



Configuring Local EAP

- [Local EAP, on page 1](#)
- [Restrictions for Local EAP, on page 2](#)
- [Configuring Local EAP \(GUI\), on page 3](#)
- [Configuring Local EAP \(CLI\), on page 6](#)

Local EAP

Local EAP is an authentication method that allows users and wireless clients to be authenticated locally. It is designed for use in remote offices that want to maintain connectivity to wireless clients when the backend system becomes disrupted or the external authentication server goes down. When you enable local EAP, the controller serves as the authentication server and the local user database, which removes dependence on an external authentication server. Local EAP retrieves user credentials from the local user database or the LDAP backend database to authenticate users. Local EAP supports LEAP, EAP-FAST, EAP-TLS, PEAPv0/MSCHAPv2, and PEAPv1/GTC authentication between the controller and wireless clients.



Note The LDAP backend database supports these local EAP methods: EAP-TLS, EAP-FAST/GTC, and PEAPv1/GTC. LEAP, EAP-FAST/MSCHAPv2, and PEAPv0/MSCHAPv2 are also supported but only if the LDAP server is set up to return a clear-text password.



Note Cisco wireless LAN controllers support Local EAP authentication against external LDAP databases such as Microsoft Active Directory and Novell's eDirectory. For more information about configuring the controller for Local EAP authentication against Novell's eDirectory, see the [Configure Unified Wireless Network for Authentication Against Novell's eDirectory Database](http://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/112137-novell-edirectory-00.html) whitepaper at <http://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/112137-novell-edirectory-00.html>

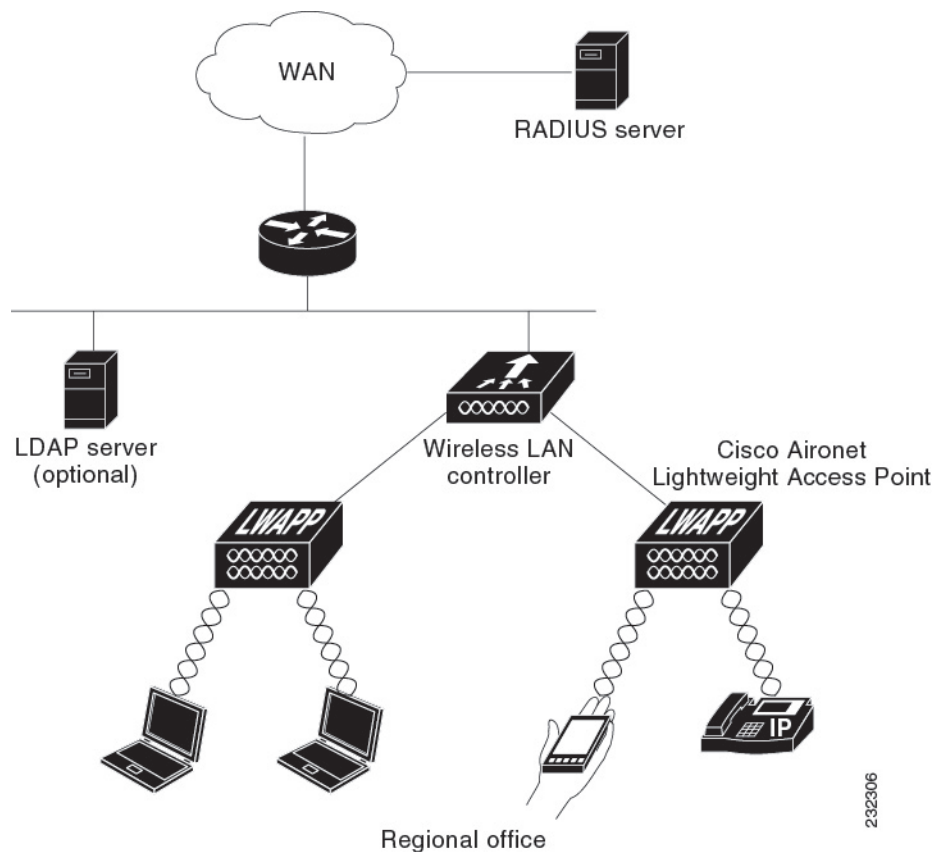


Note Local authentication with certificates of second level hierarchy (CA + intermediate CA + device) is not supported.

If any RADIUS servers are configured on the controller, the controller tries to authenticate the wireless clients using the RADIUS servers first. Local EAP is attempted only if no RADIUS servers are found, either because the RADIUS servers timed out or no RADIUS servers were configured. If four RADIUS servers are configured, the controller attempts to authenticate the client with the first RADIUS server, then the second RADIUS server, and then local EAP. If the client attempts to then reauthenticate manually, the controller tries the third RADIUS server, then the fourth RADIUS server, and then local EAP. If you never want the controller to try to authenticate clients using an external RADIUS server, enter these CLI commands in this order:

- `config wlan disable wlan_id`
- `config wlan radius_server auth disable wlan_id`
- `config wlan enable wlan_id`

Figure 1: Local EAP Example



This section contains the following subsections:

Restrictions for Local EAP

- In Release 8.6 and later releases, legacy clients that require RC4 or 3DES encryption types are not supported in Local EAP authentication.

Configuring Local EAP (GUI)

Before you begin



Note EAP-TLS, P EAPv0/MSCHAPv2, and PEAPv1/GTC use certificates for authentication, and EAP-FAST uses either certificates or PACs. The controller is shipped with Cisco-installed device and Certificate Authority (CA) certificates. However, if you want to use your own vendor-specific certificates, they must be imported on the controller.

- Step 1** If you are configuring local EAP to use one of the EAP types listed in the note above, make sure that the appropriate certificates and PACs (if you will use manual PAC provisioning) have been imported on the controller.
- Step 2** If you want the controller to retrieve user credentials from the local user database, make sure that you have properly configured the local network users on the controller.
- Step 3** If you want the controller to retrieve user credentials from an LDAP backend database, make sure that you have properly configured an LDAP server on the controller.
- Step 4** Specify the order in which user credentials are retrieved from the backend database servers as follows:
- Choose **Security > Local EAP > Authentication Priority** to open the **Priority Order > Local-Auth** page.
 - Determine the priority order in which user credentials are to be retrieved from the local and/or LDAP databases. For example, you may want the LDAP database to be given priority over the local user database, or you may not want the LDAP database to be considered at all.
 - When you have decided on a priority order, highlight the desired database. Then use the left and right arrows and the Up and Down buttons to move the desired database to the top of the right User Credentials box.
- Note** If both LDAP and LOCAL appear in the right User Credentials box with LDAP on the top and LOCAL on the bottom, local EAP attempts to authenticate clients using the LDAP backend database and fails over to the local user database if the LDAP servers are not reachable. If the user is not found, the authentication attempt is rejected. If LOCAL is on the top, local EAP attempts to authenticate using only the local user database. It does not fail over to the LDAP backend database.- Click **Apply** to commit your changes.

Step 5 Specify values for the local EAP timers as follows:

 - Choose **Security > Local EAP > General** to open the General page.
 - In the **Local Auth Active Timeout** text box, enter the amount of time (in seconds) in which the controller attempts to authenticate wireless clients using local EAP after any pair of configured RADIUS servers fails. The valid range is 1 to 3600 seconds, and the default setting is 300 seconds.

Step 6 Specify values for the Advanced EAP parameters as follows:

 - Choose **Security > Advanced EAP**.
 - In the **Identity Request Timeout** text box, enter the amount of time (in seconds) in which the controller attempts to send an EAP identity request to wireless clients using local EAP. The valid range is 1 to 120 seconds, and the default setting is 30 seconds.
 - In the **Identity Request Max Retries** text box, enter the maximum number of times that the controller attempts to retransmit the EAP identity request to wireless clients using local EAP. The valid range is 1 to 20 retries, and the default setting is 2 retries.

- d) In the **Dynamic WEP Key Index** text box, enter the key index used for dynamic wired equivalent privacy (WEP). The default value is 0, which corresponds to a key index of 1; the valid values are 0 to 3 (key index of 1 to 4).
- e) In the **Request Timeout** text box, enter the amount of time (in seconds) in which the controller attempts to send an EAP request to wireless clients using local EAP. The valid range is 1 to 120 seconds, and the default setting is 30 seconds.
- f) In the **Request Max Retries** text box, enter the maximum number of times that the controller attempts to retransmit the EAP request to wireless clients using local EAP. The valid range is 1 to 120 retries, and the default setting is 2 retries.
- g) From the **Max-Login Ignore Identity Response** drop-down list, choose **Enable** to limit the number of devices that can be connected to the controller with the same username. You can log in up to eight times from different devices (PDA, laptop, IP phone, and so on) on the same controller. The default value is enabled.
- h) In the **EAPOL-Key Timeout** text box, enter the amount of time (in seconds) in which the controller attempts to send an EAP key over the LAN to wireless clients using local EAP. The valid range is 1 to 5 seconds, and the default setting is 1 second.

Note If the controller and access point are separated by a WAN link, the default timeout of 1 second may not be sufficient.

- i) In the **EAPOL-Key Max Retries** text box, enter the maximum number of times that the controller attempts to send an EAP key over the LAN to wireless clients using local EAP. The valid range is 0 to 4 retries, and the default setting is 2 retries.
- j) In the **EAP-Broadcast Key Interval** text box, enter the interval between the Group Temporal Key (GTK) key rotation for all the stations on a BSSID that is using WPA protocol. The default interval is 3600 seconds.
- k) Click **Apply** to commit your changes.

Step 7

Create a local EAP profile, which specifies the EAP authentication types that are supported on the wireless clients as follows:

- a) Choose **Security > Local EAP > Profiles** to open the Local EAP Profiles page.

This page lists any local EAP profiles that have already been configured and specifies their EAP types. You can create up to 16 local EAP profiles.

Note If you want to delete an existing profile, hover your cursor over the blue drop-down arrow for that profile and choose **Remove**.

- b) Click **New** to open the **Local EAP Profiles > New** page.
- c) In the Profile Name text box, enter a name for your new profile and then click **Apply**.

Note You can enter up to 63 alphanumeric characters for the profile name. Make sure not to include spaces.

- d) When the Local EAP Profiles page reappears, click the name of your new profile. The **Local EAP Profiles > Edit** page appears.
- e) Select the **LEAP**, **EAP-FAST**, **EAP-TLS**, and/or **PEAP** check boxes to specify the EAP type that can be used for local authentication.

Note You can specify more than one EAP type per profile. However, if you choose multiple EAP types that use certificates (such as EAP-FAST with certificates, EAP-TLS, PEAPv0/MSCHAPv2, and PEAPv1/GTC), all the EAP types must use the same certificate (from either Cisco or another vendor).

Note If you select the **PEAP** check box, both PEAPv0/MSCHAPv2 or PEAPv1/GTC are enabled on the controller.

- f) If you chose EAP-FAST and want the device certificate on the controller to be used for authentication, select the **Local Certificate Required** check box. If you want to use EAP-FAST with PACs instead of certificates, leave this check box unselected, which is the default setting.

Note This option applies only to EAP-FAST because device certificates are not used with LEAP and are mandatory for EAP-TLS and PEAP.

- g) If you chose EAP-FAST and want the wireless clients to send their device certificates to the controller in order to authenticate, select the **Client Certificate Required** check box. If you want to use EAP-FAST with PACs instead of certificates, leave this check box unselected, which is the default setting.

Note This option applies only to EAP-FAST because client certificates are not used with LEAP or PEAP and are mandatory for EAP-TLS.

- h) If you chose EAP-FAST with certificates, EAP-TLS, or PEAP, choose which certificates will be sent to the client, the ones from **Cisco** or the ones from another **Vendor**, from the Certificate Issuer drop-down list. The default setting is Cisco.
- i) If you chose EAP-FAST with certificates or EAP-TLS and want the incoming certificate from the client to be validated against the CA certificates on the controller, select the **Check against CA certificates** check box. The default setting is enabled.
- j) If you chose EAP-FAST with certificates or EAP-TLS and want the common name (CN) in the incoming certificate to be validated against the Local Net Users configured on the controller, select the **Verify Certificate CN Identity** check box. The default setting is disabled.
- k) If you chose EAP-FAST with certificates or EAP-TLS and want the controller to verify that the incoming device certificate is still valid and has not expired, select the **Check Certificate Date Validity** check box. The default setting is enabled.

Note Certificate date validity is checked against the current UTC (GMT) time that is configured on the controller. Timezone offset will be ignored.

- l) Click **Apply** to commit your changes.

Step 8

If you created an EAP-FAST profile, follow these steps to configure the EAP-FAST parameters:

- Choose **Security > Local EAP > EAP-FAST Parameters** to open the EAP-FAST Method Parameters page.
- In the Server Key and Confirm Server Key text boxes, enter the key (in hexadecimal characters) used to encrypt and decrypt PACs.
- In the Time to Live for the PAC text box, enter the number of days for the PAC to remain viable. The valid range is 1 to 1000 days, and the default setting is 10 days.
- In the Authority ID text box, enter the authority identifier of the local EAP-FAST server in hexadecimal characters. You can enter up to 32 hexadecimal characters, but you must enter an even number of characters.
- In the Authority ID Information text box, enter the authority identifier of the local EAP-FAST server in text format.
- If you want to enable anonymous provisioning, select the **Anonymous Provision** check box. This feature allows PACs to be sent automatically to clients that do not have one during PAC provisioning. If you disable this feature, PACS must be manually provisioned. The default setting is enabled.

Note If the local and/or client certificates are required and you want to force all EAP-FAST clients to use certificates, unselect the **Anonymous Provision** check box.

- g) Click **Apply** to commit your changes.

Step 9

Enable local EAP on a WLAN as follows:

- Choose **WLANs** to open the WLANs page.
- Click the ID number of the desired WLAN.
- When the **WLANs > Edit** page appears, choose the **Security > AAA Servers** tabs to open the **WLANs > Edit (Security > AAA Servers)** page.
- Unselect the **Enabled** check boxes for Radius Authentication Servers and Accounting Server to disable RADIUS accounting and authentication for this WLAN.

- e) Select the **Local EAP Authentication** check box to enable local EAP for this WLAN.
- f) From the EAP Profile Name drop-down list, choose the EAP profile that you want to use for this WLAN.
- g) If desired, choose the LDAP server that you want to use with local EAP on this WLAN from the **LDAP Servers** drop-down lists.
- h) Click **Apply** to commit your changes.

Step 10 Click **Save Configuration** to save your changes.

Configuring Local EAP (CLI)

Before you begin



Note EAP-TLS, P EAPv0/MSCHAPv2, and PEAPv1/GTC use certificates for authentication, and EAP-FAST uses either certificates or PACbs. The controller is shipped with Cisco-installed device and Certificate Authority (CA) certificates. However, if you want to use your own vendor-specific certificates, they must be imported on the controller.

- Step 1** If you are configuring local EAP to use one of the EAP types listed in the note above, make sure that the appropriate certificates and PACs (if you will use manual PAC provisioning) have been imported on the controller.
- Step 2** If you want the controller to retrieve user credentials from the local user database, make sure that you have properly configured the local network users on the controller.
- Step 3** If you want the controller to retrieve user credentials from an LDAP backend database, make sure that you have properly configured an LDAP server on the controller.
- Step 4** Specify the order in which user credentials are retrieved from the local and/or LDAP databases by entering this command:
config local-auth user-credentials {local | ldap}
 - Note** If you enter the **config local-auth user-credentials ldap local** command, local EAP attempts to authenticate clients using the LDAP backend database and fails over to the local user database if the LDAP servers are not reachable. If the user is not found, the authentication attempt is rejected. If you enter the **config local-auth user-credentials local ldap** command, local EAP attempts to authenticate using only the local user database. It does not fail over to the LDAP backend database.
- Step 5** Specify values for the local EAP timers by entering these commands:
 - **config local-auth active-timeout** *timeout*—Specifies the amount of time (in seconds) in which the controller attempts to authenticate wireless clients using local EAP after any pair of configured RADIUS servers fails. The valid range is 1 to 3600 seconds, and the default setting is 100 seconds.
 - **config advanced eap identity-request-timeout** *timeout*—Specifies the amount of time (in seconds) in which the controller attempts to send an EAP identity request to wireless clients using local EAP. The valid range is 1 to 120 seconds, and the default setting is 30 seconds.
 - **config advanced eap identity-request-retries** *retries*—Specifies the maximum number of times that the controller attempts to retransmit the EAP identity request to wireless clients using local EAP. The valid range is 1 to 20 retries, and the default setting is 20 retries.

- **config advanced eap key-index** *index*—Specifies the key index used for dynamic wired equivalent privacy (WEP). The default value is 0, which corresponds to a key index of 1; the valid values are 0 to 3 (key index of 1 to 4).
- **config advanced eap request-timeout** *timeout*—Specifies the amount of time (in seconds) in which the controller attempts to send an EAP request to wireless clients using local EAP. The valid range is 1 to 120 seconds, and the default setting is 30 seconds.
- **config advanced eap request-retries** *retries*—Specifies the maximum number of times that the controller attempts to retransmit the EAP request to wireless clients using local EAP. The valid range is 1 to 120 retries, and the default setting is 20 retries.
- **config advanced eap eapol-key-timeout** *timeout*—Specifies the amount of time (in seconds) in which the controller attempts to send an EAP key over the LAN to wireless clients using local EAP. The valid range is 1 to 5 seconds, and the default setting is 1 second.

Note If the controller and access point are separated by a WAN link, the default timeout of 1 second may not be sufficient.

- **config advanced eap eapol-key-retries** *retries*—Specifies the maximum number of times that the controller attempts to send an EAP key over the LAN to wireless clients using local EAP. The valid range is 0 to 4 retries, and the default setting is 2 retries.
- **config advanced eap max-login-ignore-identity-response** {**enable** | **disable**}—When enabled, this command ignores the limit set for the number of devices that can be connected to the controller with the same username through 802.1x authentication. When disabled, this command limits the number of devices that can be connected to the controller with the same username. This is not applicable for web authentication users. You can log in up to eight times from different devices (PDA, laptop, IP phone, and so on) on the same controller. The default value is enabled. Use the command **config netuser maxUserLogin** to set the limit of maximum number of devices per same username.

Step 6 Create a local EAP profile by entering this command:

```
config local-auth eap-profile add profile_name
```

Note Do not include spaces within the profile name.

Note To delete a local EAP profile, enter the **config local-auth eap-profile delete** *profile_name* command.

Step 7 Add an EAP method to a local EAP profile by entering this command:

```
config local-auth eap-profile method add method profile_name
```

The supported methods are leap, fast, tls, and peap.

Note If you choose peap, both P EAPv0/MSCHAPv2 or PEAPv1/GTC are enabled on the controller.

Note You can specify more than one EAP type per profile. However, if you create a profile with multiple EAP types that use certificates (such as EAP-FAST with certificates, EAP-TLS, PEAPv0/MSCHAPv2, and PEAPv1/GTC), all of the EAP types must use the same certificate (from either Cisco or another vendor).

Note To delete an EAP method from a local EAP profile, enter the **config local-auth eap-profile method delete** *method profile_name* command.

Step 8 Configure EAP-FAST parameters if you created an EAP-FAST profile by entering this command:

```
config local-auth method fast ?
```

where ? is one of the following:

- **anon-prov** {**enable** | **disable**}—Configures the controller to allow anonymous provisioning, which allows PACs to be sent automatically to clients that do not have one during PAC provisioning.

- **authority-id** *auth_id*—Specifies the authority identifier of the local EAP-FAST server.
- **pac-ttl** *days*—Specifies the number of days for the PAC to remain viable.
- **server-key** *key*—Specifies the server key used to encrypt and decrypt PACs.

Step 9 Configure certificate parameters per profile by entering these commands:

- **config local-auth eap-profile method fast local-cert {enable | disable} profile_name**— Specifies whether the device certificate on the controller is required for authentication.

Note This command applies only to EAP-FAST because device certificates are not used with LEAP and are mandatory for EAP-TLS and PEAP.

- **config local-auth eap-profile method fast client-cert {enable | disable} profile_name**— Specifies whether wireless clients are required to send their device certificates to the controller in order to authenticate.

Note This command applies only to EAP-FAST because client certificates are not used with LEAP or PEAP and are mandatory for EAP-TLS.

- **config local-auth eap-profile cert-issuer {cisco | vendor} profile_name**—If you specified EAP-FAST with certificates, EAP-TLS, or PEAP, specifies whether the certificates that will be sent to the client are from Cisco or another vendor.
- **config local-auth eap-profile cert-verify ca-issuer {enable | disable} profile_name**—If you chose EAP-FAST with certificates or EAP-TLS, specifies whether the incoming certificate from the client is to be validated against the CA certificates on the controller.
- **config local-auth eap-profile cert-verify cn-verify {enable | disable} profile_name**—If you chose EAP-FAST with certificates or EAP-TLS, specifies whether the common name (CN) in the incoming certificate is to be validated against the CA certificates' CN on the controller.
- **config local-auth eap-profile cert-verify date-valid {enable | disable} profile_name**—If you chose EAP-FAST with certificates or EAP-TLS, specifies whether the controller is to verify that the incoming device certificate is still valid and has not expired.

Step 10 Enable local EAP and attach an EAP profile to a WLAN by entering this command:

```
config wlan local-auth enable profile_name wlan_id
```

Note To disable local EAP for a WLAN, enter the **config wlan local-auth disable wlan_id** command.

Step 11 Save your changes by entering this command:

```
save config
```

Step 12 View information pertaining to local EAP by entering these commands:

- **show local-auth config**—Shows the local EAP configuration on the controller.

```
User credentials database search order:
  Primary ..... Local DB

Timer:
  Active timeout ..... 300

Configured EAP profiles:
  Name ..... fast-cert
  Certificate issuer ..... vendor
  Peer verification options:
```



```

    Check against CA certificates ..... Enabled
    Verify certificate CN identity ..... Disabled
    Check certificate date validity ..... Enabled
EAP-FAST configuration:
    Local certificate required ..... Yes
    Client certificate required ..... Yes
    Enabled methods ..... fast
    Configured on WLANs ..... 1

Name ..... tls
Certificate issuer ..... vendor
Peer verification options:
    Check against CA certificates ..... Enabled
    Verify certificate CN identity ..... Disabled
    Check certificate date validity ..... Enabled
EAP-FAST configuration:
    Local certificate required ..... No
    Client certificate required ..... No
    Enabled methods ..... tls
    Configured on WLANs ..... 2

EAP Method configuration:
Low-Cipher Support(TLSv1.0 for local EAP).... Enabled
EAP-FAST:
    Server key ..... <hidden>
    TTL for the PAC ..... 10
    Anonymous provision allowed ..... Yes
    Accept client on auth prov ..... No
    Authority ID ..... 436973636f000000000000000000000000
    Authority Information ..... Cisco A-ID

```

- **show local-auth statistics**—Shows the local EAP statistics.
- **show local-auth certificates**—Shows the certificates available for local EAP.
- **show local-auth user-credentials**—Shows the priority order that the controller uses when retrieving user credentials from the local and/or LDAP databases.
- **show advanced eap**—Shows the timer values for local EAP.

```

EAP-Identity-Request Timeout (seconds)..... 1
EAP-Identity-Request Max Retries..... 20
EAP Key-Index for Dynamic WEP..... 0
EAP Max-Login Ignore Identity Response..... enable
EAP-Request Timeout (seconds)..... 20
EAP-Request Max Retries..... 20
EAPOL-Key Timeout (seconds)..... 1
EAPOL-Key Max Retries..... 2

```

- **show ap stats wlan *Cisco_AP***—Shows the EAP timeout and failure counters for a specific access point for each WLAN.
- **show client detail *client_mac***—Shows the EAP timeout and failure counters for a specific associated client. These statistics are useful in troubleshooting client association issues.

```

...
Client Statistics:
    Number of Bytes Received..... 10
    Number of Bytes Sent..... 10
    Number of Packets Received..... 2
    Number of Packets Sent..... 2
    Number of EAP Id Request Msg Timeouts..... 0
    Number of EAP Id Request Msg Failures..... 0
    Number of EAP Request Msg Timeouts..... 2

```

```

Number of EAP Request Msg Failures..... 1
Number of EAP Key Msg Timeouts..... 0
Number of EAP Key Msg Failures..... 0
Number of Policy Errors..... 0
Radio Signal Strength Indicator..... Unavailable
Signal to Noise Ratio..... Unavailable

```

- **show wlan *wlan_id***—Shows the status of local EAP on a particular WLAN.

Step 13 (Optional) Troubleshoot local EAP sessions by entering these commands:

- **debug aaa local-auth eap method {all | errors | events | packets | sm} {enable | disable}**— Enables or disables debugging of local EAP methods.
- **debug aaa local-auth eap framework {all | errors | events | packets | sm} {enable | disable}**— Enables or disables debugging of the local EAP framework.

Note In these two debug commands, **sm** is the state machine.

- **clear stats local-auth**—Clears the local EAP counters.
- **clear stats ap wlan *Cisco_AP***—Clears the EAP timeout and failure counters for a specific access point for each WLAN.

```

WLAN      1
  EAP Id Request Msg Timeouts..... 0
  EAP Id Request Msg Timeouts Failures..... 0
  EAP Request Msg Timeouts..... 2
  EAP Request Msg Timeouts Failures..... 1
  EAP Key Msg Timeouts..... 0
  EAP Key Msg Timeouts Failures..... 0
WLAN      2
  EAP Id Request Msg Timeouts..... 1
  EAP Id Request Msg Timeouts Failures..... 0
  EAP Request Msg Timeouts..... 0
  EAP Request Msg Timeouts Failures..... 0
  EAP Key Msg Timeouts..... 3
  EAP Key Msg Timeouts Failures..... 1

```
