SSL Proxy Commands

sslproxy

To enter the sslproxy configuration mode, use the **sslproxy** command in global configuration mode. This command does not have a **no** form.

sslproxy

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

A typical SSL handshake involves authentication using certificates signed by trusted, third-party Certificate Authorities (CAs). TLS is the successor of SSL although is sometimes still referred to as SSL. This command can be used to enter the sslproxy configuration mode where further configurations can be done.

Example

The following example shows how to enter the sslproxy configuration mode.

```
Device(config)# sslproxy
```

Table 1: Related Commands

Command	Description
ca-cert-bundle	Filename of CA certificate bundle.
ca-tp-label	Default Trustpoint label for SSL Proxy.
certificate-lifetime	Certificate lifetime in days.
eckey-type	EC key type for SSL Proxy.
enable	Enables SSL Proxy.
rsa-key-modulus	RSA key length.
settings	Advanced settings for SSL Proxy.

sslproxy ca-tp-label

To set the Default Trustpoint label for SSL proxy, use the **ca-tp-label** command in sslproxy configuration mode. To reset the default Trustpoint label for SSL proxy to the default label of PROXY-SIGNING-CA, use the **no** form of this command.

ca-tp-label *label*
no ca-tp-label

Syntax Description

label	Name of the label <string, Minimum characters: 1, Maximum characters: 128>.

Command Default

Default Trustpoint label is PROXY-SIGNING-CA.

Command Modes

SSL Proxy configuration (config-sslproxy).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

SSL proxy devices act as man-in-the-middle (MitM) to decrypt encrypted SSL traffic traveling across WAN, and send it to UTD for inspection. The Trustpoint label is a name for the RSA key pair. Use this **ca-tp-label** command to set the default Trustpoint label for SSL proxy.

Example

The following example shows how to set the default Trustpoint label for SSL proxy to NEW-PROXY-CA.

```
Device(config)# sslproxy
Device(config-sslproxy)# ca-tp-label NEW-PROXY-CA
```

Table 2: Related Commands

Command	Description
ca-cert-bundle	Filename of CA certificate bundle.
certificate-lifetime	Certificate lifetime in days.
eckey-type	EC key type for SSL proxy.
enable	Enables SSL proxy.
rsa-key-modulus	RSA key length.
settings	Advanced settings for SSL Proxy.

sslproxy certificate-lifetime

To set the lifetime of the proxy certificate, use the **certificate-lifetime** command in sslproxy configuration mode. To reset the lifetime of the proxy certificate to the default value, use the **no** form of this command.

certificate-lifetime *value*
no certificate-lifetime

Syntax Description

value	Sets the lifetime of the proxy certificate in days. The range is from 1 to 4294967295.

Command Default

Default value is 730 (days).

Command Modes

SSL Proxy configuration (config-sslproxy).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Once you configure a Certificate Authorities (CA) for SSL proxy, the CA issues signing certificates to the SSL proxy device. The device then securely stores the subordinate CA keys, and dynamically generates and signs the proxy certificates. Use this **certificate-lifetime** command to set the lifetime of the proxy certificate.

Example

The following example shows how to set the lifetime of the proxy certificate to 365 days.

```
Device(config)# sslproxy
Device(config-sslproxy)# certificate-lifetime 365
```

Table 3: Related Commands

Command	Description
ca-cert-bundle	Filename of CA certificate bundle.
ca-tp-label	Default Trustpoint label for SSL proxy.
eckey-type	EC key type for SSL proxy.
enable	Enables SSL Proxy.
rsa-key-modulus	RSA key length.
settings	Advanced settings for SSL proxy.

sslproxy eckey-type

To set the elliptic curve cryptography key type for SSL proxy, use the **eckey-type** command in sslproxy configuration mode. To reset the elliptic curve cryptography key type to the default value of P256, use the **no** form of this command.

eckey-type { **P256** | **P384** | **P521** }
no eckey-type

Syntax Description

P256	Specifies the EC key type to P256.
P384	Specifies the EC key type to P384.
P521	Specifies the EC key type to P521.

Command Default

The default value is P256.

Command Modes

SSL Proxy configuration (config-sslproxy).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. One of the main benefits in comparison with non-ECC cryptography is

the same level of security provided by keys of smaller size. Larger keys offer stronger security but takes longer to use. Use this **eckey-type** command to set the EC key type.

Example

The following example shows how to set the EC key type to P521.

```
Device(config)# sslproxy
Device(config-sslproxy)# eckey-type P521
```

Table 4: Related Commands

Command	Description
ca-cert-bundle	Filename of CA certificate bundle.
ca-tp-label	Default Trustpoint label for SSL proxy.
certificate-lifetime	Certificate lifetime in days.
enable	Enables SSL proxy.
rsa-key-modulus	RSA key length.
settings	Advanced settings for SSL proxy.

sslproxy enable

To enable SSL proxy, use the **enable** command in sslproxy configuration mode. To disable SSL proxy, use the **no** form of this command.

enable
no enable

Syntax Description

This command has no keywords or arguments.

Command Default

SSL proxy is not enabled.

Command Modes

SSL proxy configuration (config-sslproxy).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

SSL proxy devices act as man-in-the-middle (MitM) to decrypt encrypted SSL traffic traveling across WAN, and send it to UTD for inspection. SSL proxy thus allows devices to identify risks that are hidden by end-to-end encryption over SSL channels. The data is re-encrypted post inspection before being sent to its final destination. TLS is the successor of SSL, although, it is sometimes still referred to as SSL. Use this **enable** command to enable SSL proxy.

Example

The following example shows how to enable SSL proxy.

```
Device(config)# sslproxy
Device(config-sslproxy)# enable
```

Table 5: Related Commands

Command	Description
ca-cert-bundle	Filename of CA certificate bundle.
ca-tp-label	Default Trustpoint label for SSL proxy.
certificate-lifetime	Certificate lifetime in days.
eckey-type	EC key type for SSL proxy.
rsa-key-modulus	RSA key length.
settings	Advanced settings for SSL proxy.

sslproxy rsa-key-modulus

To set the rsa-key-modulus key size, use the **rsa-key-modulus** command in sslproxy configuration mode. To reset the rsa-key-modulus to the default key size of 2048, use the **no** form of this command.

rsa-key-modulus *key size*
no rsa-key-modulus

Syntax Description

key size	Specifies the key size. Range: 1024 to 4096.

Command Default

The default key size is 2048.

Command Modes

SSL proxy configuration (config-sslproxy).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

The command can be used to set the rsa-key-modulus key size. The longer the modulus, the stronger the security. However, a longer modulus takes longer to generate and to use.

Example

The following example shows how to set the rsa-key-modulus key size to 4096.

```
Device(config)# sslproxy
Device(config-sslproxy)# rsa-key-modulus 4096
```

Table 6: Related Commands

Command	Description
ca-cert-bundle	Filename of CA certificate bundle.
ca-tp-label	Default Trustpoint label for SSL proxy.
certificate-lifetime	Certificate lifetime in days.
eckey-type	EC key type for SSL proxy.
enable	Enables SSL proxy.
settings	Advanced settings for SSL proxy.

sslproxy settings certificate-revocation-check

To change the sslproxy certificate-revocation-check setting, use the **settings certificate-revocation-check** command in sslproxy configuration mode. To reset the sslproxy certificate-revocation-check setting to the default value of none, use the **no** form of this command.

settings certificate-revocation-check { **none** | **ocsp** }
no settings certificate-revocation-check

Syntax Description

none	Disables certificate revocation checking.
ocsp	Specifies that the method Online Certificate Status Protocol (OCSP) be used to check the revocation status of the server certificate.

Command Default

Default setting is none.

Command Modes

SSL proxy configuration (config-sslproxy).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

A typical SSL handshake involves authentication using certificates signed by trusted, third-party Certificate Authorities. TLS is the successor of SSL, although, it is sometimes still referred to as SSL. Use the **settings certificate-revocation-check** command to set the method the SSL proxy uses to check the certificate status.

Example

The following example show how to set OSCP as the method for SSL proxy to use to check the certificate status.

```
Device(config)# sslproxy
Device(config-sslproxy)# settings certificate-revocation-check ocsp
```

Table 7: Related Commands

Commands	Description
expired-certificate	Specifies the action for expired certificate.
failure-mode	Specifies the action for failure mode.
minimum-tls-ver	Specifies the minimum TLS version for SSL proxy.
unknown-status	Specifies the action for unknown status.
unsupported-cipher-suites	Specifies the action for unsupported cipher suite.
unsupported-protocol-versions	Specifies the action for unsupported protocol version.
untrusted-certificate	Specifies the action for untrusted certificate.

sslproxy settings expired-certificate

To change the sslproxy expired-certificate setting, use the **settings expired-certificate** command in sslproxy configuration mode. To reset the sslproxy expired-certificate setting to the default value of drop, use the **no** form of this command.

settings expired-certificate { **decrypt** | **drop** }
no settings expired-certificate

Syntax Description

decrypt	The packet is forwarded to the client and goes through the following: • TCP optimization for optimization of traffic • Decryption of encrypted traffic through TLS proxy • Threat inspection through UTD • Re-encryption of decrypted traffic through TLS proxy
drop	The hello packet from the client is dropped and the connection is reset.

Command Default

The default setting is dropped.

Command Modes

SSL proxy configuration (config-sslproxy).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

A typical SSL handshake involves authentication using certificates signed by trusted, third-party Certificate Authorities (CAs). TLS is the successor of SSL although is sometimes still referred to as SSL. Use this **settings expired-certificate** command to set the action the SSL proxy should do if the server certificate is expired.

Example

The following example shows how to set the action to decrypt the encrypted traffic if the server certificate has expired.

```
Device(config)# sslproxy
Device(config-sslproxy)# settings expired-certificate decrypt
```

Table 8: Related Commands

Commands	Description
certificate-revocation-check	Specifies ocsp or none.
failure-mode	Specifies action for failure mode.
minimum-tls-ver	Specifies minimum TLS version for SSL proxy.
unknown-status	Specifies action for unknown status.
unsupported-cipher-suites	Specifies action for unsupported cipher suite.
unsupported-protocol-versions	Specifies action for unsupported protocol version.
untrusted-certificate	Specifies action for untrusted certificate.

sslproxy settings failure-mode

To change the sslproxy failure-mode setting, use the **settings failure-mode** command in sslproxy configuration mode. To reset the sslproxy failure-mode setting to the default value of close, use the **no** form of this command.

settings failure-mode { **close** | **open** }
no settings failure-mode

Syntax Description

close	Specifies the failure mode to close.
open	Specifies the failure mode to open.

Command Default

The default setting is close.

Command Modes

SSL proxy configuration (config-sslproxy).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

A typical SSL handshake involves authentication using certificates signed by trusted, third-party Certificate Authorities (CAs). TLS is the successor of SSL, although, it is sometimes still referred to as SSL. Use this **settings failure-mode** command to set the failure mode when the SSL handshake fails.

Example

The following example shows how to set the failure mode when the SSL handshake fails to open.

```
Device(config)# sslproxy
Device(config-sslproxy)# settings failure-mode open
```

Table 9: Related Commands

Commands	Description
certificate-revocation-check	Specifies ocsp or none.
expired-certificate	Specifies action for expired certificate.
minimum-tls-ver	Specifies minimum TLS version for SSL proxy.
unknown-status	Specifies action for unknown status.
unsupported-cipher-suites	Specifies action for unsupported cipher suite.
unsupported-protocol-versions	Specifies action for unsupported protocol version.
untrusted-certificate	Specifies action for untrusted certificate.

sslproxy settings minimum-tls-ver

To change the sslproxy minimum-tls-ver setting, use the **settings minimum-tls-ver** command in sslproxy configuration mode. To reset the sslproxy minimum-tls-ver setting to the default value of TLSv1, use the **no** form of this command.

settings minimum-tls-ver { **TLSv1** | **TLSv1.1** | **TLSv1.2** }
no settings minimum-tls-ver

Syntax Description

TLSv1	Specifies the minimum supported TLS version as 1.
TLSv1.1	Specifies the minimum supported TLS version as 1.1.
TLSv1.2	Specifies the minimum supported TLS version as 1.2.

Command Default

The default setting is TLSv1.

Command Modes SSL proxy configuration (config-sslproxy).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines A typical SSL handshake involves authentication using certificates signed by trusted, third-party Certificate Authorities. TLS is the successor of SSL, although, it is sometimes still referred to as SSL. Use the **settings minimum-tls-ver** command to set the minimum supported TLS version.

Example

The following example shows how to set the minimum supported TLS version to TLSv1.2.

```
Device(config)# sslproxy
Device(config-sslproxy)# settings minimum-tls-ver tlsv1.2
```

Table 10: Related Commands

Commands	Description
certificate-revocation-check	Specifies OCSP or none.
expired-certificate	Specifies the action for expired certificate.
failure-mode	Specifies the action for failure mode.
unknown-status	Specifies the action for unknown status.
unsupported-cipher-suites	Specifies the action for unsupported cipher suite.
unsupported-protocol-versions	Specifies the action for unsupported protocol version.
untrusted-certificate	Specifies the action for untrusted certificate.

sslproxy settings unknown-status

To change the sslproxy unknown-status setting, use the **settings unknown-status** command in sslproxy configuration mode. To reset the sslproxy unknown-status setting to the default value of drop, use the **no** form of this command.

settings unknown-status { **decrypt** | **drop** }
no settings unknown-status

Syntax Description

decrypt	The packet is forwarded to the client and goes through the following: • TCP optimization for optimization of traffic. • Decryption of encrypted traffic through TLS proxy. • Threat inspection through Unified Threat Defense (UTD). • Re-encryption of decrypted traffic through TLS proxy.
drop	The hello packet from the client is dropped and the connection is reset.

Command Default

The default setting is drop.

Command Modes

SSL proxy configuration (config-sslproxy).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

A typical SSL handshake involves authentication using certificates signed by trusted, third-party Certificate Authorities. TLS is the successor of SSL although is sometimes still referred to as SSL. Use the **settings unknown-status** command to set the action the SSL proxy should do if the server certificate status is unknown.

Example

The following example shows how to set the action to decrypt the encrypted traffic if the server certificate status is unknown.

```
Device(config)# sslproxy
Device(config-sslproxy)# settings unknown-status decrypt
```

Table 11: Related Commands

Commands	Description
certificate-revocation-check	Specifies OCSP or none.
expired-certificate	Specifies the action for expired certificate.
failure-mode	Specifies the action for failure mode.
minimum-tls-ver	Specifies the minimum TLS version for SSL proxy.
unsupported-cipher-suites	Specifies the action for unsupported cipher suite.
unsupported-protocol-versions	Specifies the action for unsupported protocol version.
untrusted-certificate	Specifies the action for untrusted certificate.

sslproxy settings untrusted-certificate

To change the sslproxy untrusted-certificate setting, use the **settings untrusted-certificate** command in sslproxy configuration mode. To reset the setting to default value of drop, use the **no** form of this command.

settings untrusted-certificate { **decrypt** | **drop** }
no settings untrusted-certificate

Syntax Description

decrypt	The packet is forwarded to the client and goes through the following: • TCP optimization for optimization of traffic • Decryption of encrypted traffic through TLS proxy • Threat inspection through UTD • Re-encryption of decrypted traffic through TLS proxy
drop	The hello packet from the client is dropped and the connection is reset.

Command Default

The default setting is drop.

Command Modes

SSL Proxy configuration (config-sslproxy)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

A typical SSL handshake involves authentication using certificates signed by trusted, third-party Certificate Authorities (CAs). TLS is the successor of SSL although it is sometimes still referred to as SSL. Use this **settings untrusted-certificate** command to set the action, the SSL proxy should do if the server certificate is untrusted.

Example

The following example shows how to set the action to decrypt the encrypted traffic if the server certificate is untrusted.

```
Device(config)# sslproxy
Device(config-sslproxy)# settings untrusted-certificate decrypt
```

Table 12: Related Commands

Commands	Description
certificate-revocation-check	Specifies ocsp or none.
expired-certificate	Specifies action for expired certificate.
failure-mode	Specifies action for failure mode.

Commands	Description
minimum-tls-ver	Specifies minimum TLS version for SSL proxy.
unknown-status	Specifies action for unknown status.
unsupported-cipher-suites	Specifies action for unsupported cipher suite.
unsupported-protocol-versions	Specifies action for unsupported protocol version.

sslproxy settings unsupported-cipher-suites

To change the sslproxy unsupported-cipher-suites setting, use the **settings unsupported-cipher-suites** command in sslproxy configuration mode. To reset the sslproxy unsupported-cipher-suites setting to the default value of drop, use the **no** form of this command.

settings unsupported-cipher-suites { **drop** | **no-decrypt** }
no settings unsupported-cipher-suites

Syntax Description

drop	The hello packet from the client is dropped and the connection is reset.
no-decrypt	The hello packet from the client bypasses the SSL proxy.

Command Default

The default setting of this command is drop.

Command Modes

SSL proxy configuration (config-sslproxy).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

A typical SSL handshake involves authentication using certificates signed by trusted, third-party Certificate Authorities (CAs). TLS is the successor of SSL, although, it is sometimes still referred to as SSL. The SSL Proxy feature in Cisco Catalyst SD-WAN only supports certain cipher suites. Use this **settings unsupported-cipher-suites** command to set the action the SSL proxy should do if the cipher suite detected is unsupported.

Example

The following example shows how to set the action to no-decrypt if the cipher suite detected is unsupported.

```
Device(config)# sslproxy
Device(config-sslproxy)# settings unsupported-cipher-suites no-decrypt
```

Table 13: Related Commands

Commands	Description
certificate-revocation-check	Specifies ocsp or none.
expired-certificate	Specifies action for expired certificate.
failure-mode	Specifies action for failure mode.
minimum-tls-ver	Specifies minimum TLS version for SSL proxy.
unknown-status	Specifies action for unknown status.
unsupported-protocol-versions	Specifies action for unsupported protocol version.
untrusted-certificate	Specifies action for untrusted certificate.

sslproxy settings unsupported-protocol-versions

To change the sslproxy unsupported-protocol-versions setting, use the **settings unsupported-protocol-versions** command in sslproxy configuration mode. To reset the sslproxy unsupported-protocol-versions setting to the default value of drop, use the **no** form of this command.

settings unsupported-protocol-versions { **drop** | **no-decrypt** }
no settings unsupported-protocol-versions

Syntax Description

drop	The hello packet from the client is dropped and the connection is reset.
no-decrypt	The hello packet from the client bypasses SSL proxy.

Command Default

The default setting is drop.

Command Modes

SSL proxy configuration (config-sslproxy).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

A typical SSL handshake involves authentication using certificates signed by trusted, third-party Certificate Authorities. TLS is the successor of SSL, although, it is sometimes still referred to as SSL. The SSL proxy can be set to require a minimum TLS protocol version. Use the **settings unsupported-protocol-versions** command to set the action the SSL proxy should do if the protocol version detected is unsupported.

Example

The following example shows how to set the action to no-decrypt if the protocol version detected is unsupported.

```
Device(config)# sslproxy
Device(config-sslproxy)# settings unsupported-protocol-versions no-decrypt
```

Table 14: Related Commands

Commands	Description
certificate-revocation-check	Specifies OCSP or none.
expired-certificate	Specifies the action for expired certificate.
failure-mode	Specifies the action for failure mode.
unknown-status	Specifies the action for unknown status.
minimum-tls-ver	Specifies the minimum TLS version for SSL proxy.
unsupported-cipher-suites	Specifies the action for unsupported cipher suite.
untrusted-certificate	Specifies the action for untrusted certificate.