

802.1x サプリカントとしての Lightweight アクセス ポイントの設定

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[LAP の設定](#)

[スイッチの設定](#)

[ISE サーバを設定して下さい](#)

[確認](#)

[トラブルシューティング](#)

概要

この資料に Identity Services Engine (ISE) サーバに対して認証するために 802.1X サプリカントで Lightweight アクセスポイント (LAP) を設定する方法を記述されています。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ワイヤレス LAN コントローラ (WLC) および LAP
- 802.1X on Cisco スイッチ
- ISE
- Extensible Authentication Protocol (EAP) -セキュアなトンネリング (ファースト) による適用範囲が広い認証

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- WS-C3560CX-8PC-S、15.2(4)E1
- AIR-CT-2504-K9、8.2.141.0
- ISE 2.0

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。こ

のドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

背景説明

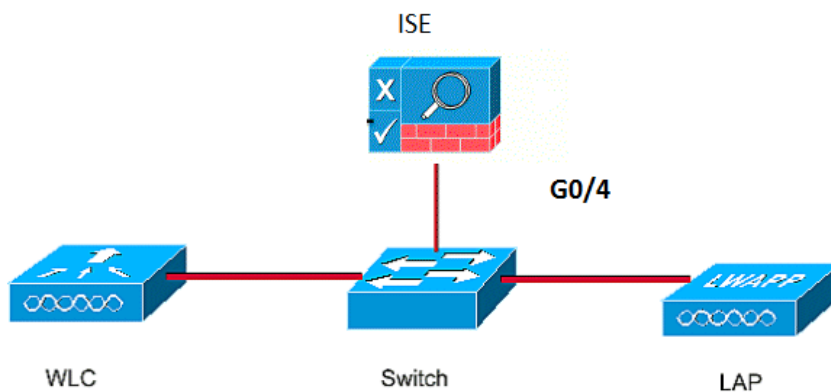
Access Point（AP）設定されるこのので 802.1X サブリカントとして機能し、EAP-FAST な匿名保護されたアクセス 資格情報（PAC）提供の使用 ISE に対するスイッチによって認証されます。ポートが 802.1X 認証のために設定されれば、スイッチはパススルーに 802.1X トラフィック以外ポートに接続されるデバイスが認証に成功するまであらゆるトラフィックにポートを与えません。AP の認証は、WLC に参加する前か、WLC に参加した後に実行できます。後者の場合、LAP が WLC に参加した後で 802.1x をスイッチに設定します。

設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。



設定

このドキュメントでは、次の IP アドレスを使用します。

- スwitchの IP アドレスは 10.48.39.141 です

- ISE サーバの IP アドレスは 10.48.39.161 です
- WLC の IP アドレスは 10.48.39.142 です

LAP の設定

このセクションでは、802.1x サプリカントとしての LAP の設定について説明しています。

1. AP が WLC に既に加わっている場合、Wireless タブは行き、AP をクリックし、フィールド先頭に立つ 802.1X サプリカント 資格情報の下で資格情報チェックしますこの AP のための 802.1X ユーザ名 および パスワードを設定 するために上書きグローバル なチェックボックスを去き。

The screenshot shows the Cisco WLC configuration interface for an AP named 'Aks_desk_3502'. The 'Wireless' tab is selected, and the '802.1x Supplicant Credentials' section is expanded. The 'Over-ride Global credentials' checkbox is checked. The 'Username' field contains 'ritmahaj', and the 'Password' and 'Confirm Password' fields are masked with dots.

またグローバルコンフィギュレーションメニューとの WLC に加入されるすべての AP のためのよくあるユーザ名 および パスワードを設定できます。

The screenshot shows the Cisco WLC configuration interface with the 'Global Configuration' menu item highlighted in the left sidebar. The main content area shows the '802.1x Supplicant Credentials' section for the AP. The '802.1x Authentication' checkbox is checked. The 'Username' field is empty, and the 'Password' and 'Confirm Password' fields are masked with dots.

2. AP が WLC にまだ加入しない場合資格情報を設定し、これらの CLI コマンドを使用するために、LAP にコンソール接続を行って下さい:

```
LAP#debug capwap console cli
LAP#capwap ap dot1x username <username> password <password>
```

スイッチの設定

1. スwitchの dot1x をグローバルに有効にし、スイッチに ISE サーバを追加して下さい。

```
aaa new-model
!
aaa authentication dot1x default group radius
!
dot1x system-auth-control
!
radius server ISE
address ipv4 10.48.39.161 auth-port 1645 acct-port 1646
key 7 123A0C0411045D5679
```

2. この場合、AP スwitchポートを設定して下さい。

```
interface GigabitEthernet0/4

switchport access vlan 231
switchport mode access
authentication order dot1x
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast edge
```

ISE サーバを設定して下さい

1. ISE サーバの認証、許可、アカウントिंग (AAA) クライアントとしてスイッチを追加して下さい。

Identity Services Engine Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Identity Mapping

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM

Network Devices List > akshat_sw

Network devices

Default Device

Network Devices

* Name: akshat_sw

Description:

* IP Address: 10.48.39.141 / 32

* Device Profile: Cisco

Model Name:

Software Version:

* Network Device Group

Location: All Locations [Set To Default]

Device Type: All Device Types [Set To Default]

RADIUS Authentication Settings

Enable Authentication Settings

Protocol: RADIUS

* Shared Secret: [Show]

Identity Services Engine Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Identity Mapping

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM

Network devices

Default Device

Network Devices

Edit Add Duplicate Import Export Generate PAC Delete

Name	IP/Mask	Profile Name	Location	Type
<input type="checkbox"/> GurpWLC1	10.48.39.155/32	Cisco	All Locations	All Device Types
<input type="checkbox"/> GurpWLC2	10.48.39.156/32	Cisco	All Locations	All Device Types
<input type="checkbox"/> akshat_sw	10.48.39.141/32	Cisco	All Locations	All Device Types

2. ISE で、認証ポリシーおよび承認ポリシーを設定して下さい。この場合、配線された dot.1x であるデフォルトの認証ルールは要件によって、1 それをカスタマイズできます使用されます。

Identity Services Engine Home Operations Policy Guest Access Administration Work

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity source. For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Policy Type Simple Rule-Based

<input checked="" type="checkbox"/>	MAB	: If Wired_MAB OR
	Wireless_MAB	Allow Protocols : Default Network Access and
<input checked="" type="checkbox"/>	Default	:use Internal Endpoints
<input checked="" type="checkbox"/>	Dot1X	: If Wired_802.1X OR
	Wireless_802.1X	Allow Protocols : Default Network Access and
<input checked="" type="checkbox"/>	Default	:use All_User_ID_Stores
<input checked="" type="checkbox"/>	Default Rule (If no match)	: Allow Protocols : Default Network Access and use : All_User_ID_Stores

EAP-FAST な デフォルトネットワーク アクセスが与えられる許可されたプロトコルでそれを確認して下さい。

Identity Services Engine Home Operations Policy Guest Access Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionary Conditions Results

Allow EAP-FAST

EAP-FAST Inner Methods

- Allow EAP-MS-CHAPv2
 - Allow Password Change Retries (Valid Range 0 to 3)
- Allow EAP-GTC
 - Allow Password Change Retries (Valid Range 0 to 3)
- Allow EAP-TLS
 - Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy
- Use PACs Don't Use PACs
 - Tunnel PAC Time To Live
 - Proactive PAC update will occur after % of PAC Time To Live has expired
 - Allow Anonymous In-Band PAC Provisioning
 - Allow Authenticated In-Band PAC Provisioning
 - Server Returns Access Accept After Authenticated Provisioning
 - Accept Client Certificate For Provisioning

3. 承認ポリシー (Port_AuthZ) に関しては、この場合 AP 資格情報はユーザグループ (AP) に追加されました。使用された条件はユーザグループ AP および配線された dot1x をすることに押します「ありましたり属したり、デフォルト許可 プロファイル割り当てアクセスを」。再度、これは要件によってカスタマイズすることができます。

Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order. For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

First Matched Rule Applies

Exceptions (0)

+ Create a New Rule

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Port_AuthZ	if APs AND Wired_802.1X	then PermitAccess

Identity Groups

- Endpoint Identity Groups
- User Identity Groups

User Identity Groups > APs

Identity Group

Name: APs
 Description: Credentials for APs

Save Reset

Member Users

Users Selected 0 | Total 1

+ Add - Delete Show All

Status	Email	Username	First Name	Last Name
<input checked="" type="checkbox"/> Enabled		ritmahaj		

確認

このセクションでは、設定が正常に機能していることを確認します。

802.1x がスイッチ ポートで有効になると、802.1x トラフィック以外のすべてのトラフィックがポートでブロックされます。WLC に既に登録されたら、引き離されて得る LAP。他のトラフィックは、802.1x 認証に成功した場合に限り、通過が許可されます。802.1x がスイッチ上で有効になった後、WLC に対して LAP の登録が成功したということは、LAP 認証が成功したことを示します。また LAP が認証したかどうか確認するためにこれらのメソッドを使用できます。

1. スイッチで、ポートが認証されるかどうか確認するために show コマンドの 1 つを入力して下さい。

```
akshat_sw#show dot1x interface g0/4
```

```
Dot1x Info for GigabitEthernet0/4
-----
PAE = AUTHENTICATOR
QuietPeriod = 60
ServerTimeout = 0
SuppTimeout = 30
ReAuthMax = 2
MaxReq = 2
TxPeriod = 30
```

```
akshat_sw#show dot1x interface g0/4 details
```

```
Dot1x Info for GigabitEthernet0/4
```

```
-----  
PAE = AUTHENTICATOR  
QuietPeriod = 60  
ServerTimeout = 0  
SuppTimeout = 30  
ReAuthMax = 2  
MaxReq = 2  
TxPeriod = 30
```

```
Dot1x Authenticator Client List
```

```
-----  
EAP Method = FAST  
Supplicant = 588d.0997.061d  
Session ID = 0A30278D000000A088F1F604  
Auth SM State = AUTHENTICATED  
Auth BEND SM State = IDLE
```

```
akshat_sw#show authentication sessions
```

```
Interface MAC Address Method Domain Status Fg Session ID  
Gi0/4 588d.0997.061d dot1x DATA Auth 0A30278D000000A088F1F604
```

2. ISE で、**オペレーション > Radius Livelogs** を選択し、認証が正常であり、正しい許可プロファイルが押されることがわかって下さい。

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles
2017-03-09 10:32:28.956	All		0	ritmahaj	58:8D:09:97:06:1D	Cisco-Device	Default >> Dot1X >> Default	Default >> Port_AuthZ	PermitAccess
2017-03-09 10:31:29.227	All		0	ritmahaj	58:8D:09:97:06:1D	Cisco-Device	Default >> Dot1X >> Default	Default >> Port_AuthZ	

トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を提供します。

1. ISE サーバがスイッチから到達可能であるかどうか確認するために ping コマンドを入力して下さい。
2. スイッチが ISE サーバの AAA クライアントで設定されることを確かめて下さい。
3. スイッチと ACS サーバの共有秘密が同一であることを確認します。
4. EAP-FAST かどうか有効にされる ISE サーバで確認して下さい。
5. 802.1X 資格情報が LAP のために設定され、ISE サーバに同じであるかどうか確認して下さい。注: ユーザ名とパスワードは大文字小文字が区別されます。
6. 認証が失敗した場合、スイッチのこれらのコマンドを入力して下さい: dot1x および debug authentication をデバッグして下さい。