

Countermeasures for vulnerability (CTX230612)

- Countermeasures
- Setting method
 - Setting method via GUI
 - Deauthorize client certificate for realserver
 - Disable CipherSuite DHE
 - Setting method via CLI
 - Deauthorize client certificate for realserver
 - Disable CipherSuite DHE

Countermeasures

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

- Stop using client certificate.
- Do not use Cipher 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

Citrix NetScaler VPX (3000) user-admin

Dashboard Configuration Reporting Documentation Downloads

Load Balancing Service

Basic Settings

Service Name	test1	Traffic Domain	LD
Server Name	TD_10_1.1.1.1	Number of Active Connections	-
IP Address	1.1.1.1	Hash ID	-
Server State	DOWN	Server ID	None
Protocol	SSL	Clear Text Port	-
Port	443	Cache Type	SERVER
Comments		Cacheable	NO
Monitoring Connection Close Bit	NONE	Health Monitoring	YES
		AppFlow Logging	ENABLED

Service Settings

Sure Connect	OFF	Use Source IP Address	YES
Surge Protection	YES	Client Keep-Alive	NO
Use Proxy Port	ENABLED	TCP Buffering	NO
Down State Flush	NO	Compression	NO
Access Down	NO	Insert Client IP Address	DISABLED
		Header	CLIENT_IP

Monitors

1 Service to Load Balancing Monitor Binding

SSL Parameters

Enable DH Param	DISABLED	SSL Redirect Port Rewrite	DISABLED	OCSP Stapling	DISABLED
Refresh Count	0	Enable Cipher Redirect	DISABLED	SSLv2 Redirect	DISABLED
File Path		Redirect URL		SSLv2 URL	
Enable DH Key Expire Size Limit	DISABLED	Send Close-Notify	YES	SSLv2	DISABLED
Enable Ephemeral RSA	DISABLED	SNI Enable	DISABLED	SSLv3	DISABLED
Refresh Count	0	HSTS		TLSv1	DISABLED
Enable Session Reuse	ENABLED	Max Age		TLSv1.1	DISABLED
Time-out	300	Include Subdomains		TLSv1.2	ENABLED
SSL Redirect	DISABLED	Enable Server Authentication	DISABLED		
DTLS Profile	-	Client Authentication	DISABLED		
Strict Signature Digest Check	DISABLED	Client Certificate			

SSL Ciphers

Configured (8)

- Remove All
- TLSS2-ECDFE-RSA-AES-256-SHA384
- TLSS2-ECDFE-RSA-AES-128-SHA256
- TLSS2-ECDFE-RSA-AES256-GCM-SHA384
- TLSS2-ECDFE-RSA-AES128-GCM-SHA256
- TLSS2-DHE-RSA-AES-256-SHA256
- TLSS2-DHE-RSA-AES-128-SHA256
- TLSS2-DHE-RSA-AES256-GCM-SHA384
- TLSS2-DHE-RSA-AES128-GCM-SHA256

Certificate

- 1 CA Certificates
- 1 Client Certificate

Done

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

Citrix NetScaler VPX (3000) user-admin

Dashboard Configuration Reporting Documentation Downloads

Load Balancing Service

SSL Service Client Certificate Binding

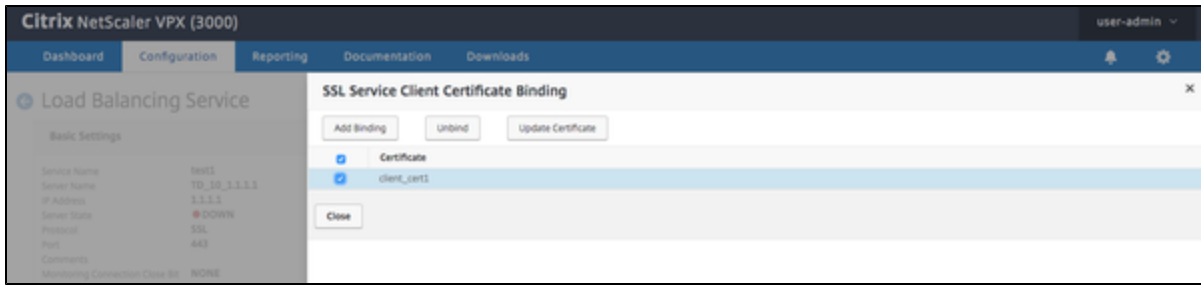
Add Binding Unbind Update Certificate

Certificate

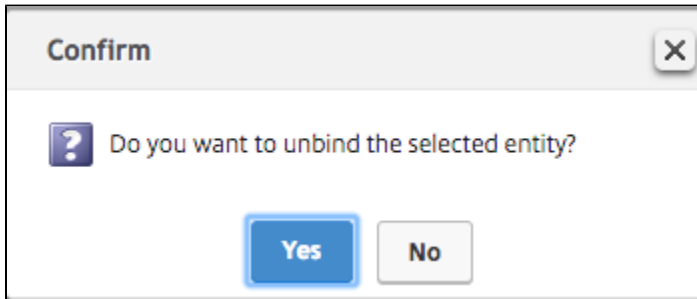
client_cert1

Close

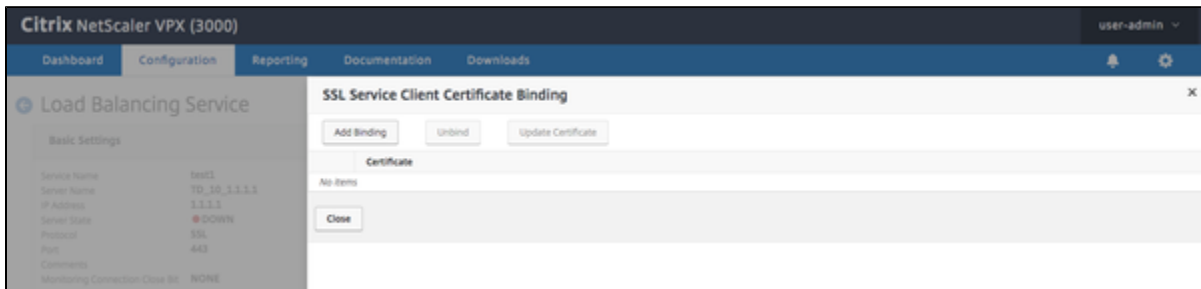
Select the client certificate and click the Unbind button.



Select Yes if the following message is displayed.



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



Citrix NetScaler VPX (3000) user-admin

Dashboard Configuration Reporting Documentation Downloads

Load Balancing Service

Basic Settings

Service Name	test1	Traffic Domain	10
Server Name	TD_10_1.1.1.1	Number of Active Connections	-
IP Address	1.1.1.1	Hash ID	-
Server State	● DOWN	Server ID	None
Protocol	SSL	Clear Text Port	-
Port	443	Cache Type	SERVER
Comments		Cacheable	NO
Monitoring Connection Close Bit	NONE	Health Monitoring	YES
		AppFlow Logging	ENABLED

Service Settings

Sure Connect	OFF	Use Source IP Address	YES
Surge Protection	YES	Client Keep-Alive	NO
Use Proxy Port	ENABLED	TCP Buffering	NO
Down State Flush	NO	Compression	NO
Access Down	NO	Insert Client IP Address Header	DISABLED (REMOVED)

Monitors

Service to Load Balancing Monitor Binding

SSL Parameters

Enable DH Param	DISABLED	SSL Redirect Port Rewrite	DISABLED	OCSP Stapling	DISABLED
Refresh Count	0	Enable Cipher Redirect	DISABLED	SSLv2 Redirect	DISABLED
File Path		Redirect URL		SSLv2 URL	
Enable DH Key Expire Size Limit	DISABLED	Send Close-Notify	YES	SSLv3 URL	DISABLED
Enable Ephemeral RSA	DISABLED	SN Enable	DISABLED	SSLv3	DISABLED
Refresh Count	0	HSTS		TLsv1	DISABLED
Enable Session Reuse	ENABLED	Max-Age		TLsv1.1	DISABLED
Time-out	300	Include Subdomains		TLsv1.2	ENABLED
SSL Redirect	DISABLED	Enable Server Authentication	DISABLED		
DTLS Profile	-	Client Authentication	DISABLED		
Strict Signature Digest Check	DISABLED	Client Certificate			

SSL Ciphers

Configured (8) Remove All

- TLSSL2-ECDH-RSA-AES-256-SHA384
- TLSSL2-ECDH-RSA-AES-128-SHA256
- TLSSL2-ECDH-RSA-AES256-GCM-SHA384
- TLSSL2-ECDH-RSA-AES128-GCM-SHA256
- TLSSL2-DHE-RSA-AES-256-SHA256
- TLSSL2-DHE-RSA-AES-128-SHA256
- TLSSL2-DHE-RSA-AES256-GCM-SHA384
- TLSSL2-DHE-RSA-AES128-GCM-SHA256

Certificate

CA Certificates

No Client Certificate

Done

Help

Advanced Settings

- + Thresholds & Timeouts
- + Profiles
- + Policies
- + SSL Profile
- + SSL Policies
- + ECC Curve

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.

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	OFF
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 Header	DISABLED
	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
TLSv1.1	DISABLED
TLSv1.2	ENABLED

SSL Ciphers
Configured (1) Remove All
DEFAULT



- Help
- Advanced Settings
 - Thresholds & Timeouts
 - Profiles
 - Policies
 - SSL Profile
 - SSL Policies
 - ECC Curve

Load Balancing Service

Basic Settings

Service Name	test1	Traffic Domain	10
Server Name	TD_10_1.1.1.1	Number of Active Connections	-
IP Address	1.1.1.1	Hash ID	-
Server State	DOWN	Server ID	None
Protocol	SSL	Clear Text Port	-
Port	443	Cache Type	SERVER
Comments		Cacheable	NO
Monitoring Connection Close Bit	NONE	Health Monitoring	YES
		Appflow Logging	ENABLED

Service Settings

Sure Connect	OFF	Use Source IP Address	YES
Surge Protection	YES	Client Keep-Alive	NO
Use Proxy Port	ENABLED	TCP Buffering	NO
Down State Flush	NO	Compression	NO
Access Down	NO	Insert Client IP Address	DISABLED
		Header	client-ip

Monitors

1 Service to Load Balancing Monitor Binding

SSL Parameters

Enable DH Param	DISABLED	SSL Redirect Port Rewrite	DISABLED	OCSP Stapling	DISABLED
Refresh Count	0	Enable Cipher Redirect	DISABLED	SSLv2 Redirect	DISABLED
File Path		Redirect URL		SSLv2 URL	
Enable DH Key Expire Size Limit	DISABLED	Send Close-Notify	YES	SSLv2	DISABLED
Enable Ephemeral RSA	DISABLED	SNI Enable	DISABLED	SSLv3	DISABLED
Refresh Count	0	HSTS		TLSv1	DISABLED
Enable Session Reuse	ENABLED	Max Age		TLSv1.1	DISABLED
Time-out	300	Include Subdomains		TLSv1.2	ENABLED
SSL Redirect	DISABLED	Enable Server Authentication	DISABLED		
DTLS Profile	-	Client Authentication	DISABLED		
Strict Signature Digest Check	DISABLED	Client Certificate			

SSL Ciphers

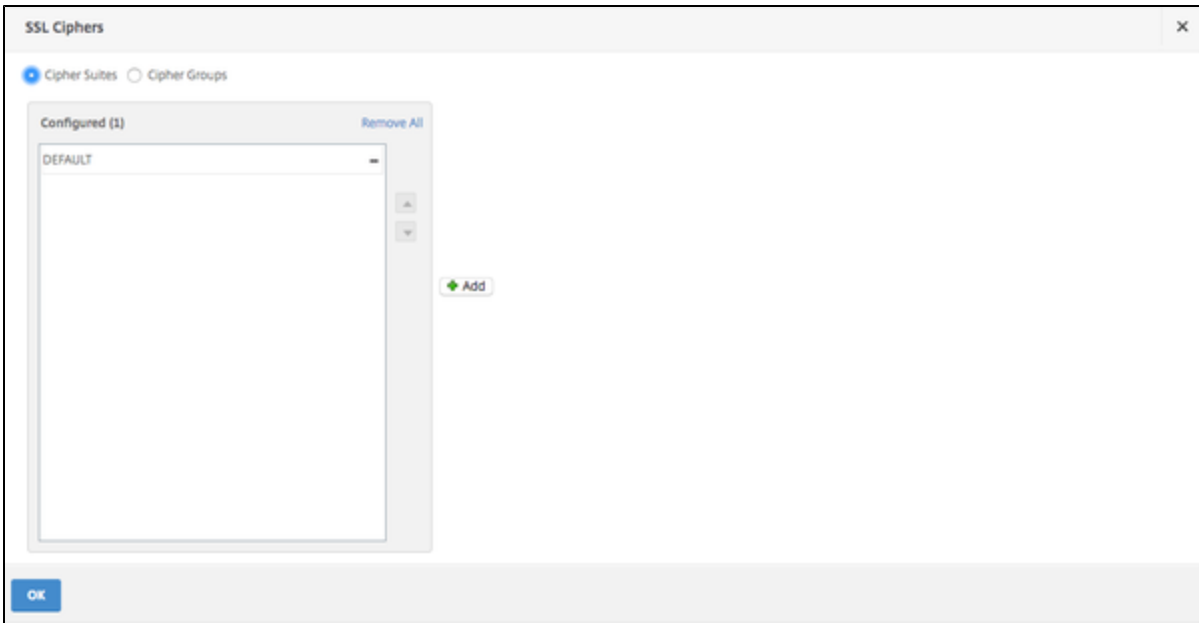
Configured (8)	Remove All
TLS1.2-ECDHE-RSA-AES-256-SHA384	-
TLS1.2-ECDHE-RSA-AES-128-SHA256	-
TLS1.2-ECDHE-RSA-AES256-GCM-SHA384	-
TLS1.2-ECDHE-RSA-AES128-GCM-SHA256	-
TLS1.2-DHE-RSA-AES-256-SHA256	-
TLS1.2-DHE-RSA-AES-128-SHA256	-
TLS1.2-DHE-RSA-AES256-GCM-SHA384	-
TLS1.2-DHE-RSA-AES128-GCM-SHA256	-

Help

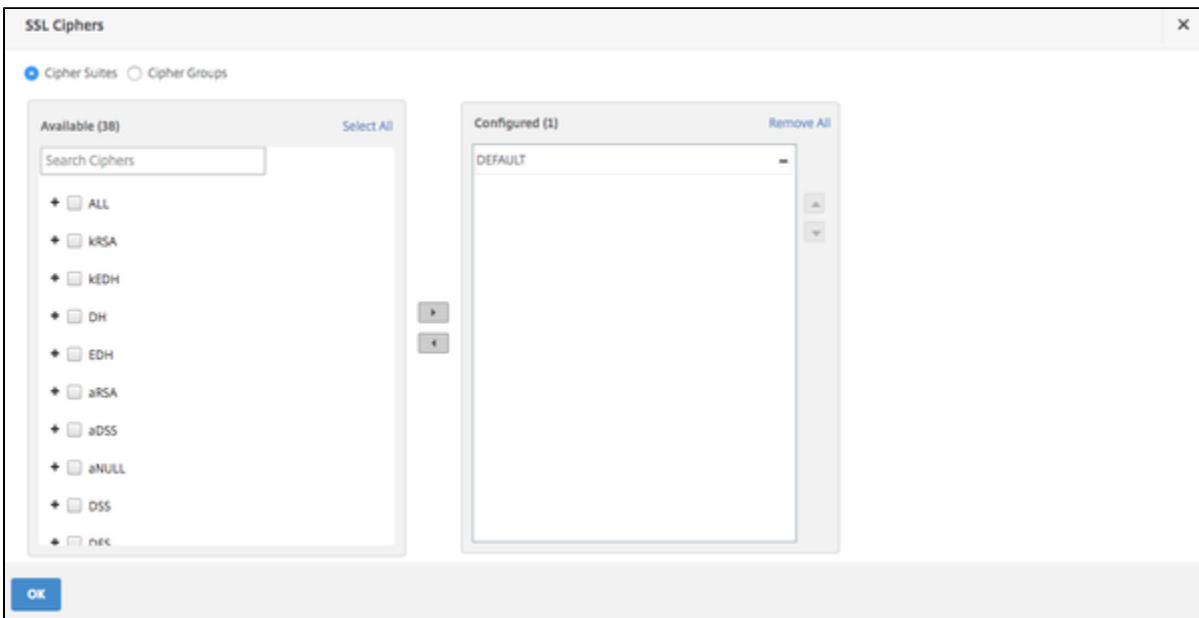
Advanced Settings

- + Thresholds & Timeouts
- + Profiles
- + Policies
- + SSL Profile
- + SSL Policies
- + ECC Curve

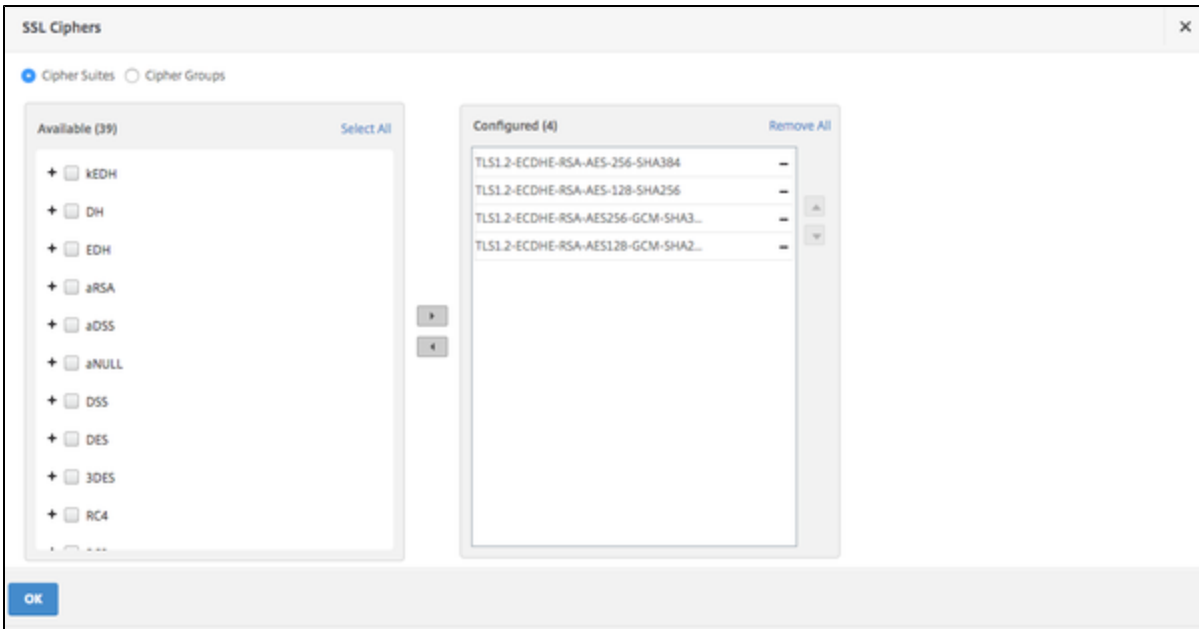
Click the SSL Ciphers edit button and the Add button in the center.



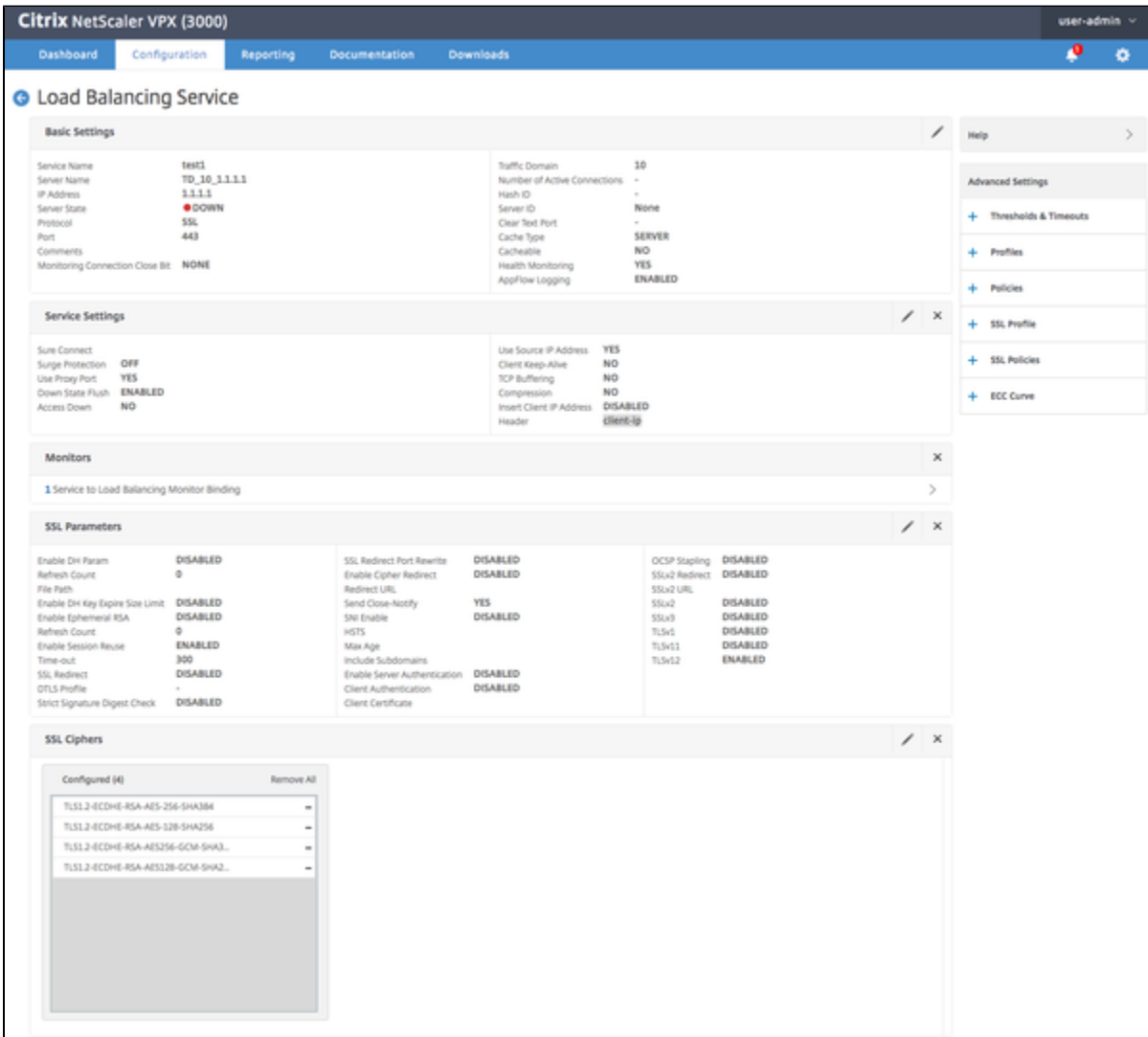
Select the necessary CipherSuite from Available on the left frame and click the rightward button at the center to add it. Also, click - on the right side of unnecessary CipherSuite from Configured in the right frame and delete it.



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 - Cipher Groups screen, select the Cipher Group you are using and click the Edit button.

The screenshot shows the Citrix NetScaler VPX (3000) interface. The top navigation bar includes Dashboard, Configuration, Reporting, Documentation, and Downloads. The user is logged in as 'user-admin'. The left sidebar shows the navigation menu with 'Traffic Management' expanded. The main content area is titled 'Cipher Groups' and contains a table of cipher groups. The 'test_CSGroup' entry is selected, and the 'Add' button is highlighted.

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	EXP	Export ciphers
<input type="checkbox"/>	EXPORT	Export ciphers
<input type="checkbox"/>	EXPORT40	Export ciphers with 40bit encryption
<input type="checkbox"/>	EXPORT56	Export ciphers with 56bit encryption
<input type="checkbox"/>	LOW	Low strength ciphers (56bit encryption)
<input type="checkbox"/>	MEDIUM	Medium strength ciphers (128bit encryption)
<input type="checkbox"/>	HIGH	High strength ciphers (168bit encryption)
<input type="checkbox"/>	AES	AES Ciphers
<input type="checkbox"/>	FIPS	FIPS Approved Ciphers
<input type="checkbox"/>	ECDHE	Elliptic Curve Ephemeral DH Ciphers
<input type="checkbox"/>	AES-GCM	Ciphers with Enc algo as AES-GCM
<input type="checkbox"/>	SHA2	Ciphers with MAC algo as SHA-2
<input type="checkbox"/>	DEFAULT_BACKEND	Default cipher list for Backend SSL session
<input type="checkbox"/>	ECDSA	Ciphers with Auth algo as ECDSA
<input checked="" type="checkbox"/>	test_CSGroup	User Defined Cipher Group

Total 40 25 Per Page Page 2 of 2

Click the Add button in the center.

← Configure Cipher Group

Cipher Group Name

test_CSGroup

Configured (8)

Remove All

TLS1.2-ECDHE-RSA-AES-256-SHA3...	-
TLS1.2-ECDHE-RSA-AES-128-SHA2...	-
TLS1.2-ECDHE-RSA-AES256-GCM-...	-
TLS1.2-ECDHE-RSA-AES128-GCM-...	-
TLS1.2-DHE-RSA-AES-256-SHA256	-
TLS1.2-DHE-RSA-AES-128-SHA256	-
TLS1.2-DHE-RSA-AES256-GCM-SH...	-
TLS1.2-DHE-RSA-AES128-GCM-SH...	-

+ Add

OK

Close

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

Citrix NetScaler VPX (3000)

Dashboard Configuration Reporting Documentation Downloads

← Configure Cipher Group

Cipher Group Name
test_CSGroup

Available (40) [Select All](#)

Search Ciphers

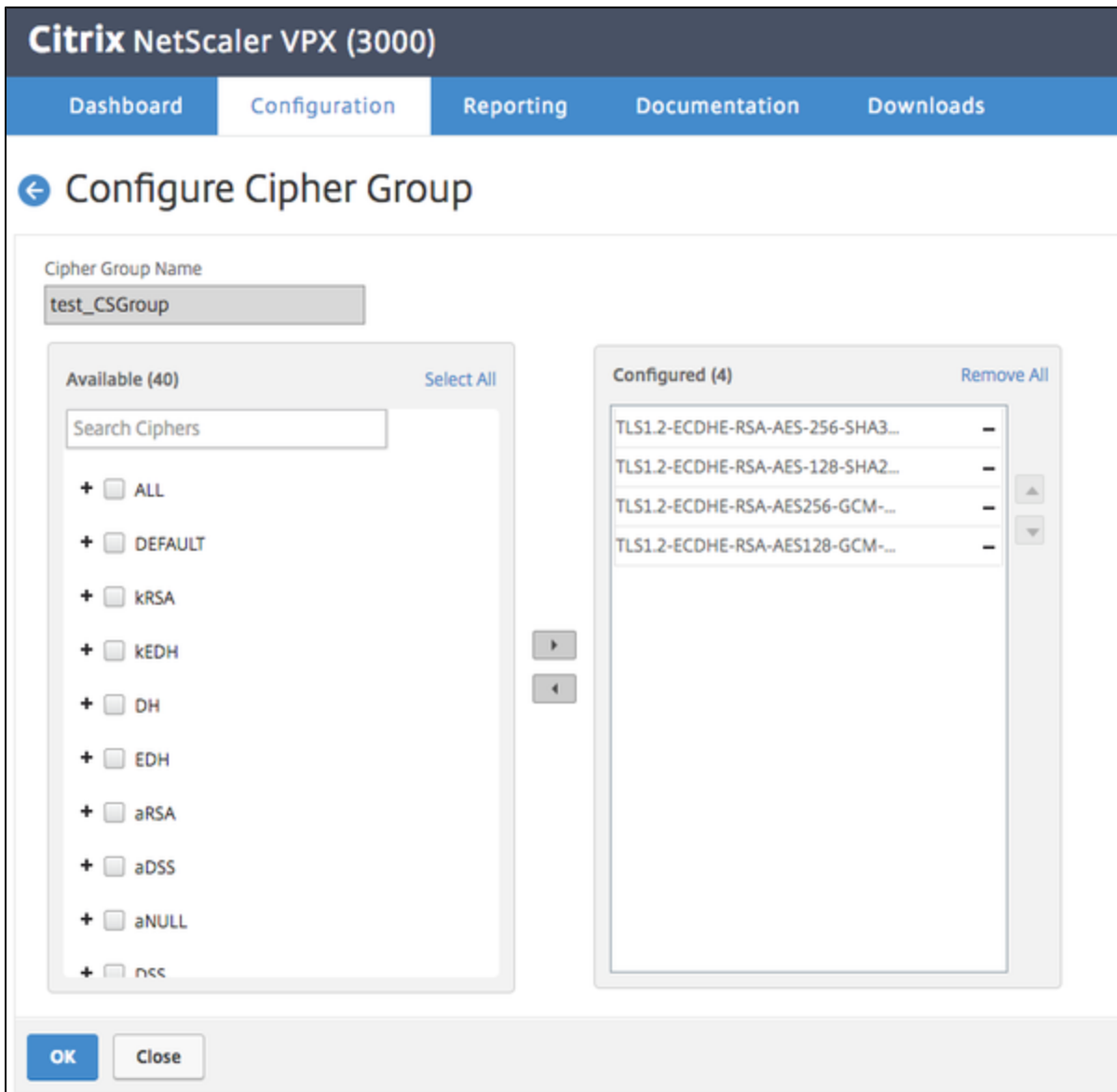
- + ALL
- + DEFAULT
- + kRSA
- + kEDH
- + DH
- + EDH
- + aRSA
- + aDSS
- + aNULL
- + NULL

Configured (8) [Remove All](#)

TLS1.2-ECDHE-RSA-AES-256-SHA3...	-
TLS1.2-ECDHE-RSA-AES-128-SHA2...	-
TLS1.2-ECDHE-RSA-AES256-GCM-...	-
TLS1.2-ECDHE-RSA-AES128-GCM-...	-
TLS1.2-DHE-RSA-AES-256-SHA256	-
TLS1.2-DHE-RSA-AES-128-SHA256	-
TLS1.2-DHE-RSA-AES256-GCM-SH...	-
TLS1.2-DHE-RSA-AES128-GCM-SH...	-

OK Close

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
```