Configuring Local Authentication Using LDAP

Configuring Local Authentication Using LDAP

This module provides information about configuring local authentication for Cisco Identity Based Networking Services.

Information About Local Authentication Using LDAP

Local Authentication Using LDAP

Local authentication using Lightweight Directory Access Protocol (LDAP) allows an endpoint to be authenticated using 802.1X, MAC authentication bypass (MAB), or web authentication with LDAP as a backend. Local authentication in Identity-Based Networking Services also supports associating an authentication, authorization, and accounting (AAA) attribute list with the local username for wireless sessions.

How to Configure Local Authentication Using LDAP

Configuring Local Authentication Using LDAP

Perform this task to specify the AAA method list for local authentication and to associate an attribute list with a local username.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa local authentication** {*method-list-name* | **default**} **authorization** {*method-list-name* | **default**}
5. **username** *name* **aaa attribute list** *aaa-attribute-list* [**password** *password*]
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables the authentication, authorization, and accounting (AAA) access control model.
Step 4	**aaa local authentication** {*method-list-name* | **default**} **authorization** {*method-list-name* | **default**} **Example:** `Device(config)# aaa local authentication default authorization default`	Specifies the method lists to use for local authentication and authorization from a LDAP server.
Step 5	**username** *name* **aaa attribute list** *aaa-attribute-list* [**password** *password*] **Example:** `Device(config)# username USER_1 aaa attribute list LOCAL_LIST password CISCO`	Associates a AAA attribute list with a local username.
Step 6	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring MAC Filtering Support

Perform this task to set the RADIUS compatibility mode, the MAC delimiter, and the MAC address as the username to support MAC filtering.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa group server radius** *group-name*
5. **subscriber mac-filtering security-mode** {**mac** | **none** | **shared-secret**}
6. **mac-delimiter** {**colon** | **hyphen** | **none** | **single-hyphen**}
7. **exit**
8. **username** *mac-address* **mac** [**aaa attribute list** *aaa-attribute-list*]
9. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables the authentication, authorization, and accounting (AAA) access control model.
Step 4	**aaa group server radius** *group-name* **Example:** `Device(config)# aaa group server radius RAD_GROUP1`	Groups different RADIUS server hosts into distinct lists.
Step 5	**subscriber mac-filtering security-mode** {**mac** | **none** | **shared-secret**} **Example:** `Device(config-sg-radius)# subscriber mac-filtering security-mode mac`	Specifies the RADIUS compatibility mode for MAC filtering. • The default value is **none**.
Step 6	**mac-delimiter** {**colon** | **hyphen** | **none** | **single-hyphen**} **Example:** `Device(config-sg-radius)# mac-delimiter hyphen`	Specifies the MAC delimiter for RADIUS compatibility mode. • The default value is **none**.
Step 7	**exit** **Example:** `Device(config-sg-radius)# exit`	Exits server group configuration mode and returns to global configuration mode.
Step 8	**username** *mac-address* **mac** [**aaa attribute list** *aaa-attribute-list*] **Example:** `Device(config)# username 00-22-WP-EC-23-3C mac aaa attribute list AAA_list1`	Allows a MAC address to be used as the username for MAC filtering done locally.
Step 9	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Configuration Examples for Local Authentication Using LDAP

Example: Configuring Local Authentication Using LDAP

The following example shows a configuration for local authentication:

```
!
username USER_1 password 0 CISCO
username USER_1 aaa attribute list LOCAL_LIST
aaa new-model
aaa local authentication EAP_LIST authorization EAP_LIST
!
```

Example: Configuring MAC Filtering Support

The following example shows a configuration for MAC filtering:

```
username 00-22-WP-EC-23-3C mac aaa attribute list AAA_list1
!
aaa new-model
aaa group server radius RAD_GROUP1
subscriber mac-filtering security-mode mac
mac-delimiter hyphen
```

Feature Information for Local Authentication Using LDAP

This table provides release and related information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Table 1: Feature Information for Cisco Identity Based Networking Services Overview

Release	Feature Name	Feature Information
Cisco IOS XE Gibraltar 16.11.1	Local Authentication Using LDAP	Introduces support for local authentication using Lightweight Directory Access Protocol (LDAP).