



Configuring an Access Point as a Local Authenticator

This chapter describes how to configure the access point as a local authenticator to serve as a stand-alone authenticator for a small wireless LAN or to provide backup authentication service. As a local authenticator, the access point performs both LEAP and MAC-based authentication for up to 50 client devices. This chapter contains these sections:

- [Understanding Local Authentication, page 8-2](#)
- [Configuring a Local Authenticator, page 8-2](#)

Understanding Local Authentication

Many small wireless LANs that could be made more secure with 802.1x authentication do not have access to a RADIUS server. On many wireless LANs that use 802.1x authentication, access points rely on RADIUS servers housed in a distant location to authenticate client devices, and the authentication traffic must cross a WAN link. If the WAN link fails, or if the access points cannot access the RADIUS servers for any reason, client devices cannot access the wireless network even if the work they wish to do is entirely local.

To provide local authentication service or backup authentication service in case of a WAN link or a server failure, you can configure an access point to act as a local authentication server. The access point can authenticate up to 50 wireless client devices using LEAP or MAC-based authentication. The access point performs up to 5 authentications per second.

You configure the local authenticator access point manually with client usernames and passwords because it does not synchronize its database with the main RADIUS servers. You can also specify a VLAN and a list of SSIDs that a client is allowed to use.



Note If your wireless LAN contains only one access point, you can configure the access point as both the 802.1x authenticator and the local authenticator. However, users associated to the local authenticator access point might notice a drop in performance when the access point authenticates client devices.

You can configure your access points to use the local authenticator when they cannot reach the main servers, or you can configure your access points to use the local authenticator or as the main authenticator if you do not have a RADIUS server. When you configure the local authenticator as a backup to your main servers, the access points periodically check the link to the main servers and stop using the local authenticator automatically when the link to the main servers is restored.

**Caution**

The access point you use as an authenticator contains detailed authentication information for your wireless LAN, so you should secure it physically to protect its configuration.

Configuring a Local Authenticator

This section provides instructions for setting up an access point as a local authenticator and includes these sections:

- [Guidelines for Local Authenticators, page 8-3](#)
- [Configuration Overview, page 8-3](#)
- [Configuring the Local Authenticator Access Point, page 8-3](#)
- [Configuring Other Access Points to Use the Local Authenticator, page 8-6](#)
- [Unblocking Locked Usernames, page 8-7](#)
- [Viewing Local Authenticator Statistics, page 8-7](#)
- [Using Debug Messages, page 8-7](#)

Guidelines for Local Authenticators

Follow these guidelines when configuring an access point as a local authenticator:

- Use an access point that does not serve a large number of client devices. When the access point acts as an authenticator, performance might degrade for associated client devices.
- Secure the access point physically to protect its configuration.

Configuration Overview

You complete four major steps when you set up a local authenticator:

1. On the local authenticator, create a list of access points authorized to use the authenticator to authenticate client devices. Each access point that uses the local authenticator is a Network Access Server (NAS).



Note If your local authenticator access point also serves client devices, you must enter the local authenticator access point as a NAS. When a client associates to the local authenticator access point, the access point uses itself to authenticate the client.

2. On the local authenticator, create user groups and configure parameters to be applied to each group (optional).
3. On the local authenticator, create a list of up to 50 LEAP users or MAC addresses that the local authenticator is authorized to authenticate.
4. On the access points that use the local authenticator, enter the local authenticator as a RADIUS server.



Note If your local authenticator access point also serves client devices, you must enter the local authenticator as a RADIUS server in the local authenticator's configuration. When a client associates to the local authenticator access point, the access point uses itself to authenticate the client.

Configuring the Local Authenticator Access Point

Beginning in Privileged Exec mode, follow these steps to configure the access point as a local authenticator:

	Command	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>aaa new-model</code>	Enable AAA.
Step 3	<code>radius-server local</code>	Enable the access point as a local authenticator and enter configuration mode for the authenticator.

	Command	Purpose
Step 4	nas <i>ip-address</i> key <i>shared-key</i>	<p>Add an access point to the list of units that use the local authenticator. Enter the access point's IP address and the shared key used to authenticate communication between the local authenticator and other access points. You must enter this shared key on the access points that use the local authenticator. If your local authenticator also serves client devices, you must enter the local authenticator access point as a NAS.</p> <p>Note Leading spaces in the key string are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key.</p> <p>Repeat this step to add each access point that uses the local authenticator.</p>
Step 5	group <i>group-name</i>	(Optional) Enter user group configuration mode and configure a user group to which you can assign shared settings.
Step 6	vlan <i>vlan</i>	(Optional) Specify a VLAN to be used by members of the user group. The access point moves group members into that VLAN, overriding other VLAN assignments. You can assign only one VLAN to the group.
Step 7	ssid <i>ssid</i>	(Optional) Enter up to 20 SSIDs to limit members of the user group to those SSIDs. The access point checks that the SSID that the client used to associate matches one of the SSIDs in the list. If the SSID does not match, the client is disassociated.
Step 8	reauthentication time <i>seconds</i>	(Optional) Enter the number of seconds after which access points should reauthenticate members of the group. The reauthentication provides users with a new encryption key. The default setting is 0, which means that group members are never required to reauthenticate.
Step 9	lockout count <i>count</i> time { <i>seconds</i> infinite }	<p>(Optional) To help protect against password guessing attacks, you can lock out group members for a length of time after a set number of incorrect passwords.</p> <ul style="list-style-type: none"> count—The number of failed passwords that triggers a lockout of the user name. time—The number of seconds the lockout should last. If you enter infinite, an administrator must manually unblock the locked user name. See the “Unblocking Locked Usernames” section on page 8-7 for instructions on unblocking client devices.
Step 10	exit	Exit group configuration mode and return to authenticator configuration mode.

	Command	Purpose
Step 11	user <i>username</i> { password nthash } <i>password</i> [group <i>group-name</i>]	Enter the users allowed to authenticate using the local authenticator. You must enter a user name and password for each user. If you only know the NT value of the password, which you can often find in the authentication server database, you can enter the NT hash as a string of hexadecimal digits. To add a client device for MAC-based authentication, enter the client's MAC address as both the username and password. To add the user to a user group, enter the group name. If you do not specify a group, the user is not assigned to a specific VLAN and is never forced to reauthenticate.
Step 12	end	Return to privileged EXEC mode.
Step 13	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to set up a local authenticator used by three access points with three user groups and several users:

```

AP# configure terminal
AP(config)# radius-server local
AP(config-radsrv)# nas 10.91.6.159 key 110337
AP(config-radsrv)# nas 10.91.6.162 key 110337
AP(config-radsrv)# nas 10.91.6.181 key 110337
AP(config-radsrv)# group clerks
AP(config-radsrv-group)# vlan 87
AP(config-radsrv-group)# ssid batman
AP(config-radsrv-group)# ssid robin
AP(config-radsrv-group)# reauthentication time 1800
AP(config-radsrv-group)# lockout count 2 time 600
AP(config-radsrv-group)# group cashiers
AP(config-radsrv-group)# vlan 97
AP(config-radsrv-group)# ssid deer
AP(config-radsrv-group)# ssid antelope
AP(config-radsrv-group)# ssid elk
AP(config-radsrv-group)# reauthentication time 1800
AP(config-radsrv-group)# lockout count 2 time 600
AP(config-radsrv-group)# group managers
AP(config-radsrv-group)# vlan 77
AP(config-radsrv-group)# ssid mouse
AP(config-radsrv-group)# ssid chipmunk
AP(config-radsrv-group)# reauthentication time 1800
AP(config-radsrv-group)# lockout count 2 time 600
AP(config-radsrv-group)# exit
AP(config-radsrv)# user jsmith password twain74 group clerks
AP(config-radsrv)# user stpatrick password snake100 group clerks
AP(config-radsrv)# user nick password uptown group clerks
AP(config-radsrv)# user 00095125d02b password 00095125d02b group cashiers
AP(config-radsrv)# user 00079431f04a password 00079431f04a group cashiers
AP(config-radsrv)# user carl password 272165 group managers
AP(config-radsrv)# user vic password lid178 group managers
AP(config-radsrv)# end

```

Configuring Other Access Points to Use the Local Authenticator

You add the local authenticator to the list of servers on the access point the same way that you add other servers. For detailed instructions on setting up RADIUS servers on your access points, see [Chapter 12, “Configuring RADIUS and TACACS+ Servers.”](#)



Note

If your local authenticator access point also serves client devices, you must configure the local authenticator to use itself to authenticate client devices.

On the access points that use the local authenticator, use the **radius-server host** command to enter the local authenticator as a RADIUS server. The order in which the access point attempts to use the servers matches the order in which you enter the servers in the access point configuration. If you are configuring the access point to use RADIUS for the first time, enter the main RADIUS servers first, and enter the local authenticator last.



Note

You must enter **1812** as the authentication port and **1813** as the accounting port. The local authenticator listens on UDP port 1813 for RADIUS accounting packets. It discards the accounting packets but sends acknowledge packets back to RADIUS clients to prevent clients from assuming that the server is down.

Use the **radius-server deadtime** command to set an interval during which the access point does not attempt to use servers that do not respond, thus avoiding the wait for a request to time out before trying the next configured server. A server marked as dead is skipped by additional requests for the duration of minutes that you specify, up to 1440 (24 hours).

This example shows how to set up two main servers and a local authenticator with a server deadtime of 10 minutes:

```
AP(config)# aaa new-model
AP(config)# radius-server host 172.20.0.1 auth-port 1000 acct-port 1001 key 77654
AP(config)# radius-server host 172.10.0.1 auth-port 1645 acct-port 1646 key 77654
AP(config)# radius-server host 10.91.6.151 auth-port 1812 acct-port 1813 key 110337
AP(config)# radius-server deadtime 10
```

In this example, if the WAN link to the main servers fails, the access point completes these steps when a LEAP-enabled client device associates:

1. It tries the first server, times out multiple times, and marks the first server as dead.
2. It tries the second server, times out multiple times, and marks the second server as dead.
3. It tries and succeeds using the local authenticator.

If another client device needs to authenticate during the 10-minute dead-time interval, the access point skips the first two servers and tries the local authenticator first. After the dead-time interval, the access point tries to use the main servers for authentication. When setting a dead time, you must balance the need to skip dead servers with the need to check the WAN link and begin using the main servers again as soon as possible.

Each time the access point tries to use the main servers while they are down, the client device trying to authenticate might report an authentication timeout. The client device retries and succeeds when the main servers time out and the access point tries the local authenticator. You can extend the timeout value on Cisco client devices to accommodate expected server timeouts.

To remove the local authenticator from the access point configuration, use the **no radius-server host hostname | ip-address** global configuration command.

Unblocking Locked Usernames

You can unblock usernames before the lockout time expires, or when the lockout time is set to infinite. In Privileged Exec mode on the local authenticator, enter this command to unblock a locked username:

```
AP# clear radius local-server user username
```

Viewing Local Authenticator Statistics

In privileged exec mode, enter this command to view statistics collected by the local authenticator:

```
AP# show radius local-server statistics
```

This example shows local authenticator statistics:

```
Successes           : 0           Unknown usernames   : 0
Client blocks       : 0           Invalid passwords   : 0
Unknown NAS         : 0           Invalid packet from NAS: 0

NAS : 10.91.6.158
Successes           : 0           Unknown usernames   : 0
Client blocks       : 0           Invalid passwords   : 0
Corrupted packet    : 0           Unknown RADIUS message : 0
No username attribute : 0       Missing auth attribute : 0
Shared key mismatch : 0           Invalid state attribute: 0
Unknown EAP message : 0           Unknown EAP auth type : 0

Username           Successes  Failures  Blocks
nicky              0         0         0
jones              0         0         0
jsmith            0         0         0
```

The first section of statistics lists cumulative stats from the local authenticator. The second section lists stats for each access point (NAS) authorized to use the local authenticator. The third section lists stats for individual users. If a user is blocked and the lockout time is set to infinite, *blocked* appears at the end of the stat line for that user. If the lockout time is not infinite, *Unblocked in x seconds* appears at the end of the stat line for that user.

Use this privileged exec mode command to reset local authenticator statistics to zero:

```
AP# clear radius local-server statistics
```

Using Debug Messages

In privileged exec mode, enter this command to control the display of debug messages for the local authenticator:

```
AP# debug radius local-server { packets | error | client }
```

Use the command options to display this debug information:

- Use the **packets** option to turn on display of the content of RADIUS packets sent and received.
- Use the **error** option to display error messages related to the local authenticator.
- Use the **client** option to display error messages related to failed client authentications.

