Name create-ssl– creates and configures the SSL element in the selected HTTP listener, IIOP listener, or IIOP service

Synopsis

```
create-ssl
[--help]

 --type  listener_or_service_type  --certname cert_name
[--ssl2enabled=false ] [--ssl2ciphers ss12ciphers ]
[--ssl3enabled=true ] [--tlsenabled=true ]
[--ssl3tlsciphers ssl3tlsciphers ] [--tlsrollbackenabled=true ]
[--clientauthenabled=false ] [listener_id]
```

Description The `create-ssl` subcommand creates and configures the SSL element in the selected HTTP listener, IIOP listener, or IIOP service to enable secure communication on that listener/service.

This subcommand is supported in remote mode only.

Options If an option has a short option name, then the short option precedes the long option name. Short options have one dash whereas long options have two dashes.

`--help`
Displays the help text for the subcommand.

`--target`
Do not specify this option. This option is retained for compatibility with other releases. If you specify this option, a syntax error does not occur. Instead, the subcommand runs successfully and the option is silently ignored.

`--type`
The type of service or listener for which the SSL is created. The type can be:

- `http-listener`
- `iiop-listener`
- `iiop-service`

When the type is `iiop-service`, the `ssl-client-config` along with the embedded `ssl` element is created in `domain.xml`.

`--certname`
The nickname of the server certificate in the certificate database or the PKCS#11 token. The format of the name in the certificate is *tokenname:nickname*. For this property, the *tokenname:* is optional.

`--ssl2enabled`
Set this property to `true` to enable SSL2. The default value is `false`. If both SSL2 and SSL3 are enabled for a virtual server, the server tries SSL3 encryption first. In the event SSL3 encryption fails, the server then tries SSL2 encryption.

`--ssl2ciphers`
A comma-separated list of the SSL2 ciphers to be used. Use the prefix + to enable or – to disable a particular cipher. Allowed values are:

- `rc4`
- `rc4export`
- `rc2`
- `rc2export`
- `idea`
- `des`
- `desede3`

If no value is specified, all supported ciphers are assumed to be enabled.

`--ssl3enabled`
Set this property to `false` to disable SSL3. The default value is `true`. If both SSL2 and SSL3 are enabled for a virtual server, the server tries SSL3 encryption first. In the event SSL3 encryption fails, the server then tries SSL2 encryption.

`--tlsenabled`
Set this property to `false` to disable TLS. The default value is `true` It is good practice to enable TLS, which is a more secure version of SSL.

`--ssl3tlsciphers`
A comma-separated list of the SSL3 and/or TLS ciphers to be used. Use the prefix + to enable or – to disable a particular cipher. Allowed values are:

- `SSL_RSA_WITH_RC4_128_MD5`
- `SSL_RSA_WITH_3DES_EDE_CBC_SHA`
- `SSL_RSA_WITH_DES_CBC_SHA`
- `SSL_RSA_EXPORT_WITH_RC4_40_MD5`
- `SSL_RSA_WITH_NULL_MD5`
- `SSL_RSA_WITH_RC4_128_SHA`
- `SSL_RSA_WITH_NULL_SHA`

If no value is specified, all supported ciphers are assumed to be enabled.

`--tlsrollbackenabled`
Set to `true` (default) to enable TLS rollback. TLS rollback should be enabled for Microsoft Internet Explorer 5.0 and 5.5. This option is only valid when `-tlsenabled=true`.

`--clientauthenabled`
Set to `true` if you want SSL3 client authentication performed on every request independent of ACL-based access control. Default value is `false`.

Operands *listener_id*
The ID of the HTTP or IIOP listener for which the SSL element is to be created. The *listener_id* is not required if the `--type` is `iiop-service`.

Examples

EXAMPLE 1 Creating an SSL element for an HTTP listener

The following example shows how to create an SSL element for an HTTP listener named `http-listener-1`.

```
asadmin> create-ssl
--type http-listener
--certname sampleCert http-listener-1
Command create-ssl executed successfully.
```

Exit Status

0	command executed successfully
1	error in executing the command

See Also

`delete-ssl`(1)

`asadmin`(1M)