Local EAP Ciphersuite

Information About Local EAP Ciphersuite

Prior to Cisco IOS XE Cupertino 17.7.1 Release, the controller acts as an SSL server supporting a hardcoded list of ciphersuites for each EAP application. From Cisco IOS XE Cupertino 17.7.1 Release onwards, the controller is equipped with a knob that controls the list of ciphersuites when using local authentication.

The following table lists the hardcoded list of ciphersuites:

Table 1: Hardcoded List of Ciphersuites

Ciphersuites	Description
aes128-sha	Encryption Type tls_rsa_with_aes_128_cbc_sha.
aes256-sha	Encryption Type tls_rsa_with_aes_256_cbc_sha.
dhe-rsa-aes-gcm-sha2	Encryption Type tls_dhe_rsa_with_aes_128_gcm_sha256 and tls_dhe_rsa_with_aes_256_gcm_sha384(TLS1.2 and above).
dhe-rsa-aes-sha2	Encryption Type tls_dhe_rsa_with_aes_128_cbc_sha256 and tls_dhe_rsa_with_aes_256_cbc_sha256 (TLS 1.2 and above).
dhe-rsa-aes128-sha	Encryption Type tls_dhe_rsa_with_aes_128_cbc_sha.
dhe-rsa-aes256-sha	Encryption Type tls_dhe_rsa_with_aes_256_cbc_sha.
ecdhe-ecdsa-aes-gcm-sha2	Encryption Type tls_ecdhe_ecdsa_with_aes_128_gcm_sha256 and tls_ecdhe_ecdsa_with_aes_256_gcm_sha384(TLS1.2 and above).

Ciphersuites	Description
ecdhe-ecdsa-aes-sha	Encryption Type tls_ecdhe_ecdsa_with_aes_128_cbc_sha and tls_ecdhe_ecdsa_with_aes_256_cbc_sha.
ecdhe-ecdsa-aes-sha2	Encryption Type tls_ecdhe_ecdsa_with_aes_128_cbc_sha256 and tls_ecdhe_ecdsa_with_aes_256_cbc_sha384(TLS1.2 and above).
ecdhe-rsa-aes-gcm-sha2	Encryption Type tls_ecdhe_rsa_with_aes_128_gcm_sha256 and tls_ecdhe_rsa_with_aes_256_gcm_sha384(TLS1.2 and above).
ecdhe-rsa-aes-sha	Encryption Type tls_ecdhe_rsa_with_aes_128_cbc_sha and tls_ecdhe_rsa_with_aes_256_cbc_sha.
ecdhe-rsa-aes-sha2	Encryption Type tls_ecdhe_rsa_with_aes_128_cbc_sha256 and tls_ecdhe_rsa_with_aes_256_cbc_sha384(TLS1.2 and above).

When the Client and Server Hello messages are exchanged, the client sends a prioritized list of ciphersuites it supports in Client Hello. The server then responds with the ciphersuite selected from the list in Server Hello. The server needs to select a ciphersuite that is acceptable to both the client and server. Using this approach, only one ciphersuite is selected and sent to the client.

The Local EAP ciphersuite feature controls the list of ciphersuites the controller as SSL server supports.

Note By default, all the ciphersuites are supported. Using the Local EAP ciphersuite feature, you can enable or disable the ciphersuites based on your requirement.

Restrictions for Local EAP Ciphersuite

- SNMP is not supported.
- Ciphersuites are specific to Dot1x.

Configuring Local EAP Ciphersuite (CLI)

Procedure

	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	**eap profile** *name* **Example:** `Device(config)# eap profile local_EAP_TLSv1`	Creates an EAP profile.
Step 4	**ciphersuite** *cipher-suite* **Example:** `Device(config-eap-profile)# ciphersuite <cipher-suite>`	Select a ciphersuite. **Note** Using this command, you will be able to configure only one ciphersuite. To configure more than one ciphersuite, you need to issue this command with various ciphersuites. To remove the ciphersuites, you need to remove the ciphersuites one by one or all at once. By default all ciphersuites are supported, if you issue the **no ciphersuite** command.
Step 5	**end** **Example:** `Device(config-eap-profile)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.