Countermeasures for vulnerability (CTX230612)

Countermeasures

If you use client certificate for authentication between NetScaler and realserver, please take one of the following countermeasures.

- Stop usingclient certificate.
- Do not use Chiper Suite of DHE.

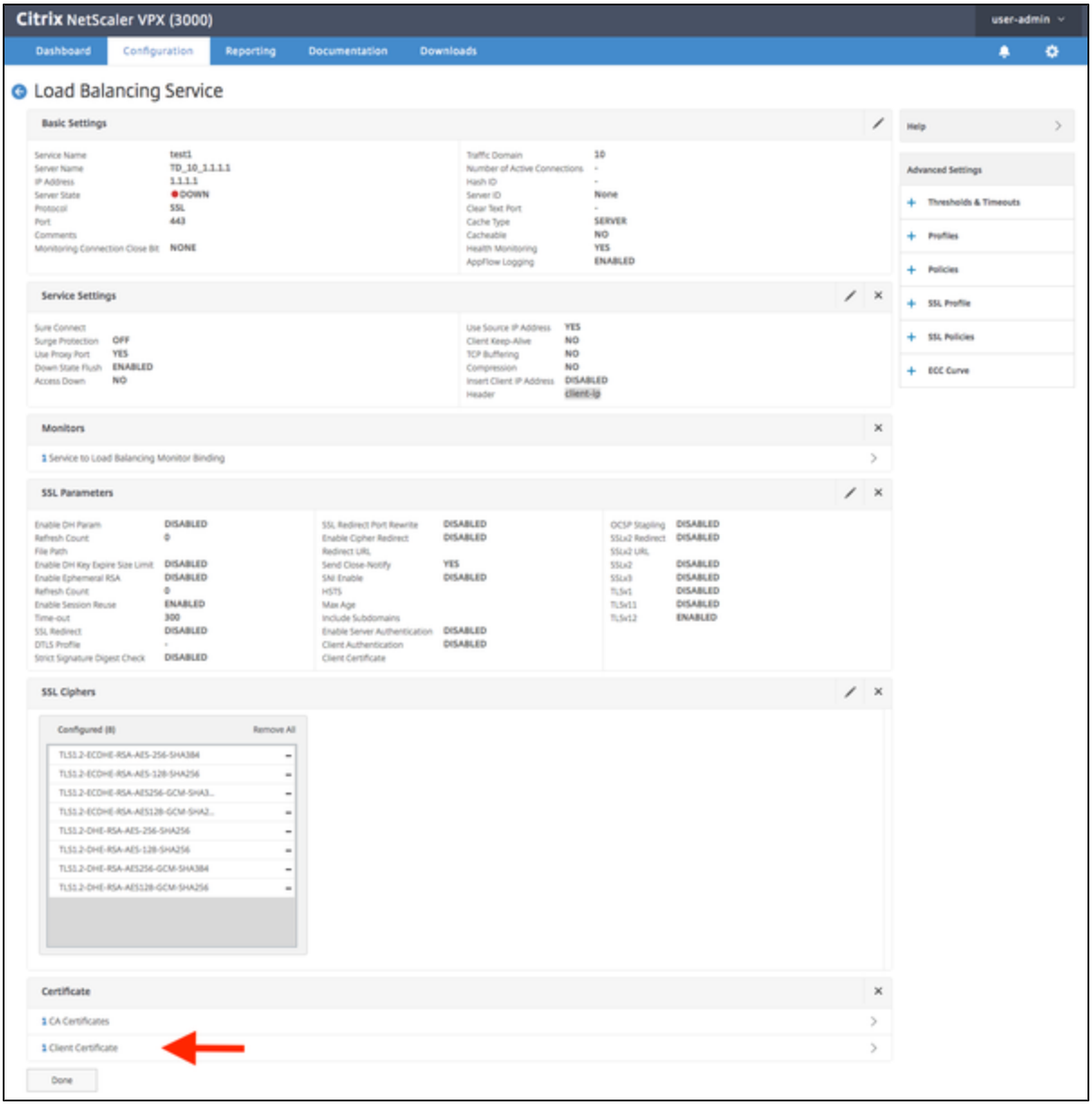
Setting method

Setting method via GUI

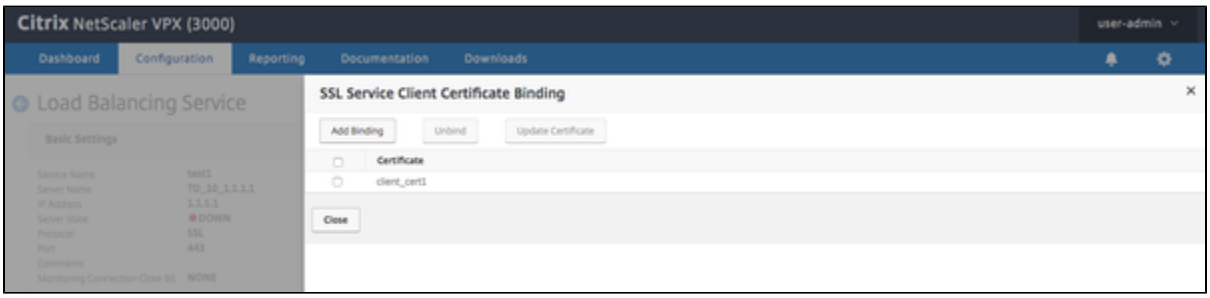
Deauthorize client certificate for realserver

As for the setting of the web server specified on the realserver side, it is necessary to change it according to the environment.

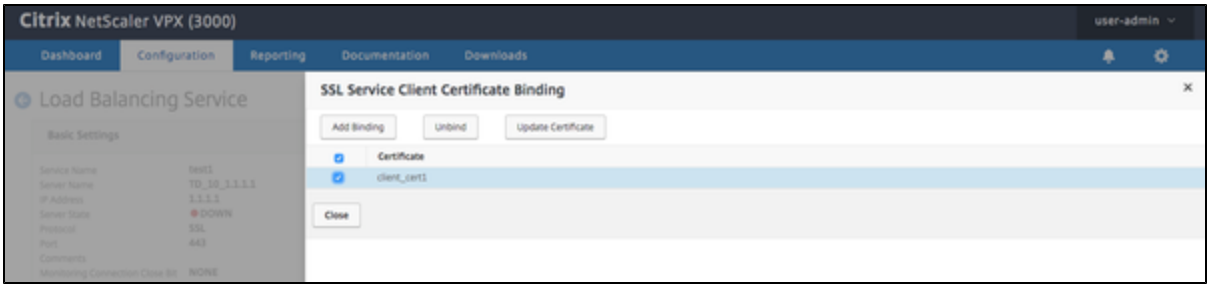
Client certificate is registered in certificate when using client certificate authentication on Load Balancing -> Load Balancing Service setting screen of Traffic Management - Load Balancing - Services



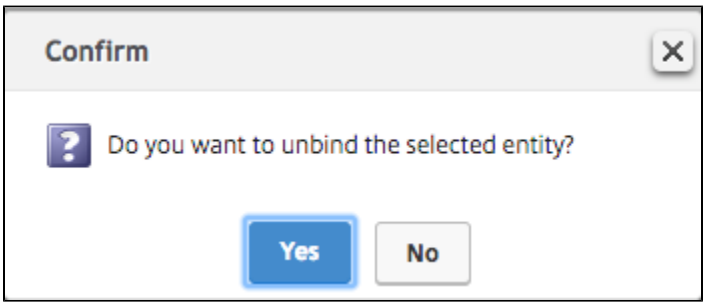
It will transition to the screen below by clicking on the above Client Certificate.



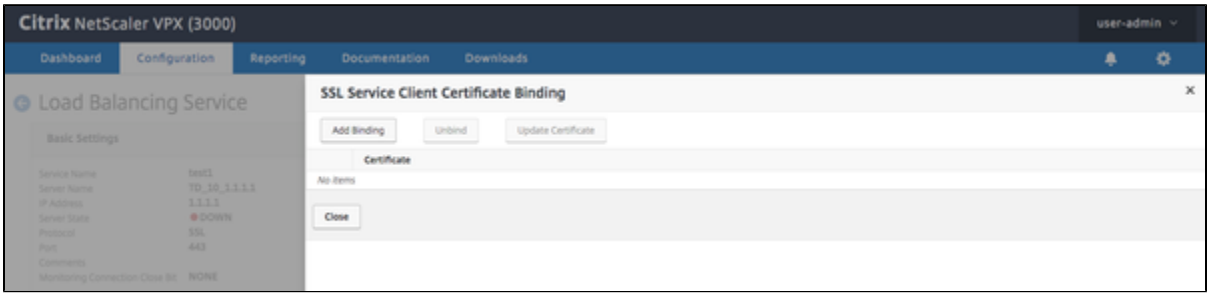
Select the client certificate and click the Unbind button.

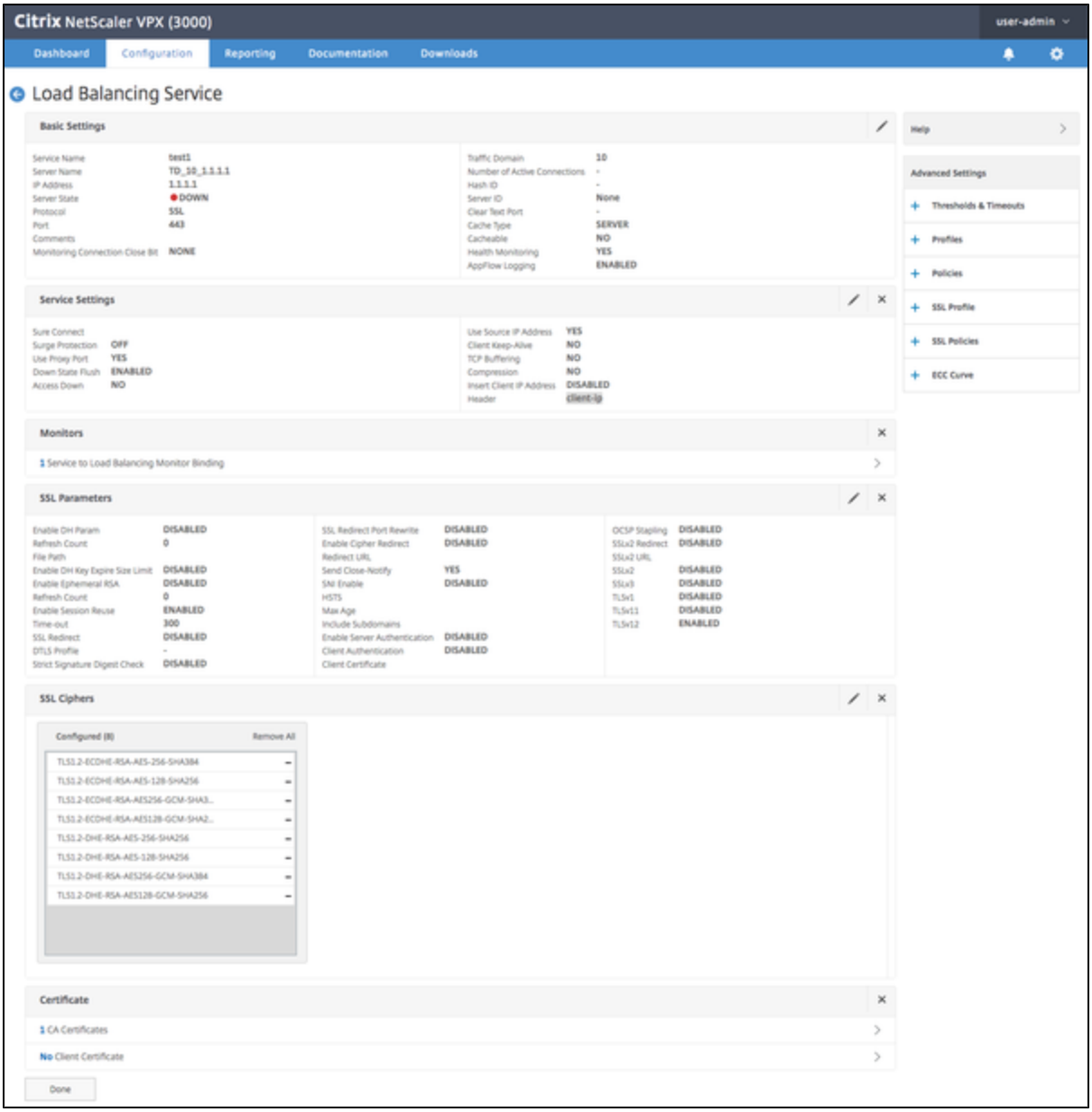


Select Yes if the following message is displayed.



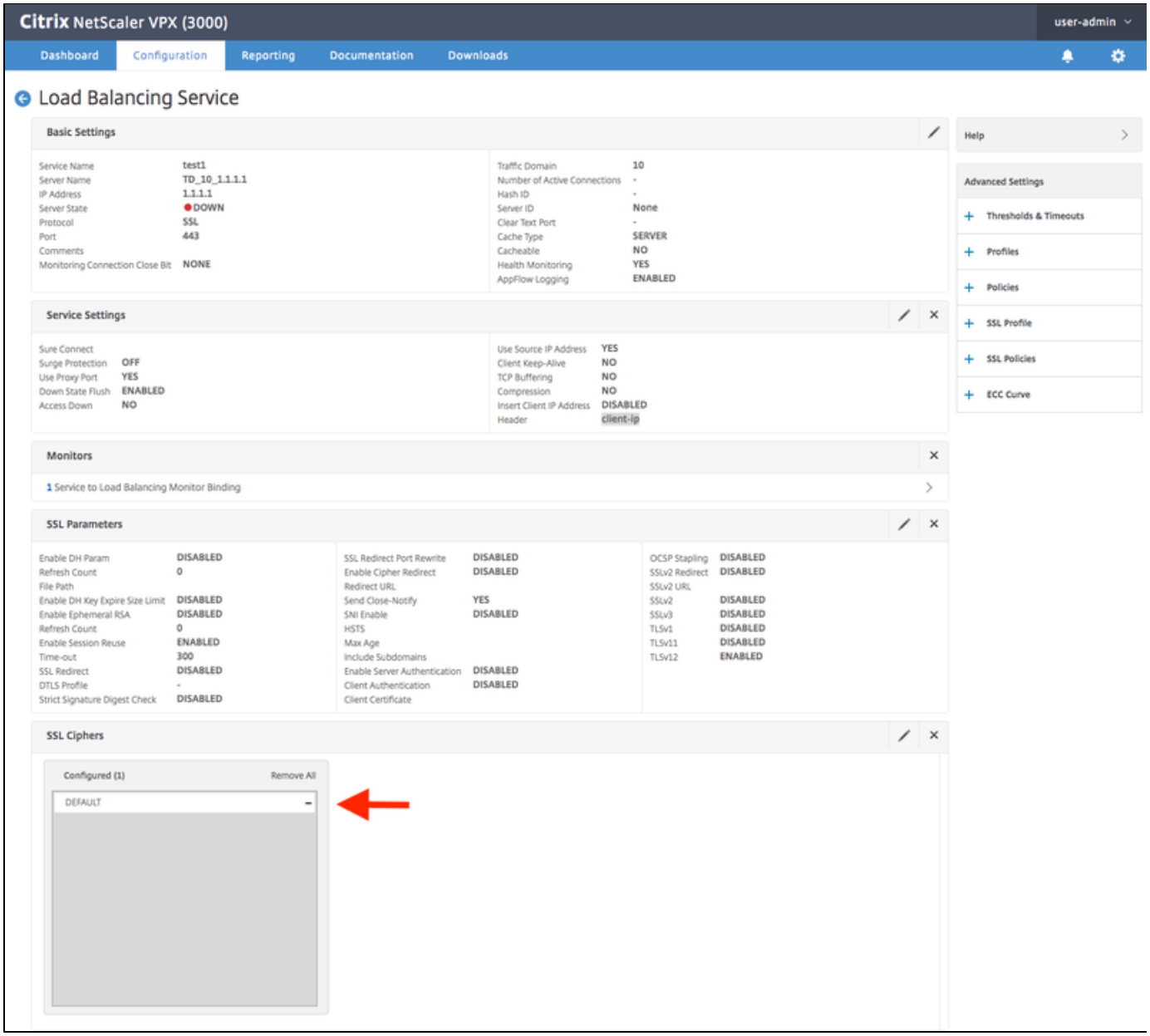
Make sure that it is unbinded and click the Close button.

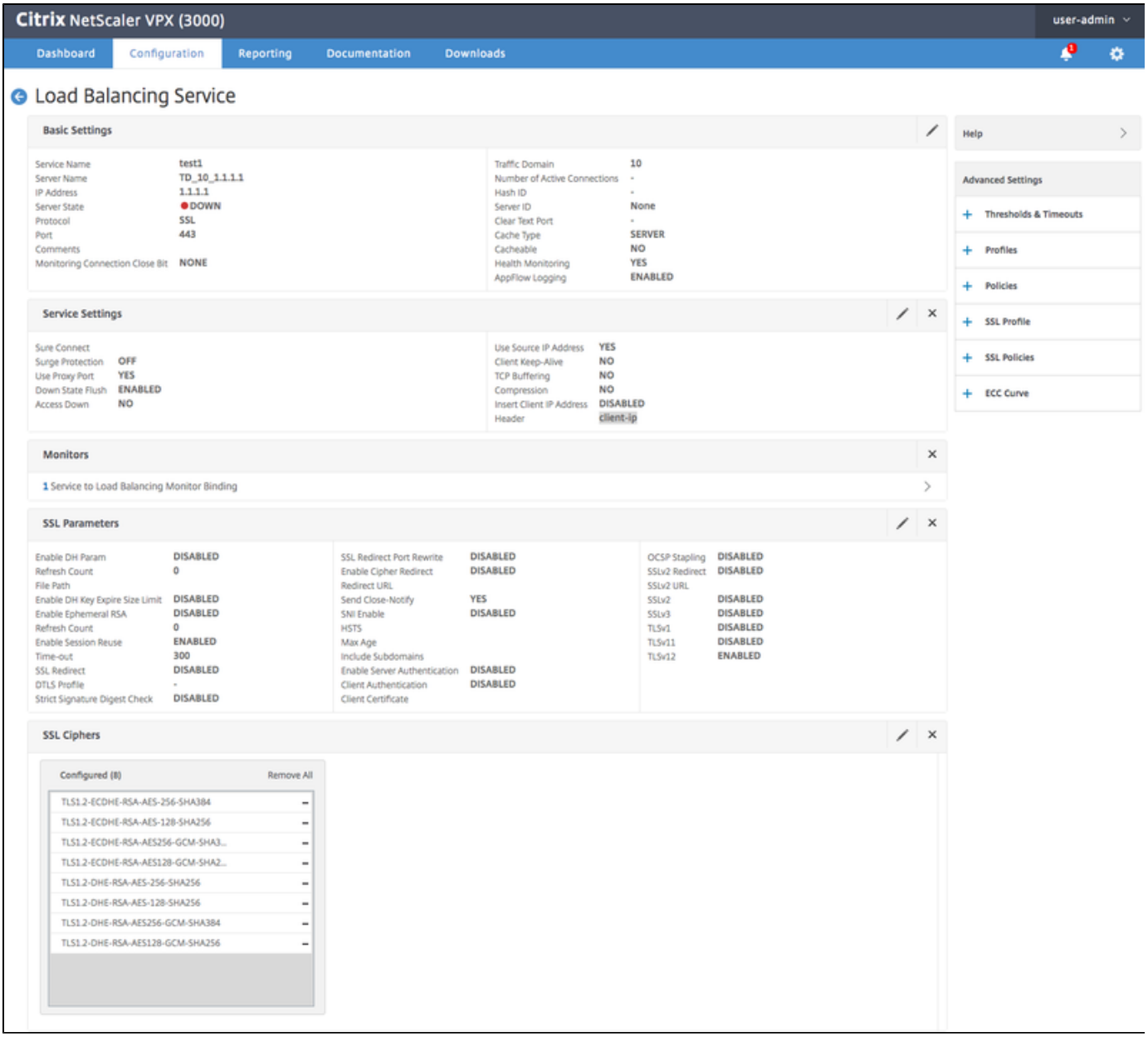




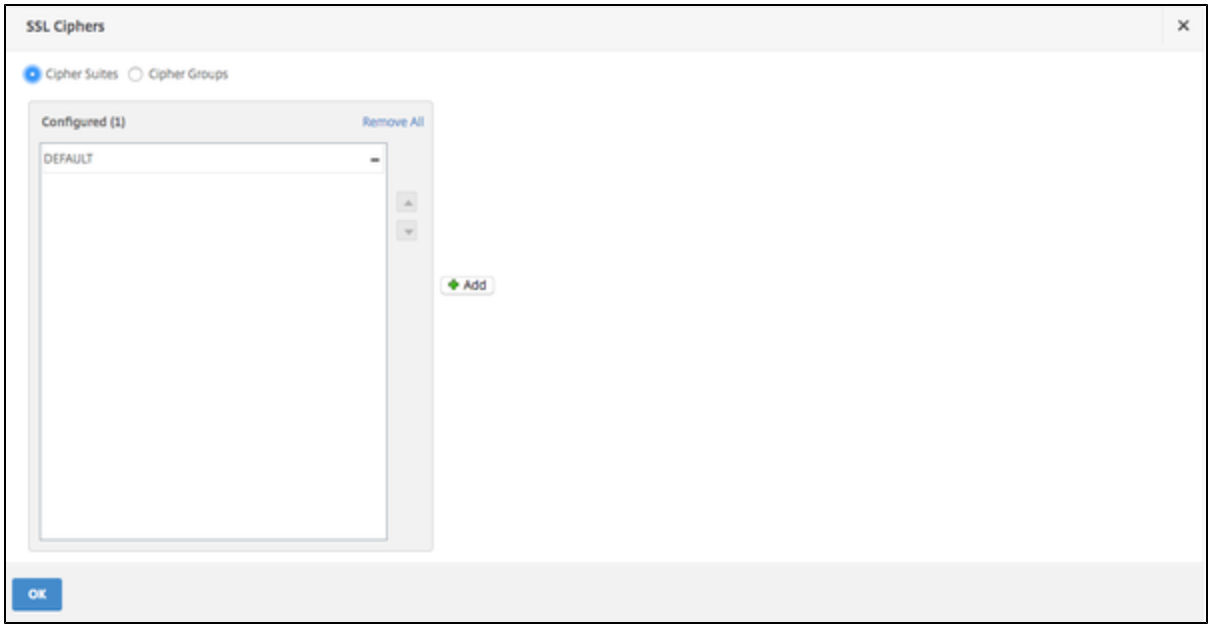
Disable CipherSuite DHE

If SSL Ciphers is default or explicitly using DHE, disable CipherSuite of DHE.On the Load Balancing Service on setting screen of Traffic Management - Load Balancing - Services.


Citrix NetScaler VPX (3000)
user-admin
Dashboard
Configuration
Reporting
Documentation
Downloads
Load Balancing Service
Basic Settings
Service Name test1
Server Name TD_10_1.1.1.1
IP Address 1.1.1.1
Server State DOWN
Protocol SSL
Port 443
Comments
Monitoring Connection Close Bit NONE
Traffic Domain 10
Number of Active Connections -
Hash ID -
Server ID None
Clear Text Port -
Cache Type SERVER
Cacheable NO
Health Monitoring YES
AppFlow Logging ENABLED
Service Settings
Sure Connect
Surge Protection OFF
Use Proxy Port YES
Down State Flush ENABLED
Access Down NO
Use Source IP Address YES
Client Keep-Alive NO
TCP Buffering NO
Compression NO
Insert Client IP Address DISABLED
Header client-ip
Monitors
1 Service to Load Balancing Monitor Binding
SSL Parameters
Enable DH Param DISABLED
Refresh Count 0
File Path
Enable DH Key Expire Size Limit DISABLED
Enable Ephemeral RSA DISABLED
Refresh Count 0
Enable Session Reuse ENABLED
Time-out 300
SSL Redirect DISABLED
DTLS Profile -
Strict Signature Digest Check DISABLED
SSL Redirect Port Rewrite DISABLED
Enable Cipher Redirect DISABLED
Redirect URL
Send Close-Notify YES
SNI Enable DISABLED
HSTS
Max Age
Include Subdomains
Enable Server Authentication DISABLED
Client Authentication DISABLED
Client Certificate
OCSP Stapling DISABLED
SSLv2 Redirect DISABLED
SSLv2 URL
SSLv2 DISABLED
SSLv3 DISABLED
TLSv1 DISABLED
TLSv11 DISABLED
TLSv12 ENABLED
SSL Ciphers
Configured (1)
Remove All
DEFAULT
Help
Advanced Settings
Thresholds & Timeouts
Profiles
Policies
SSL Profile
SSL Policies
ECC Curve

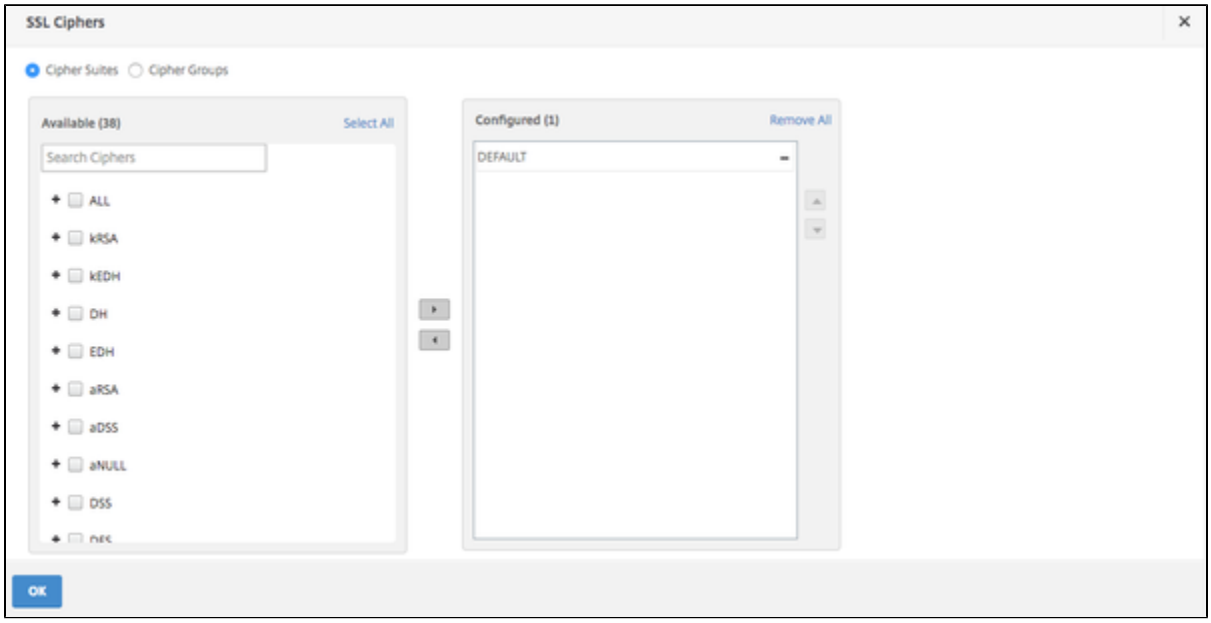


Click the SSL Ciphers edit button and the Add button in the center.

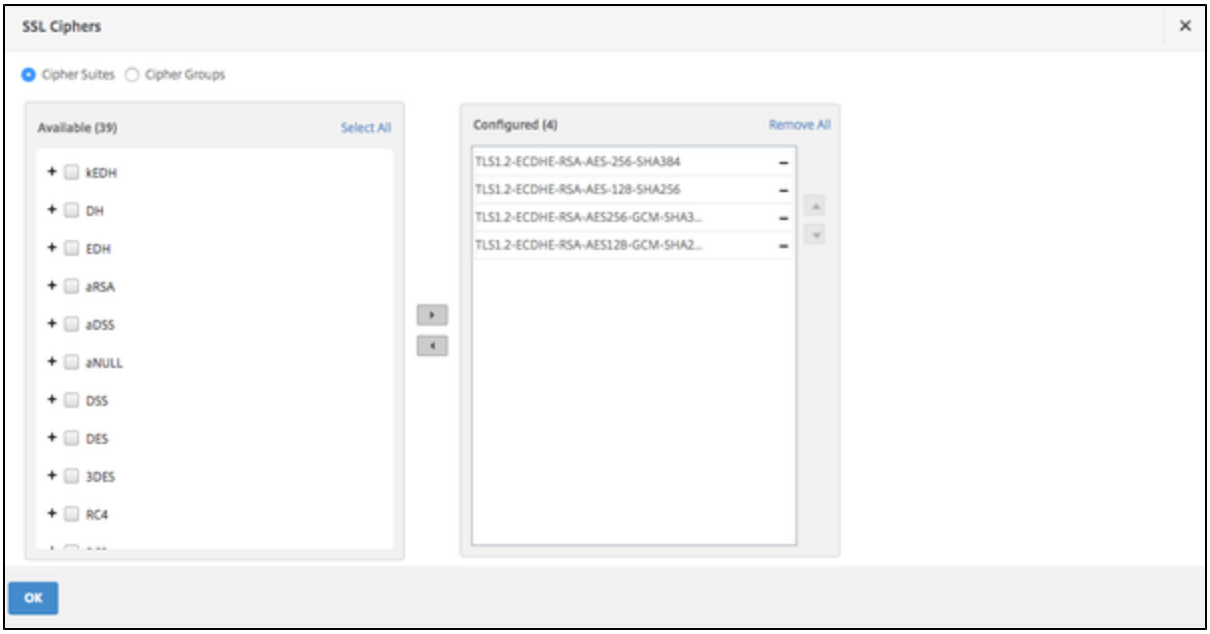


Select the necessary CipherSuite from Available on the left frame and click the rightward button at the center to add it.

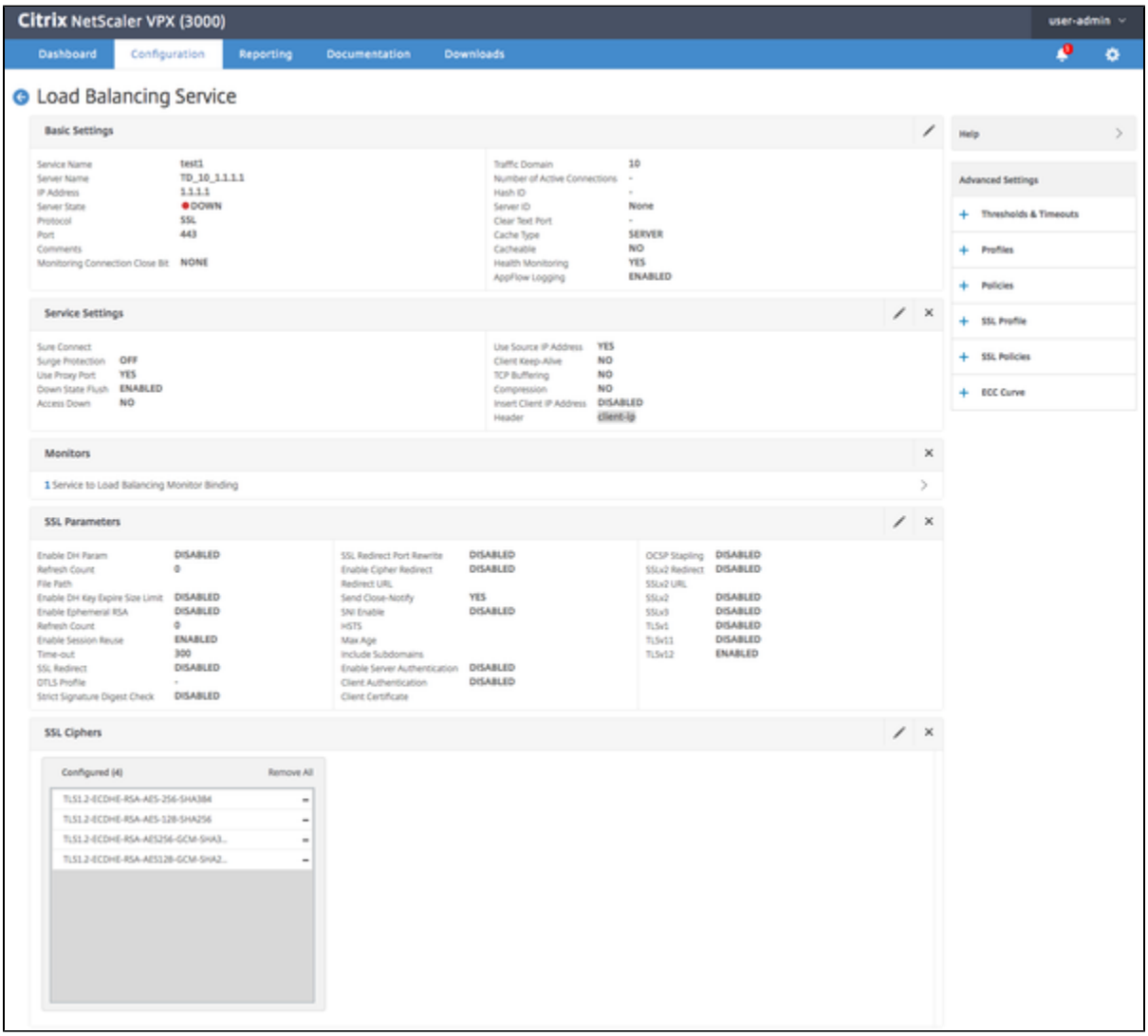
Also, click - on the right side of unnecessary CipherSuite from Configured in the right frame and delete it.



After completing the above, click the OK button (TLS 1.2 - ECDHE - RSA is selected as an example in the screen below).

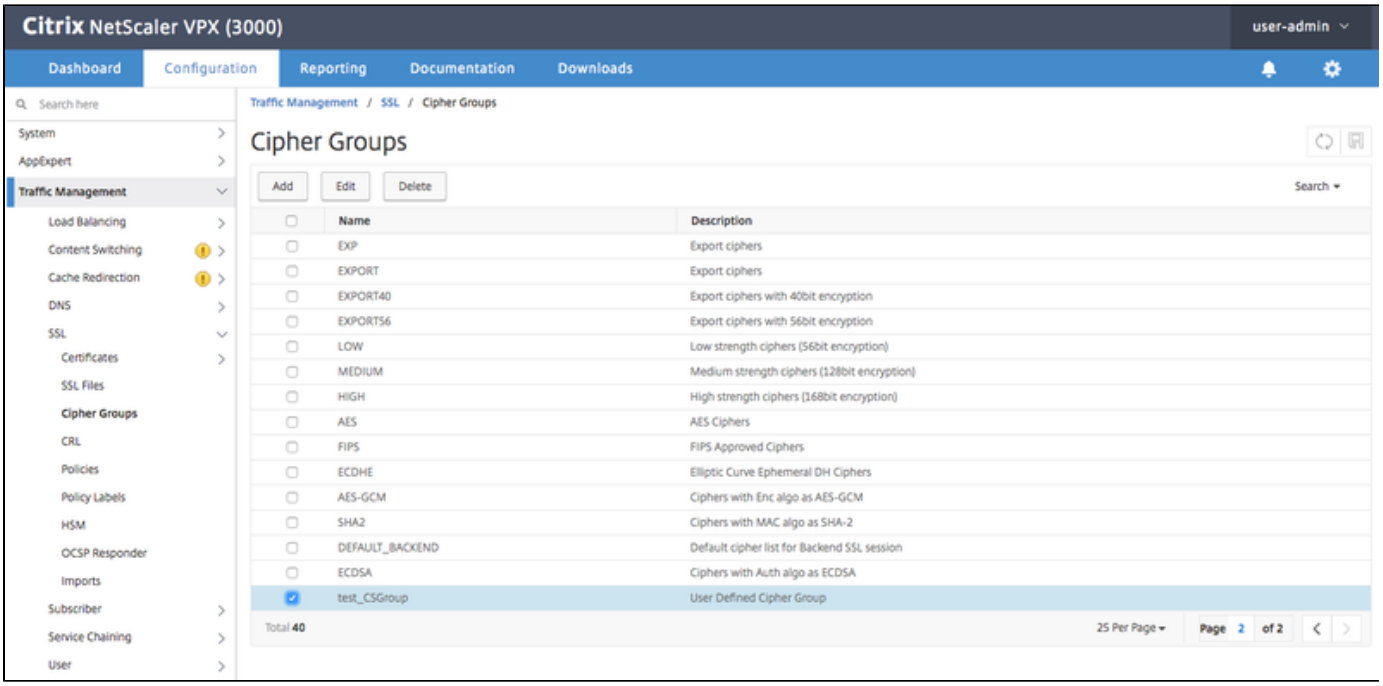


Confirm that settings are reflected correctly and save the settings.

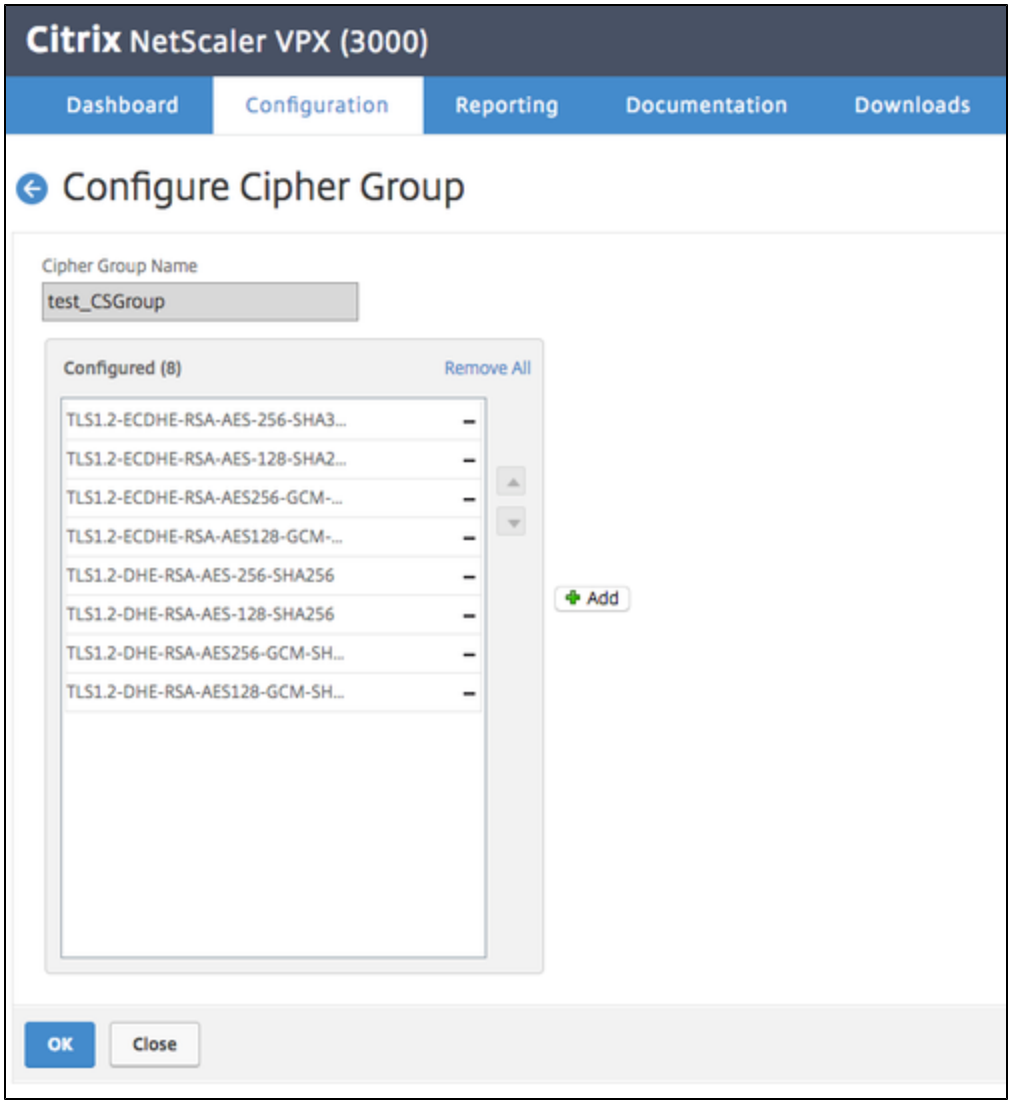


* If you create and use CipherGroup including DHE, edit CipherGroup (Since you can not edit the default Cipher Group, you need to create a new group).

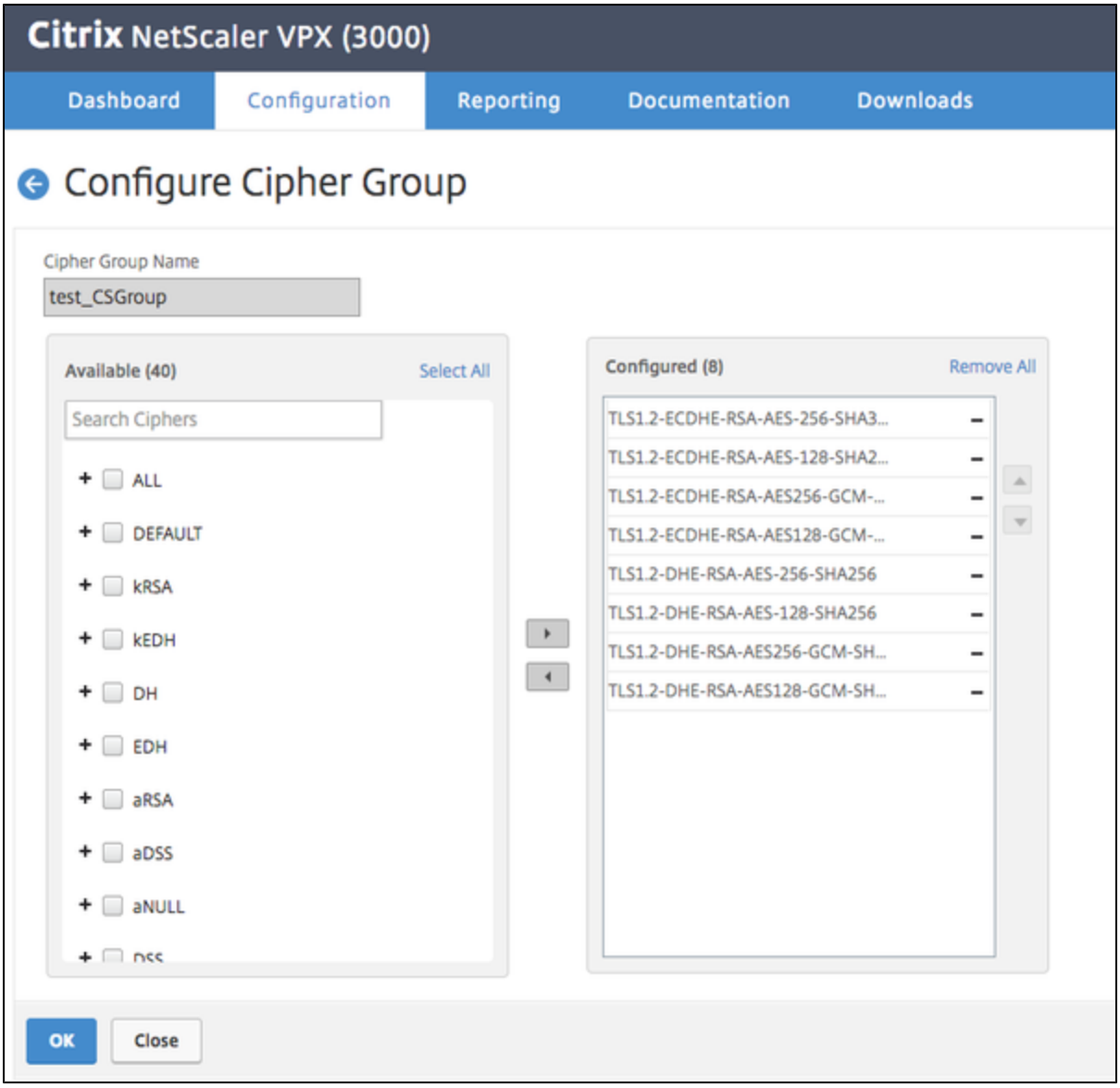
On the Traffic Management - SSL - Ciper Groups screen, select the Cipher Group you are using and click the Edit button.



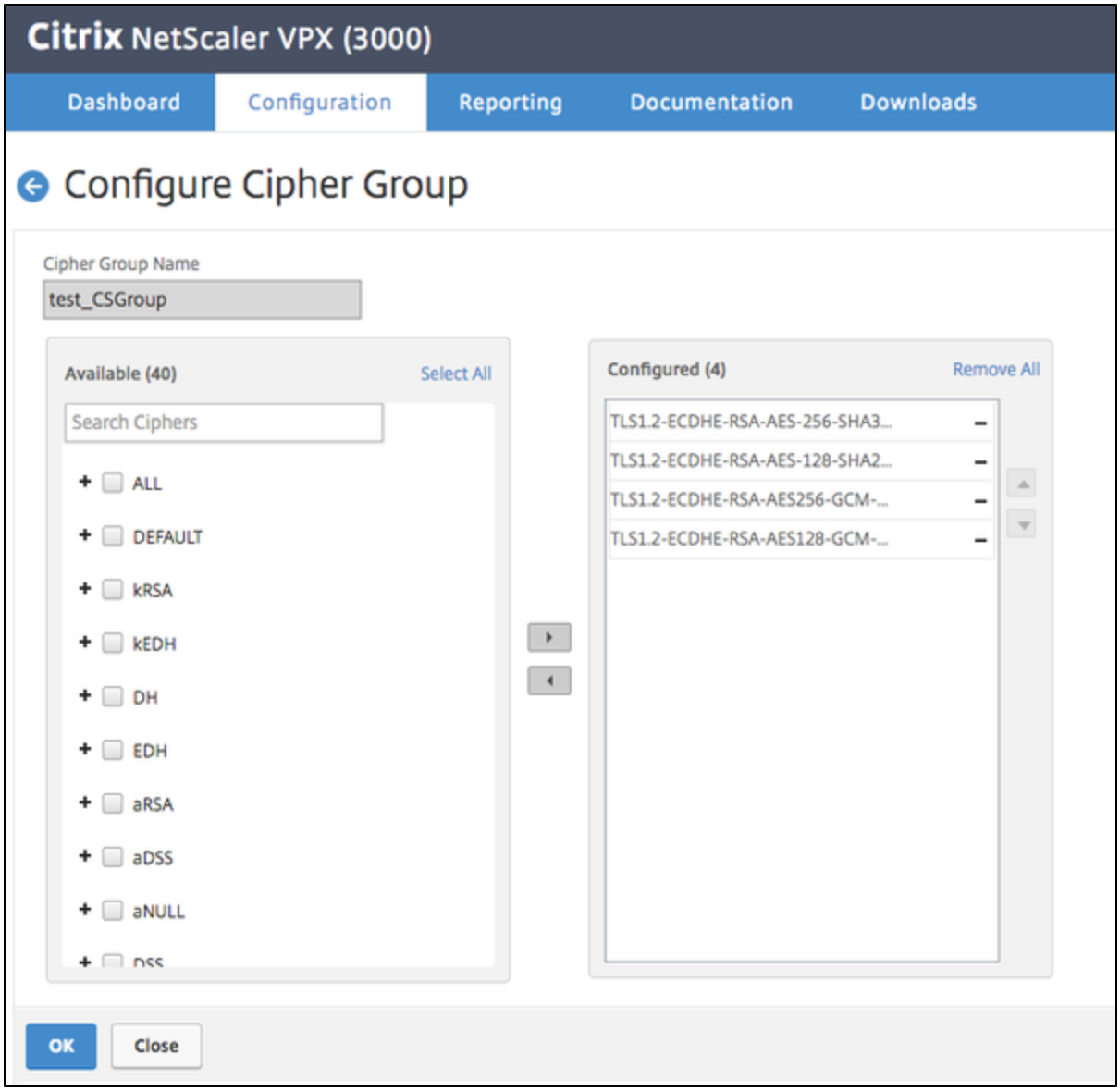
Click the Add button in the center.



From Configured in the right frame, click - on the right side of unnecessary CipherSuite and delete it.



After completing the above, click the OK button (TLS 1.2 - ECDHE - RSA is selected as an example in the screen below).



Setting method via CLI

Deauthorize client certificate for realserver

When using client certificate authentication, service's certkeyName is set.

```
bind ssl service test1 -certkeyName client_cert1
```

Execute the following command to unbind the client certificate.

```
> unbind ssl service test1 -certkeyName client_cert1
 Done
```

Regarding the client certificate, please also do not request client certificate when connecting with NetScaler in realserver.

Disable CipherSuite DHE

Check the CipherSuite with the SSL setting of VirtualServer.

```
*When using DEFAULT*
bind ssl service test1 -cipherName DEFAULT

*When specified separately (CipherSuite specified below is an example)*
bind ssl service test1 -cipherName TLS1.2-ECDHE-RSA-AES-256-SHA384
bind ssl service test1 -cipherName TLS1.2-ECDHE-RSA-AES-128-SHA256
bind ssl service test1 -cipherName TLS1.2-ECDHE-RSA-AES256-GCM-SHA384
bind ssl service test1 -cipherName TLS1.2-ECDHE-RSA-AES128-GCM-SHA256
bind ssl service test1 -cipherName TLS1.2-DHE-RSA-AES-256-SHA256 Please
delete this line.
bind ssl service test1 -cipherName TLS1.2-DHE-RSA-AES-128-SHA256 Please
delete this line.
bind ssl service test1 -cipherName TLS1.2-DHE-RSA-AES256-GCM-SHA384
Please delete this line.
bind ssl service test1 -cipherName TLS1.2-DHE-RSA-AES128-GCM-SHA256
Please delete this line.
```

If you use DEFAULT, delete the DEFAULT and set the required CipherSuite by executing the following command.

```
unbind ssl service test1 -cipherName DEFAULT
bind ssl service test1 -cipherName TLS1.2-ECDHE-RSA-AES-256-SHA384
bind ssl service test1 -cipherName TLS1.2-ECDHE-RSA-AES-128-SHA256
bind ssl service test1 -cipherName TLS1.2-ECDHE-RSA-AES256-GCM-SHA384
bind ssl service test1 -cipherName TLS1.2-ECDHE-RSA-AES128-GCM-SHA256
```

If specified individually, execute the following command and remove unnecessary CipherSuite.

```
unbind ssl service test1 -cipherName TLS1.2-DHE-RSA-AES-256-SHA256
unbind ssl service test1 -cipherName TLS1.2-DHE-RSA-AES-128-SHA256
unbind ssl service test1 -cipherName TLS1.2-DHE-RSA-AES256-GCM-SHA384
unbind ssl service test1 -cipherName TLS1.2-DHE-RSA-AES128-GCM-SHA256
```

* When creating and using CipherGroup including DHE.

```
bind ssl cipher test_CSGroup -cipherName TLS1.2-ECDHE-RSA-AES-256-SHA384
-cipherPriority 1
bind ssl cipher test_CSGroup -cipherName TLS1.2-ECDHE-RSA-AES-128-SHA256
-cipherPriority 2
bind ssl cipher test_CSGroup -cipherName
TLS1.2-ECDHE-RSA-AES256-GCM-SHA384 -cipherPriority 3
bind ssl cipher test_CSGroup -cipherName
TLS1.2-ECDHE-RSA-AES128-GCM-SHA256 -cipherPriority 4
bind ssl cipher test_CSGroup -cipherName TLS1.2-DHE-RSA-AES-256-SHA256
-cipherPriority 5 Please delete this line.
bind ssl cipher test_CSGroup -cipherName TLS1.2-DHE-RSA-AES-128-SHA256
-cipherPriority 6 Please delete this line.
bind ssl cipher test_CSGroup -cipherName
TLS1.2-DHE-RSA-AES256-GCM-SHA384 -cipherPriority 7 Please delete this
line.
bind ssl cipher test_CSGroup -cipherName
TLS1.2-DHE-RSA-AES128-GCM-SHA256 -cipherPriority 8 Please delete this
line.
```

Execute the following command and remove unnecessary CipherSuite.

```
unbind ssl cipher test_CSGroup -cipherName TLS1.2-DHE-RSA-AES-256-SHA256
unbind ssl cipher test_CSGroup -cipherName TLS1.2-DHE-RSA-AES-128-SHA256
unbind ssl cipher test_CSGroup -cipherName
TLS1.2-DHE-RSA-AES256-GCM-SHA384
unbind ssl cipher test_CSGroup -cipherName
TLS1.2-DHE-RSA-AES128-GCM-SHA256
```