# Configuring 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. This module provides information about configuring local authentication for Identity-Based Networking Services.



# Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

# Information About Local Authentication Using LDAP

## Local Authentication Using LDAP

Local authentication using LDAP allows an endpoint to be authenticated using 802.1X, MAB, or web authentication with LDAP as a backend. Local authentication also supports additional AAA attributes by associating an attribute list with a local username for wireless sessions.

# AES Key Wrap

The Advanced Encryption Standard (AES) key wrap feature makes the shared secret between the controller and the RADIUS server more secure. AES key wrap is designed for Federal Information Processing Standards (FIPS) customers and requires a key-wrap compliant RADIUS authentication server.

# 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**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **aaa new-model**<br>**Example:**<br>`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**}<br>**Example:**<br>`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*] | Associates a AAA attribute list with a local username. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`Device(config)# username USER_1 aaa attribute list LOCAL_LIST password CISCO` | |
| **Step 6** | **exit**<br>**Example:**<br>`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**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **aaa new-model**<br>**Example:**<br>`Device(config)# aaa new-model` | Enables the authentication, authorization, and accounting (AAA) access control model. |
| **Step 4** | **aaa group server radius** *group-name*<br>**Example:**<br>`Device(config)# aaa group server radius RAD_GROUP1` | Groups different RADIUS server hosts into distinct lists. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **subscriber mac-filtering security-mode** {**mac** \| **none** \| **shared-secret**}<br>**Example:**<br>`Device(config-sg-radius)# subscriber mac-filtering security-mode mac` | Specifies the RADIUS compatibility mode for MAC filtering.<br>• The default value is **none**. |
| **Step 6** | **mac-delimiter** {**colon** \| **hyphen** \| **none** \| **single-hyphen**}<br>**Example:**<br>`Device(config-sg-radius)# mac-delimiter hyphen` | Specifies the MAC delimiter for RADIUS compatibility mode.<br>• The default value is **none**. |
| **Step 7** | **exit**<br>**Example:**<br>`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*]<br>**Example:**<br>`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**<br>**Example:**<br>`Device(config)# exit` | Exits global configuration mode and returns to privileged EXEC mode. |

# Enabling AES Key Wrap

Advanced Encryption Standard (AES) key wrap makes the shared secret between the controller and the RADIUS server more secure. AES key wrap requires a key-wrap compliant RADIUS authentication server.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server host** {*hostname* | *ip-address*} **key-wrap encryption-key** *encryption-key* **message-auth-code-key** *encryption-key* [**format** {**ascii** | **hex**}]
4. **aaa new-model**
5. **aaa group server radius** *group-name*
6. **server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]
7. **key-wrap enable**
8. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable** | Enables privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`Device> enable` | • Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **radius-server host** {*hostname* \| *ip-address*} **key-wrap encryption-key** *encryption-key* **message-auth-code-key** *encryption-key* [**format** {**ascii** \| **hex**}]<br>**Example:**<br>`Device(config)# radius-server host 10.10.1.2 key-wrap encryption-key testkey99 message-auth-code-key testkey123` | Defines a RADIUS server host. |
| **Step 4** | **aaa new-model**<br>**Example:**<br>`Device(config)# aaa new-model` | Enables the authentication, authorization, and accounting (AAA) access control model. |
| **Step 5** | **aaa group server radius** *group-name*<br>**Example:**<br>`Device(config)# aaa group server radius RAD_GROUP1` | Groups different RADIUS server hosts into distinct lists. |
| **Step 6** | **server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]<br>**Example:**<br>`Device(config-sg-radius)# server 10.10.1.2` | Specifies the IP address of the RADIUS server in the server group. |
| **Step 7** | **key-wrap enable**<br>**Example:**<br>`Device(config-sg-radius)# key-wrap enable` | Enables AES key wrap for this RADIUS server. |
| **Step 8** | **end**<br>**Example:**<br>`Device(config-sg-radius)# end` | Exits server group 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
```

# Example: Configuring AES Key Wrap

The following example shows a configuration with key wrap enabled for a RADIUS server:

```
aaa new-model
aaa group server radius RAD_GROUP1
server 10.10.1.2
key-wrap enable
!
radius-server host 10.10.1.2
!
```

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Command List, All Releases |
| Identity-Based Networking Services commands | Cisco IOS Identity-Based Networking Services Command Reference |
| Address Resolution Protocol (ARP) commands | Cisco IOS IP Addressing Services Command Reference |
| ARP configuration tasks | IP Addressing - ARP Configuration Guide |
| Authentication, authorization, and accounting (AAA) configuration tasks | Authentication Authorization and Accounting Configuration Guide |
| AAA commands | Cisco IOS Security Command Reference |

### Standards and RFCs

| Standard/RFC | Title |
|---|---|
| RFC 5176 | Dynamic Authorization Extensions to RADIUS |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

# Feature Information for Local Authentication Using LDAP

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

*Table 1: Feature Information for Local Authentication Using LDAP*

| Feature Name | Releases | Feature Information |
|---|---|---|
| Local Authentication Using LDAP | Cisco IOS XE Release 3.2SE | Introduces support for local authentication using Lightweight Directory Access Protocol (LDAP).<br>In Cisco IOS XE 3.2SE, this feature is supported on the following platforms:<br>• Cisco Catalyst 3650 Series Switches<br>• Cisco Catalyst 3850 Series Switches<br>• Cisco 5700 Wireless LAN Controllers<br>The following commands were introduced or modified: **aaa local authentication**, **key-wrap enable**, **mac-delimiter**, **radius-server host**, **subscriber mac-filtering security-mode**, **username**. |