

Configure Lightweight Access Point as an 802.1x Supplicant

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[Network Diagram](#)

[Configurations](#)

[Configure the LAP](#)

[Configure the Switch](#)

[Configure the ISE Server](#)

[Verify](#)

[Troubleshoot](#)

Introduction

This document describes how to configure a Lightweight Access Point (LAP) as an 802.1x supplicant in order to authenticate against the Identity Services Engine (ISE) server.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Wireless Lan Controller (WLC) and LAP
- 802.1x on Cisco switches
- ISE
- Extensible Authentication Protocol (EAP) - Flexible Authentication via Secure Tunneling (FAST)

Components Used

The information in this document is based on these software and hardware versions:

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

The information in this document was created from the devices in a specific lab environment. All of

the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Information

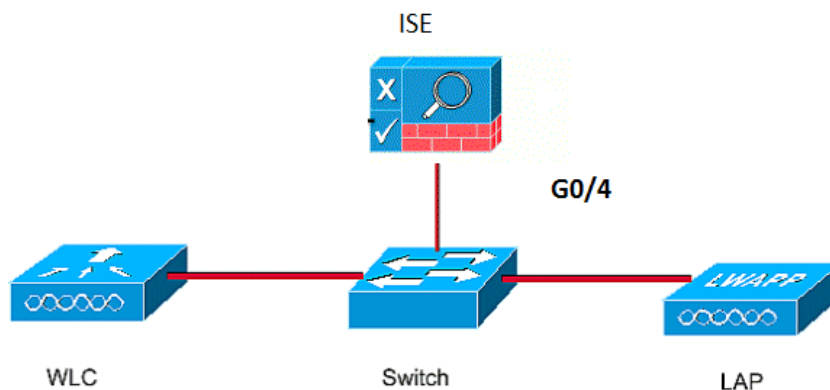
In this setup the access point (AP) acts as the 802.1x supplicant and is authenticated by the switch against the ISE that uses EAP-FAST with anonymous Protected Access Credentials (PAC) provisioning. Once the port is configured for 802.1x authentication, the switch does not allow any traffic other than 802.1x traffic to pass through the port until the device connected to the port authenticates successfully. An AP can be authenticated either before it joins a WLC or after it has joined a WLC, in which case you configure 802.1x on the switch after the LAP joins the WLC.

Configure

In this section, you are presented with the information to configure the features described in this document.

Network Diagram

This document uses this network setup:



Configurations

This document uses these IP addresses:

- IP address of the switch is 10.48.39.141

- IP address of the ISE server is 10.48.39.161
- IP address of the WLC is 10.48.39.142

Configure the LAP

In this section, you are presented with the information to configure the LAP as a 802.1x supplicant.

1. If the AP is already joined to the WLC, go the Wireless tab and click on the AP, go the Credentials field and under the 802.1x Supplicant Credentials heading, check the **Over-ride Global credentials** check box in order to set the 802.1x username and password for this AP.

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

You can also set a common username and password for all the APs that are joined to the WLC with the Global Configuration menu.

The screenshot shows the Cisco WLC configuration interface for the 'Global Configuration' menu. The 'Wireless' tab is selected, and the 'Global Configuration' menu item is highlighted. The '802.1x Supplicant Credentials' section is expanded, showing the '802.1x Authentication' checkbox checked. The 'Username', 'Password', and 'Confirm Password' fields are empty.

- If the AP has not joined a WLC yet, you must console into the LAP in order to set the credentials and use these CLI commands: `LAP#debug capwap console cli`
`LAP#capwap ap dot1x username <username> password <password>`

Configure the Switch

- Enable dot1x on the switch globally and add the ISE server to the switch. `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`
- Now, configure the AP switch port. `interface GigabitEthernet0/4`

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

Configure the ISE Server

- Add the switch as an Authentication, Authorization, and Accounting (AAA) client on the ISE server.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation is: Home > Operations > Policy > Guest Access > Administration > Work Centers. The main menu includes System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, and Identity Mapping. The current view is 'Network Devices List > akshat_sw'. The 'Network Devices' section is active, showing a list of devices on the left and a configuration form on the right. The form fields are: Name (akshat_sw), Description (empty), IP Address (10.48.39.141 / 32), Device Profile (Cisco), Model Name (empty), Software Version (empty), Network Device Group (empty), Location (All Locations), Device Type (All Device Types), and RADIUS Authentication Settings (checked, Enable Authentication Settings, Protocol RADIUS, Shared Secret masked).

Network devices

Default Device

Network Devices

* Name

Description

* IP Address: /

* Device Profile

Model Name

Software Version

* Network Device Group

Location

Device Type

RADIUS Authentication Settings

Enable Authentication Settings

Protocol **RADIUS**

* Shared Secret

Identity Services Engine Home Operations Policy Guest Access 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 Location

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. On ISE, configure the Authentication policy and Authorization policy. In this case, the default authentication rule which is wired dot.1x is used, but one can customize it as per the requirement.

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

Ensure that in the allowed protocols that Default Network Access, EAP-FAST is allowed.

Identity Services Engine Home Operations Policy Guest Access Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionary Conditions Results

Authentication

Allowed Protocols

Authorization

Profiling

Posture

Client Provisioning

Allow EAP-FAST

EAP-FAST Inner Methods

Allow EAP-MS-CHAPv2

Allow Password Change Retries 3 (Valid Range 0 to 3)

Allow EAP-GTC

Allow Password Change Retries 3 (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 90 Days

Proactive PAC update will occur after 90 % 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. As for the Authorization policy (Port_AuthZ), in this case AP credentials were added to a user group (APs). The condition used was "If the user belongs to the group AP and doing wired dot1x, then push the default Authorization Profile permit access." Again, this can be customized as per the requirement.

Identity Services Engine Home Operations Policy Guest Access Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

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
✓	Port_AuthZ	if APs AND Wired_802.1X	then PermitAccess

Identity Services Engine Home Operations Policy Guest Access Administration Work Centers

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

Identities Groups External Identity Sources Identity Source Sequences Settings

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
✓ Enabled		ritmahaj		

Verify

Use this section in order to confirm that your configuration works properly.

Once 802.1x is enabled on the switch port, all the traffic except the 802.1x traffic is blocked through the port. The LAP, which if already registered to the WLC, gets disassociated. Only after a successful 802.1x authentication is other traffic allowed to pass through. Successful registration of the LAP to the WLC after the 802.1x is enabled on the switch indicates that the LAP authentication is successful. You can also use these methods in order to verify if the LAP authenticated.

1. On the switch, enter one of the **show** commands in order to verify if the port has been authenticated or not. `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. In ISE, choose **Operations > Radius LiveLogs** and see that the authentication is successful and the correct Authorization profile is pushed.

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

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

1. Enter the **ping** command in order to check if the ISE server is reachable from the switch.
2. Make sure that the switch is configured as an AAA client on the ISE server.
3. Ensure that the shared secret is the same between switch and the ACS server.
4. Check if EAP-FAST is enabled on the ISE server.
5. Check if the 802.1x credentials are configured for the LAP and are same on the ISE server.
Note: The username and password are case sensitive.
6. If authentication fails, enter these commands on the switch: **debug dot1x** and **debug authentication**.