1X Wired

Services - Axis 802.1X Wired

Enforcement (Selected)

Summary Service Authentication Roles

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

Enforcement Policy: Axis Radius policy

Modify Add New Enforcement Policy

Description:

Default Profile: Allow_VLAN_203

Rules Evaluation Algorithm: first-applicable

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

Back to Services

Disable Copy Save Cancel

Administration

Copyright 2022 Hewlett Packard Enterprise Development LP Dec 28, 2022 09:51:01 CET ClearPass Policy Manager 6.9.12.136929 on CLABV (Trial Version) platform

先に作成した強制ポリシーが、サービスに設定されます。

HPE Aruba Networkingアクセススイッチ

Axisデバイスは、PoE対応のアクセススイッチに直接接続することも、互換性のあるAxis PoEミッドスパンを経由して接続することもできます。HPE Aruba NetworkingネットワークにAxisデバイスを安全にオンボードするには、アクセススイッチをIEEE 802.1X通信用に設定する必要があります。AxisデバイスはIEEE 802.1x EAP-TLS通信をClearPass Policy Managerに中継します。ClearPass Policy Managerは、RADIUSサーバーとして動作します。

注

ポートアクセス全体のセキュリティを強化する目的で、300秒の周期的なAxisデバイスの再認証も設定されます。

この例は、HPE Aruba Networkingアクセススイッチのグローバル設定およびポート設定を示しています。

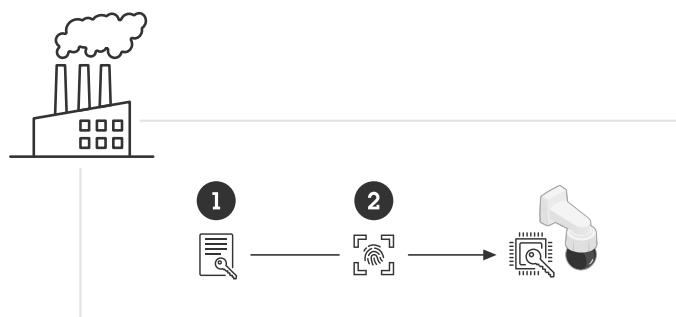
```
radius-server host MyRADIUSIPAddress key "MyRADIUSKey"
```

```
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の設定

Axisネットワーク装置

Axis Edge Vaultに対応するAxisデバイスは、製造時にAxisデバイスIDと呼ばれる安全なデバイス識別子が付与されます。AxisデバイスIDは、IEEE 802.1Xによる自動化された安全なデバイス識別およびネットワークオンボーディングの方法を定義する国際規格IEEE 802.1ARに基づいています。



信頼できるデバイスIDサービス提供のため、Axis装置はIEEE 802.1AR準拠のAxisデバイスID証明書を製造時に付与されている

- 1 AxisデバイスIDキーインフラストラクチャー (PKI)
- 2 AxisデバイスID

Axisデバイスのセキュアエレメントにより提供されるハードウェア保護型の安全なキーストアは、工場でプロビジョニングされています。さらに、Axisデバイスの信頼性をグローバルに証明するデバイス固有の証明書と対応キー (AxisデバイスID) が付属します。Axis Edge VaultとAxisデバイスIDに対応するAxisデバイスは、Axis Product Selectorを使用して確認できます。

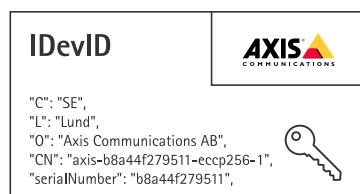
注

Axis装置のシリアル番号は、装置のMACアドレスです。

Name	Type
Axis device ID ECC-P256 (802.1AR)	Client-server
Axis device ID RSA-2048 (802.1AR)	Client-server
Axis device ID RSA-4096 (802.1AR)	Client-server
Axis device ID Intermediate CA ECC 2	CA

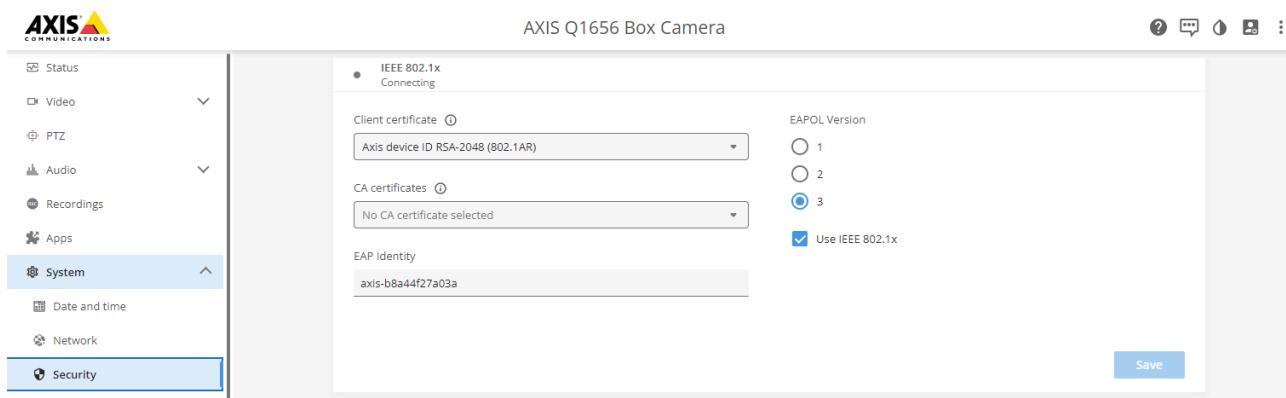
工場出荷時設定のAxisデバイスに搭載された証明書ストアとAxisデバイスID。

IEEE 802.1AR準拠のAxisデバイスID証明書には、シリアル番号に関する情報および、ベンダー固有のその他の情報が含まれています。ClearPass Policy Managerは、ネットワークへのアクセスを付与する際の分析と判断にこの情報を使用します。以下の情報は、AxisデバイスのID証明書から取得できます。



国名	SE
場所	ルンド
Issuer Organization (発行者組織)	アクシスコミュニケーションズ AB
Issuer Common Name (発行者の通称)	Axis device ID intermediate
組織	アクシスコミュニケーションズ AB
Common Name (通称)	axis-b8a44f279511-eccp256-1
シリアル番号	b8a44f279511

一般名称は、Axis社名とデバイスのシリアル番号を組み合わせ、そのシリアル番号の後に暗号アルゴリズム(ECC P256、RSA 2048、RSA 4096)を付加して構成されています。AXIS OS 10.1 (2020-09)以降、IEEE 802.1Xは事前設定されたAxisデバイスIDでデフォルトで有効になっています。これにより、デバイスはIEEE 802.1X対応ネットワーク上で自己認証を行うことができます。



Axisデバイスは工場出荷時のデフォルト設定でIEEE 802.1Xが有効化されており、AxisデバイスID証明書が事前選択されています。

AXIS Device Manager

AXIS Device ManagerとAXIS Device Manager Extendをネットワーク上で使用し、複数のAxisデバイスをコスト効率の良い方法で設定、管理することができます。AXIS Device Managerは、Microsoft Windows®ベースのアプリケーションでネットワーク内のマシンにローカルにインストールされます。AXIS Device Manager Extendはクラウドインフラストラクチャーに依存し、複数サイトのデバイス管理を実行します。いずれも手軽に管理、設定でき、以下などが可能です。

- AXIS OS更新のインストール。
- HTTPSやIEEE 802.1X証明書などのサイバーセキュリティ設定の適用。
- 画像の設定など、デバイス固有の設定の実行。

安全なネットワーク運用 - IEEE 802.1AE MACsec

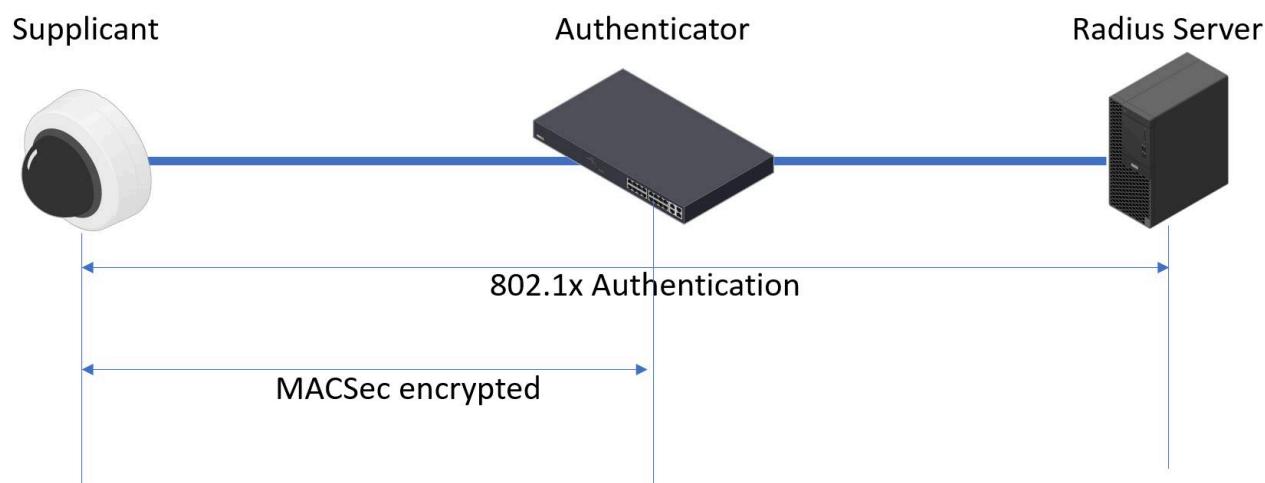


IEEE 802.1AE MACsec Layer-2 Securityによるゼロトラストネットワーク暗号化

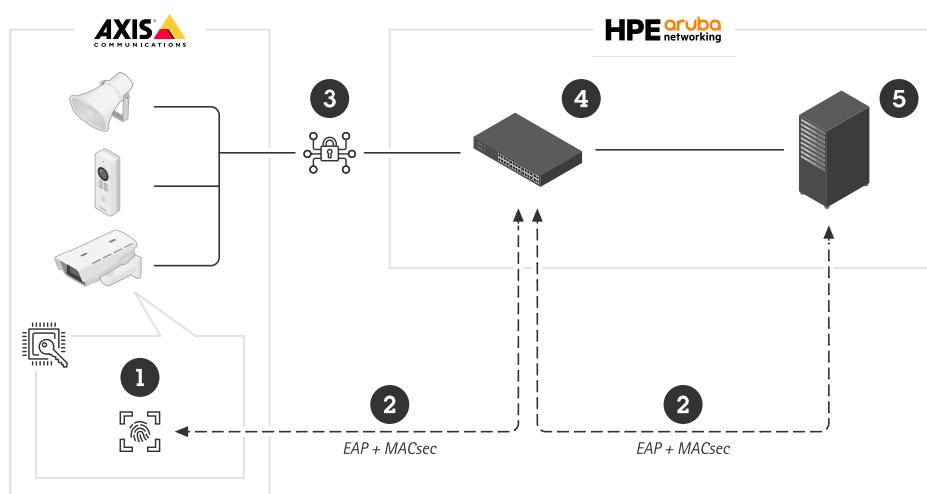
IEEE 802.1AE MACsec (Media Access Control Security) は明確に定義されたネットワークプロトコルであり、ネットワークレイヤー2にあるポイントツーポイントイーサネットリンクを暗号的に保護します。これにより、2つのホスト間のデータ送信の機密性と完全性が保証されます。

IEEE 802.1AE MACsec規格は、次の2つの運用モードを提供します。

- 手動で構成可能なPre-Shared Key/Static CAKモード
- IEEE 802.1X EAP-TLSを使用するAutomatic Master Session/Dynamic CAKモード



AXIS OS 10.1 (2020-09) 以降では、Axis device IDに対応するデバイスにおいてIEEE 802.1Xがデフォルトで有効になっています。AXIS OS 11.8以降では、デフォルトで有効になっているIEEE 802.1Xを使用する自動的モードによってMACsecに対応しています。工場出荷時の設定値でAxisデバイスを接続すると、IEEE 802.1Xネットワーク認証が実行され、成功するとMACsec Dynamic CAKモードも試行されます。



安全に保存されたAxisデバイスID(1)(IEEE 802.1AR準拠の安全なデバイスID)は、IEEE 802.1X EAP-TLSポートベースのネットワークアクセスコントロール(2)を経由して、ネットワーク(4、5)への認証に使用されます。このEAP-TLSセッションを通じてMACsecキーが自動的に交換され、安全なリンク(3)が設定されるほか、Axis装置からHPE Aruba Networkingアクセススイッチまでのすべてのネットワークトラフィックが保護されます。

IEEE 802.1AE MACsecには、HPE Aruba NetworkingアクセススイッチとClearPass Policy Manager構成の両方の準備が必要です。EAP-TLS経由のIEEE 802.1AE MACsec暗号化通信を許可する上で、Axis装置で必要な構成はありません。

HPE Aruba NetworkingアクセススイッチがMACsecによるEAP-TLSの使用をサポートしていない場合は、Pre-Shared Keyモードを使用して手動で構成できます。

HPE Aruba Networking ClearPass Policy Manager

ロールとロールマッピングポリシー

The screenshot shows the ClearPass Policy Manager interface with the URL <https://172.25.201.120/tips/tipsContent.action#tipsRoles.action>. The left sidebar shows various configuration sections like Dashboard, Monitoring, Configuration, and Administration. The main area is titled 'Roles' and contains a list of roles with descriptions. An edit dialog is open for a role named 'AxisDevice', which has a Role ID of 3001. The dialog shows the current name and allows for modification. The interface is in English.

#	Name	Description
1.	[AirGroup v1]	Role for an AirGroup protocol version 1 request
2.	[AirGroup v2]	Role for an AirGroup protocol version 2 request
3.	[Aruba TACACS+ read-only Admin]	Default role for read-only access to Aruba device
4.	[Aruba TACACS+ root Admin]	Default role for root access to Aruba device
5.	AxisDevice	Manage their own provisioned devices
6.	[BYOD Device]	Manage their own provisioned devices
7.	[Contractor]	Manage their devices, for use with MAC authentication and AirGroup sharing.
8.	[Device User]	Manage their devices, for use with MAC authentication and AirGroup sharing.
9.	[Employee]	Manage their devices, for use with MAC authentication and AirGroup sharing.
10.	[Guest]	Manage their devices, for use with MAC authentication and AirGroup sharing.
11.	[MAC Controller]	Manage their devices, for use with MAC authentication and AirGroup sharing.
12.	[Onboard iOS]	Role for an iOS device being provisioned
13.	[Onboard iPadOS]	Role for an iPadOS device being provisioned
14.	[Onboard Linux]	Role for Linux device being provisioned
15.	[Onboard macOS]	Role for a macOS device being provisioned
16.	[Onboard Windows]	Role for a Windows device being provisioned
17.	[Other]	Default role for another user or device
18.	[TACACS+ API Admin]	API administrator role for Policy Manager Admin

Axis装置の役割名を追加します。この名前は、アクセススイッチ構成のポートアクセス役割名です。

Role Mappings - Axis Role Mapping

Conditions	Role Name
1. (Authentication:Full-Username BEGINS_WITH axis-00408c)	AxisDevice
2. (Authentication:Full-Username BEGINS_WITH axis-accc8e)	AxisDevice
3. (Authentication:Full-Username BEGINS_WITH axis-b8a44f)	AxisDevice

先に作成したAxisデバイスロールに対して、Axisロールマッピングポリシーを追加します。この条件定義は、装置をAxis装置ロールにマッピングするために必要です。条件が満たされない場合、デバイスは[Guest(ゲスト)] ロールの一部になります。

デフォルトでは、AxisデバイスはEAP識別子形式"axis-serialnumber"を使用します。Axisデバイスのシリアル番号はデバイスのMACアドレスです。たとえば、「axis-b8a44f45b4e6」のようになります。

サービスの設定

Services - Axis 802.1X Wired

Conditions	Role
1. (Authentication:Full-Username BEGINS_WITH axis-00408c)	AxisDevice
2. (Authentication:Full-Username BEGINS_WITH axis-accc8e)	AxisDevice
3. (Authentication:Full-Username BEGINS_WITH axis-b8a44f)	AxisDevice

Axisデバイスのオンボーディングの接続方式としてIEEE 802.1Xを定義するサービスに、先の手順で作成したAxisロールマッピングポリシーを追加します。

The screenshot shows the ClearPass Policy Manager interface for the 'Axis 802.1X Wired' service. The 'Enforcement' tab is selected. The 'Conditions' section lists several logical AND statements involving certificate issuer and subject information, along with role and device type checks. The 'Enforcement Profiles' section shows three profiles: 'Allow_VLAN_201', 'Allow_VLAN_201', and 'Allow_VLAN_202'. At the bottom, there are buttons for 'Disable', 'Copy', 'Save', and 'Cancel'.

既存のポリシー定義に、Axis役割名を条件として追加します。

強制プロファイル

The screenshot shows the ClearPass Policy Manager interface for the 'Allow_VLAN_201' enforcement profile. The 'Profile' tab is selected. It shows the profile name is 'Allow_VLAN_201', type is 'RADIUS', and action is 'Accept'. The 'Attributes' section lists six RADIUS attributes with their values: Session-Timeout (10800), Termination-Action (RADIUS-Request (1)), Tunnel-Type (VLAN (13)), Tunnel-Medium-Type (IEEE-802 (6)), Tunnel-Private-Group-Id (201), and Aruba-User-Role (AxisDevice). At the bottom, there are buttons for 'Copy', 'Save', and 'Cancel'.

IEEE 802.1Xオンボーディングサービスで割り当てられる強制プロファイルに、Axisロール名を属性として追加します。

HPE Aruba Networkingアクセススイッチ

に記載された安全なオンボーディング設定に加えて、以下の HPE Aruba Networkingアクセススイッチのポート設定例を参照して IEEE 802.1AE MACsec を設定します。

```
macsec policy macsec-eapcipher-suite gcm-aes-128  
port-access role AxisDevice associate macsec-policy macsec-eapauth-mode client-mode  
aaa authentication port-access dot1x authenticator macsec mkacak-length 16 enable
```

レガシーオンボーディング - MAC認証

MAC Authentication Bypass (MAB) と AxisデバイスID証明書、工場出荷時の設定で有効化されているIEEE 802.1Xを使用して、IEEE 802.1ARをサポートしないAxisデバイスをオンボーディングすることができます。802.1Xオンボーディングが失敗した場合、ClearPass Policy ManagerはAxisデバイスのMACアドレスを検証し、ネットワークへのアクセスを付与します。

MABには、アクセススイッチとClearPass Policy Manager構成の両方の準備が必要です。AxisデバイスでMABによるオンボーディングを有効にするための設定は不要です。

HPE Aruba Networking ClearPass Policy Manager

強制ポリシー

ClearPass Policy Managerの強制ポリシー設定は、次の2つのサンプルポリシー条件に基づき、HPE Aruba NetworkingによるネットワークへのアクセスをAxis装置に付与するか判断します。

The screenshot shows the ClearPass Policy Manager web interface. The left sidebar navigation includes Dashboard, Monitoring, Configuration, Services, Authentication, Identity, Posture, Enforcement, Network, Administration, and Help. The main content area is titled "Services - Axis 802.1X Wired - Mac Authentication". The "Enforcement" tab is active. Under "Conditions", there is a single rule: "1. AND (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)". The "Enforcement Profiles" section shows "Allow_VLAN_203". At the bottom right, there are buttons for Enable, Copy, Save, and Cancel.

ネットワークアクセスの拒否

Axisデバイスが設定された強制ポリシーの条件を満たさない場合、ネットワークへのアクセスは拒否されます。

ゲストネットワーク (VLAN 203)

次の条件が満たされる場合、Axis装置に限定的な隔離ネットワークへのアクセスが付与されます。

- 日が平日（月曜日～金曜日）である。
- 時間が9時～17時である。
- MACアドレスのベンダーがAxis Communicationsと一致する。

MACアドレスを偽装できるため、通常のプロビジョニングネットワークへのアクセスは付与されません。MABは初回オンボーディングにのみ使用し、デバイスをさらに手動で検査することをお勧めします。

ソースの設定

[Sources (ソース)] ページでは新しい認証ソースが作成され、手動でインポートされたMACアドレスのみを許可します。

The screenshot displays two windows of the ClearPass Policy Manager web interface.

Top Window: Authentication Sources List

- Title:** ClearPass Policy Manager > Configuration > Authentication > Sources
- Content:** A table listing 11 authentication sources, each with a checkbox and a description. The sources include Admin User Repository, Denylist User Repository, Endpoints Repository, Guest Device Repository, Guest User Repository, Insight Repository, Local User Repository, Onboard Devices Repository, Social Login Repository, Time Source, and Zone Cache Repository. The last source, Zone Cache Repository, is listed as HTTP.
- Buttons:** Add, Import, Export All, Copy, Export, Delete.

Bottom Window: New Authentication Source Creation Dialog

- Title:** ClearPass Policy Manager > Configuration > Authentication > Sources > Add
- Content:**
 - General Tab:** Fields include Name (Axis Devices), Description (MAC addresses of Axis devices in use.), Type (Static Host List selected), and Use for Authorization (unchecked).
 - Static Host Lists Tab:** An empty list of authorization sources.
 - Summary Tab:** Displays the configuration details.
- Buttons:** Back to Authentication Sources, Next →, Save, Cancel.

The screenshot shows the 'ClearPass Policy Manager' interface. On the left, a navigation sidebar includes 'Dashboard', 'Monitoring', 'Configuration' (selected), 'Service Templates & Wizards', 'Services', 'Authentication' (selected), 'Identity', 'Posture', 'Enforcement', 'Network', and 'Administration'. The main content area is titled 'Authentication Sources' and shows a 'MAC Address Host Lists' section. A modal window titled 'Add Static Host List' is open, with 'Name' set to 'Axis devices', 'Host Format' set to 'List', and 'Host Type' set to 'MAC Address'. The 'Host Entries' table contains three entries:

#	Address	Description
1.	B8-A4-4F-45-B4-E6	Axis Device 1
2.	B8-A4-4F-45-B4-E7	Axis Device 2
3.	B8-A4-4F-45-B4-E8	Axis Device 3

Buttons at the bottom of the modal include 'Save Host', 'Save', and 'Cancel'.

Axis MACアドレスを含む静的ホストのリストが作成されます。

The screenshot shows the 'ClearPass Policy Manager' interface after the host list has been created. The 'List "Axis devices" added successfully' message is displayed. The 'MAC Address Host Lists' table now shows the 'Axis devices' list with options to 'Remove', 'View Details', and 'Modify'.

サービスの設定

[Services (サービス)] ページでは、設定手順がHPE Aruba Networkingネットワーク内のAxisデバイスの認証と承認を処理する1つのサービスに統合されています。

ClearPass Policy Manager

Configuration > Services

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

#	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

ClearPass Policy Manager

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

Service Rule

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

接続方式としてMABを定義する専用のAxisサービスが作成されます。

事前設定されたMAC認証方式がサービスに設定されます。また、AXISのMACアドレスのリストを含む(先に作成された)認証ソースが選択されます。

Axis Communicationsは、次のMACアドレスOUIを使用します:

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

最後のステップで、先に作成した強制ポリシーがサービスに設定されます。

HPE Aruba Networkingアクセススイッチ

に記載された安全なオンボーディング設定に加えて、以下の HPE Aruba Networkingアクセススイッチのポート設定例を参照してMABを許可します。

```
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_ja

2025-11 (M7.2)

© 2023年 – 2025 Axis Communications AB