Wireless AAA Authentication Survivability Cache

Feature history for wireless AAA authentication survivability cache

This table provides release and related information about the feature explained in this section.

This feature is also available in all the releases subsequent to the one in which they are introduced in, unless noted otherwise.

Table 1: Feature history for wireless AAA authentication survivability cache

Release	Feature Information
Cisco IOS XE 17.18.1	The Wireless AAA authentication survivability cache feature enhances the reliability of wireless client authentication by storing successful authentication results locally on the controller. Cache can be used: • When the controller loses connectivity with the AAA server, which may disconnect authenticated clients. • As the primary source of authentication, with fallback to AAA, to avoid slow authentication time due to WAN latency. This feature is supported in both local mode and FlexConnect central authentication mode.

Wireless AAA authentication survivability cache

The Wireless AAA authentication survivability cache feature enhances the reliability of wireless client authentication by storing successful authentication results locally on the controller. This cache includes details such as the client's MAC address, user name, hashed password, and Attribute-Value Pairs (AVPs) received from the RADIUS server.

Wireless AAA authentication survivability cache is a mechanism implemented in the controller that:

- provides a fallback methodology in wireless systems for AAA authentication servers,
- implements authentication and policy caching mechanism, and
- leverages the caching capability of the AAA module of System Management Daemon (SMD) in WNCd.

This feature is supported in both local mode and FlexConnect central authentication mode.

Wireless AAA authentication survivability cache as failover mechanism

If the AAA server becomes unreachable, for example, due to a network outage or server failure, the controller uses the cached credentials to authenticate clients. This ensures that the previously authenticated clients are allowed network access, even if the primary authentication source is unavailable.

Use case for wireless AAA authentication survivability cache

Some use cases for the wireless AAA authentication survivability cache feature are:

- Cache can be used when the controller loses connectivity with the AAA server, which may disconnect authenticated clients.
- Cache can be used as the primary source of authentication, with fallback to AAA, to avoid slow authentication time due to WAN latency.

Benefits of using AAA cache for failover

The benefits of using AAA cache for failover are:

- Seamless client access: If the AAA server fails, previously authenticated clients can still access the network without delays or disruptions.
- Reduced dependency on AAA server availability: This mechanism reduces the dependency on the availability of the AAA server for re-authentication, providing business continuity even if there is an issue with the server.
- Improved user experience: Clients do not experience interruptions when reconnecting, as the controller uses the cached authentication information to grant them access immediately.
- Load reduction on AAA server: During network failures or outages, the controller does not need to query the AAA server repeatedly for authentication. This helps reduce the load on the AAA server.
- Failover for high availability: If the primary AAA server temporarily fails, such as during maintenance, the AAA cache maintains client access automatically.

Configure wireless AAA authentication survivability cache

Before you begin

Ensure that the following are met:

- SSID already configured
- A RADIUS server such as Cisco ISE with authentication and authorization policy and profiles are created

Configure a cache profile and apply the cache profile to the AAA server group used for authentication and authorization.

Procedure

Step 1 Enter configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure a profile for the local RADIUS server.

Example:

```
Device# aaa server radius dynamic-author
```

This command creates the profile for local RADIUS server and enters into the local server dynamic author RADIUS configuration.

Step 3 Configure a RADIUS client.

Example:

```
Device(config-locsvr-da-radius)# client {A.B.C.D | X:X:X:X::X} server-key {{0 | 6 |
7}server-key | server-key2}
```

This command specifies the IPv4 or the IPv6 address of the RADIUS client and the RADIUS client server key.

Step 4 Specify the server authorization type.

Example:

```
Device(config-locsvr-da-radius)# auth-type {all | any | sessionkey}
```

Step 5 Exit the local server dynamic author configuration mode.

Example:

```
Device(config-locsvr-da-radius)# exit
```

Configure RADIUS dynamic-author for CoA

Follow these steps to configure RADIUS dynamic-author for CoA:

Procedure

Step 1 Enter configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure a profile for the local RADIUS server.

Example:

```
Device# aaa server radius dynamic-author
```

This command creates the profile for local RADIUS server and enters into the local server dynamic author RADIUS configuration.

Step 3 Configure a RADIUS client.

Example:

```
Device(config-locsvr-da-radius)# client {A.B.C.D | X:X:X:X::X} server-key {{0 | 6 |
7}server-key | server-key2}
```

This command specifies the IPv4 or the IPv6 address of the RADIUS client and the RADIUS client server key.

Step 4 Specify the server authorization type.

Example:

```
Device(config-locsvr-da-radius)# auth-type {all | any | sessionkey}
```

Step 5 Exit the local server dynamic author configuration mode.

Example:

```
Device(config-locsvr-da-radius)# exit
```

The RADIUS client is configured.

Example

```
Device# configure terminal
Device# aaa server radius dynamic-author
Device(config-locsvr-da-radius)# client 10.10.10.1 server-key 0 server-key | server-key2}
Device(config-locsvr-da-radius)# auth-type any
Device(config-locsvr-da-radius)# exit
```

What to do next

Configure the RADIUS server.

Configure RADIUS server

Procedure

Step 1 Enter configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the RADIUS server.

Example:

```
Device(config)# radius server radius-server-name
```

This command configures the RADIUS server and enters the RADIUS server configuration mode.

Step 3 Configure the RADIUS server address.

Example:

```
Device(config-radius-server)# address ipv4 hostname or A.B.C.D [auth-port | alias | acct-port]
 <0-65534> [acct-port] <0-65534>
```

This command configures the RADIUS server address and the UDP ports for the RADIUS authentication server and accounting server.

The default port number for the RADIUS accounting server is 1813 and the default port number for the RADIUS authentication server is 1814.

Step 4 Configure the per server encryption key.

Example:

```
Device(config-radius-server)# key key
```

The RADIUS server is configured.

Example

```
Device# configure terminal
Device(config)# radius server radius-server-name
Device(config-radius-server)# address ipv4 hostname auth-port 1645 acct-port 1646
Device(config-radius-server)# key key
```

What to do next

Configure the RADIUS server group and cache expiry.

Configure RADIUS server group and cache expiry

Before you begin

Note Only one AAA server group can be configured for AAA cache feature.

Procedure

Step 1 Enter configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the RADIUS server group definition.

Example:

```
Device(config)# aaa group server {ldap | radius | tacacs+} server-group-name
```

This command configures the server group name with 32 as the maximum string length. Here, configure the RADIUS server group name.

Step 3 Configure the RADIUS server name.

Example:

```
Device(config-sg-radius)# server {hostmame or A.B.C.D | name} server-name
```

Step 4 Configure the cache authorization profile.

Example:

```
Device(config-sg-radius)# cache authorization profile cache-auth
```

Step 5 Configure the cache authentication profile.

Example:

```
Device(config-sg-radius)# cache authentication profile cache-auth
```

Step 6 Configure the cache expiry.

Example:

```
Device(config-sg-radius)# cache expiry 0-2147483647
```

This command configures the cache expiry time in hours. The default is 24 hours. The value 0 stands for never expire.

Note
If the cache entry expires and the AAA server is still unreachable, the client is not authenticated until the server is reachable again.

Step 7 Exit the RADIUS server configuration mode.

Example:

```
Device(config-sg-radius)# exit
```

The RADIUS server group and cache profile is configured.

Example

```
Device# configure terminal
Device(config)# aaa group server radius radius-group
Device(config-sg-radius)# server name server-name
Device(config-radius-server)# cache authorization profile cache-auth
Device(config-sg-radius)# cache authentication profile cache-auth
Device(config-sg-radius)# cache expiry 24
Device(config-sg-radius)# exit
```

What to do next

Configure AAA for network access using a cache profile.

Configure AAA cache profile

Procedure

Step 1 Enter configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the AAA cache profile.

Example:

```
Device(config)# aaa cache profile aaa-cache
```

Step 3 Cache all entries.

Example:

```
Device(config-profile-map)# all
```

The cache profile is configured.

Example

```
Device# configure terminal
Device(config)# aaa cache profile aaa-cache
Device(config-profile-map)# all
```

What to do next

Configure EAP profile.

Configure EAP profile

Procedure

Step 1 Enter configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure EAP profile.

Example:

```
Device(config)# eap profile eap-profile
```

Step 3 Configure EAP-TLS allowed method.

Example:

```
Device(config-eap-profile)# method tls
```

Step 4 Configure the default PKI trustpoint.

Example:

```
Device(config-eap-profile)# pki-trustpoint pki_trustpoint_name
```

Here, you must specify the name of the PKI trustpoint.

The EAP profile is configured.

Example

```
Device# configure terminal
Device(config)# eap profile eap-profile
Device(config-eap-profile)# method tls
Device(config-eap-profile)# pki-trustpoint default-pki-trustpoint
```

What to do next

Configure WLAN.

Configure WLAN

Procedure

Step 1 Enter configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure a WLAN profile.

Example:

```
Device(config)# wlan wlan-profile 1-4096 ssid-name
```

This command configures a WLAN profile and enters the WLAN configuration mode.

Step 3 Enable local auth EAP profile.

Example:

```
Device(config-wlan)# local-auth eap-profile
```

Step 4 Enable security authentication list for dot1x security.

Example:

```
Device(config-wlan)# security dot1x authentication-list default
```

Step 5 Enable security authorization list for dot1x security.

Example:

```
Device(config-wlan)# security dot1x authorization-list default
```

Step 6 Enable WLAN.

Example:

```
Device(config-wlan)# no shutdown
```

A WLAN profile is configured.

Example

```
Device# configure terminal
Device(config)# wlan wlan-profile 2 ssid-name
Device(config-wlan)# security dot1x authentication-list default
Device(config-wlan)# security dot1x authorization-list default
Device(config-wlan)# no shutdown
```

AAA dead-server detection

AAA dead-server detection allows you to configure the criteria to be used to mark a RADIUS server as dead. If you have more than one RADIUS server, the following concepts come into picture:

- Deadtime: Defines the time in minutes a server marked as DEAD is held in that state. Once the deadtime expires, the controller marks the server as UP (ALIVE) and notifies the registered clients about the state change. If the server is still unreachable after the state is marked as UP and if the DEAD criteria is met, then server is marked as DEAD again for the deadtime interval.

  For example, `Device(config)# radius-server deadtime 5`.

Note You can configure deadtime for each server group or on a global level.

- Dead-criteria—To declare a server as DEAD, you need to configure dead-criteria and configure the conditions that determine when a RADIUS server is considered unavailable or dead.

  For example, `Device(config)# radius-server dead-criteria time 5 tries 5.`

Using AAA dead-server detection will result in less deadtime and quicker packet processing.

For more information, see the chapter AAA Dead-Server Detection.

RADIUS configuration for MSCHAPv2

Configure AV-pair attribute on RADIUS

Associate the following Cisco AV-pairs with the authorization profile associated with the client, on the ISE server:

- cisco-av-pair = AS-Username=Cisco
- cisco-av-pair = AS-Credential-Hash=F2E787D376CBF6D6DD3600132E9C215D

Note Every user must configure the AV-pair attribute on RADIUS.

The Password or AS-Credential-Hash should be in the NT-hash format (https://codebeautify.org/ntlm-hash-generator).

Configure EAP-TLS on ISE

1. Generate a CSR and the import certificate into the controller (PCKS 12 or .pkg would be convenient to import as a single file).
2. Configure a PKI trustpoint in the EAP profile as described in .

Verify wireless AAA authentication survivability cache

Verify configured cache entries

To verify the configured cache entries, run the **show aaa cache group** command.

Note This command is extended to show cache entries for the Wireless Network Controller Daemon (WNCD) process.

```
Device# show aaa cache group aaa-cache-grp all
-----------------------------------------------------------
IOSD AAA Auth Cache entries:
Entries in Profile dB aaa-cache-grp for exact match:
```

```
No entries found in Profile dB
------------------------------------------------------------
SMD AAA Auth Cache entries:
Total number of Cache entries is 0
WNCD AAA Auth Cache entries:
MAC ADDR: 0000.AAAA.BBBB
Profile Name: NEWCACHE
User Name: user1
Timeout: 3600
Created Timestamp: 03/12/25 17:11:23 UTC
Server IP Address: 1.1.1.1
MAC ADDR: AAAA.BBBB.CCCC
Profile Name: NEWCACHE
User Name: user2
Timeout: 3600
Created Timestamp: 03/12/25 17:04:59 UTC
Server IP Address: 1.1.1.1
Total number of Cache entries is 2
------------------------------------------------------------
```