To create an IKE policy by using the Cisco IOS command line

At the Cisco IOS device's command prompt, type the following commands, starting in global configuration mode, in the order shown:

Command	Example	Command Description
crypto isakmp policy *priority*	Cisco-ios-device-1(config)# crypto isakmp policy 1	Enter config-isakmp command mode and identify the policy to create. (Each policy is uniquely identified by the priority number you assign.) This example configures policy 1.
encryption(**3des**| **aes**)	Cisco-ios-device-1 (config-isakmp)# **encryption 3des**	Specify the encryption algorithm. This example configures the 3DES algorithm.
hash (**sha**| **sha256**| **sha384**| **md5**)	Cisco-ios-device-1 (config-isakmp)# **hash sha256**	Specify the hash algorithm. This example configures SHA256.
authentication pre-share	Cisco-ios-device-1 (config-isakmp)# **authentication pre-share**	Specify the pre-share authentication method. **Note**: RSA encrypted nonces (**rsa-encr**), RSA signatures (**rsa-slg**), and digital certificate authentication methods are not supported.
group 2	Cisco-ios-device-1 (config-isakmp)# **group 1**	Specify 1024-bit Diffie-Hellman group identifier (**2**).
lifetime seconds	Cisco-ios-device-1 (config-isakmp)# **lifetime 86400**	Specify the security association's lifetime in seconds. This example configures 86400 seconds (one day).
exit	Cisco-ios-device-1 (config-isakmp)# **exit** Cisco-ios-device-1 (config)#	Exit back to global configuration mode.