

# ISE 통합 문제 해결

## 목차

---

[소개](#)

[모범 사례 개요](#)

[CCV-ISE 상위 레벨 플로우 다이어그램](#)

[문제 해결 지침](#)

[수집할 데이터](#)

[예상 로그 메시지](#)

[관련 정보](#)

---

## 소개

이 문서에서는 CyberVision Center와 ISE의 통합을 위한 트러블슈팅 단계에 대해 설명합니다.

## 모범 사례 개요

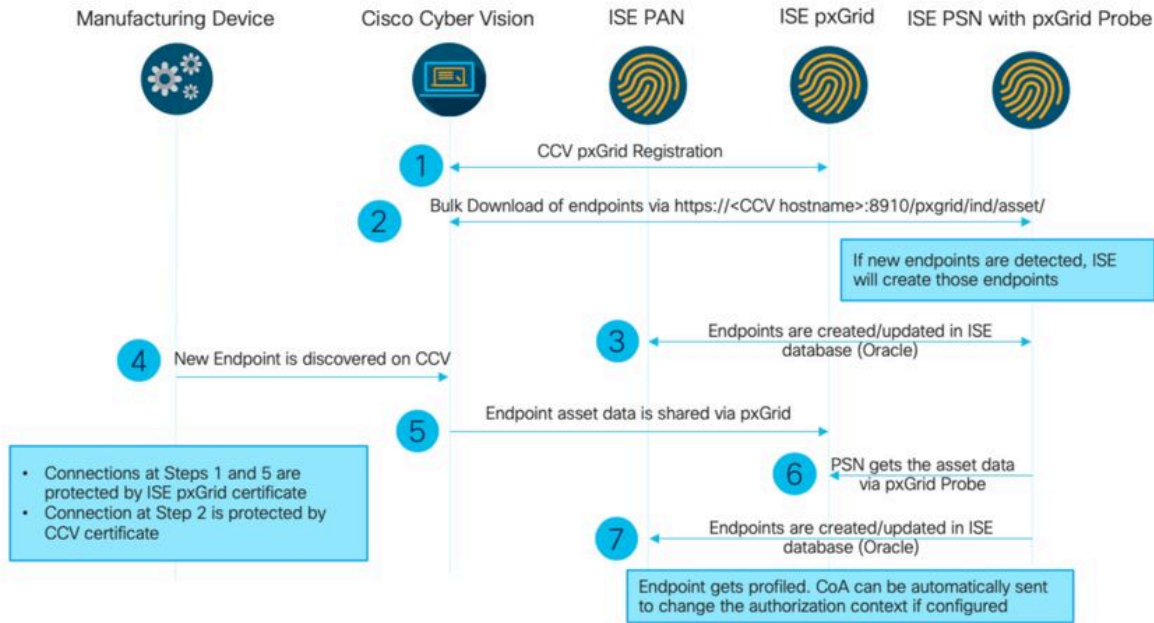
모범 사례는 시스템 컨피그레이션의 올바른 작동을 보장하기 위해 반드시 고려해야 하는 권장 단계입니다. 권장 사항:

- 최신 기능, 지침, 제한 사항 및 주의 사항은 Cisco Cyber Vision 릴리스 노트 및 Cisco ISE(Identity Services Engine) 릴리스 노트를 참조하십시오
- 새 컨피그레이션 변경 사항을 구현한 후 이를 확인하고 트러블슈팅합니다

## CCV-ISE 하이 레벨 플로우 다이어그램

## Configure

### High-Level Flow Diagram



## 문제 해결 지침

다음 질문에 답하면 문제 해결 경로와 추가 조사가 필요한 구성 요소를 확인할 수 있습니다. 설치 상태를 확인하려면 다음 질문에 답하십시오.

- 새로 설치한 시스템입니까, 아니면 기존 시스템입니까?
- CyberVision에서 ISE를 볼 수 있었습니까?

명령을 사용하여 pxGrid 서비스 상태를 확인합니다 `systemctl status pxgrid-agent`.

```

root@center1:~# systemctl status pxgrid-agent
● pxgrid-agent.service - Agent for interfacing with pxGrid
   Loaded: loaded (/lib/systemd/system/pxgrid-agent.service; enabled)
   Active: active (running) since Wed 2021-03-17 20:12:15 UTC; 17min ago
     Process: 28434 ExecStop=/usr/bin/lxc-stop -n pxgrid-agent (code=exited, status=0/SUCCESS)
    Main PID: 28447 (lxc-start)
      CGroup: /system.slice/pxgrid-agent.service
              └─28447 /usr/bin/lxc-start -F -n pxgrid-agent

Mar 17 20:12:15 center lxc-start[28447]: lxc-start: cgfsng.c: create_path_for_hierarchy: 1306 Path "/sys/fs/cgroup/pids//lxc/pxgrid-agent-6" already exists.
Mar 17 20:12:15 center lxc-start[28447]: lxc-start: cgfsng.c: cgfsng_create: 1363 File exists - Failed to create /sys/fs/cgroup/pids//lxc/pxgrid-agent-6: File exists
Mar 17 20:12:15 center lxc-start[28447]: pxgrid-agent Center type: standalone [caller=postgres.go:290]
Mar 17 20:12:16 center lxc-start[28447]: pxgrid-agent HTTP server listening to: '169.254.0.90:2027' [caller=main.go:135]
Mar 17 20:12:16 center lxc-start[28447]: pxgrid-agent RPC server listening to: '/tmp/pxgrid-agent.sock' [caller=main.go:102]
Mar 17 20:12:16 center lxc-start[28447]: pxgrid-agent Account activated [caller=pxgrid.go:81]
Mar 17 20:12:16 center lxc-start[28447]: pxgrid-agent Service registered, ID: 3d7bee0f-3840-4dc7-a121-a8740f86fa06 [caller=pxgrid.go:99]
Mar 17 20:13:19 center lxc-start[28447]: pxgrid-agent API: getSyncStatus [caller=sync_status.go:34]
Mar 17 20:13:19 center lxc-start[28447]: pxgrid-agent Cyber Vision is in sync with ISE [caller=assets.go:67]
Mar 17 20:23:19 center lxc-start[28447]: pxgrid-agent API: getSyncStatus [caller=sync_status.go:34]
    
```

- ISE에서 pxGrid를 고가용성으로 실행합니까?
- 애플리케이션이 문제를 일으키기 직전에 구성 또는 전체 인프라에서 어떤 변화가 있었습니까?

네트워크 문제를 발견하려면 일반적인 네트워크 문제 해결 단계를 사용합니다.

1단계. ISE에서 CyberVision Center 호스트 이름을 ping할 수 있습니까?

```

ESCISE2/admin# ping center
PING center (10.2.3.138) 56(84) bytes of data.
64 bytes from 10.2.3.138: icmp_seq=1 ttl=64 time=1.53 ms
64 bytes from 10.2.3.138: icmp_seq=2 ttl=64 time=1.73 ms
64 bytes from 10.2.3.138: icmp_seq=3 ttl=64 time=1.87 ms
64 bytes from 10.2.3.138: icmp_seq=4 ttl=64 time=1.80 ms

--- center ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.539/1.737/1.878/0.125 ms

```

ping할 수 없는 경우 SSH(Secure Shell)를 사용하여 ISE CLI에 연결하고 호스트 이름을 추가합니다.

```

ESCISE2/admin# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ESCISE2/admin(config)# ip host 10.2.3.138 center
Add Host alias was modified. You must restart ISE for change to take effect.
Do you want to restart ISE now? (yes/no) yes

```

2단계. CyberVision Center에서 ISE 호스트 이름을 ping할 수 있습니까?

```

root@center:~# ping ESCISE2.ccv.local
PING ESCISE2.ccv.local (10.2.3.118) 56(84) bytes of data.
64 bytes from ESCISE2.ccv.local (10.2.3.118): icmp_seq=1 ttl=64 time=2.04 ms
64 bytes from ESCISE2.ccv.local (10.2.3.118): icmp_seq=2 ttl=64 time=1.88 ms
64 bytes from ESCISE2.ccv.local (10.2.3.118): icmp_seq=3 ttl=64 time=1.75 ms
64 bytes from ESCISE2.ccv.local (10.2.3.118): icmp_seq=4 ttl=64 time=1.98 ms
64 bytes from ESCISE2.ccv.local (10.2.3.118): icmp_seq=5 ttl=64 time=2.02 ms
64 bytes from ESCISE2.ccv.local (10.2.3.118): icmp_seq=6 ttl=64 time=1.97 ms
^C
--- ESCISE2.ccv.local ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5006ms
rtt min/avg/max/mdev = 1.754/1.945/2.045/0.109 ms

```

그렇지 않은 경우 ISE 호스트 이름을 Center의 /data/etc/hosts 파일에 추가해 봅니다.

```

root@Center:~# cat /data/etc/hosts
127.0.0.1        localhost.localdomain        localhost

# The following lines are desirable for IPv6 capable hosts
::1            localhost ip6-localhost ip6-loopback
fe00::0        ip6-localnet
ff00::0        ip6-mcastprefix
ff02::1        ip6-allnodes
ff02::2        ip6-allrouters
127.0.1.1      center
10.48.60.131  ise31-tm2.cisco.com

```

3단계. 인증서 문제를 검색합니다.

CyberVision Centeropenssl s\_client -connect YourISEHostname:8910에서 명령을 입력합니다.

```
root@center:~# openssl s_client -connect ESCISE2.ccv.local:8910
CONNECTED(00000003)
depth=3 CN = Certificate Services Root CA - ESCISE2
verify error:num=19:self signed certificate in certificate chain
verify return:1
depth=3 CN = Certificate Services Root CA - ESCISE2
verify return:1
depth=2 CN = Certificate Services Node CA - ESCISE2
verify return:1
depth=1 CN = Certificate Services Endpoint Sub CA - ESCISE2
verify return:1
depth=0 OU = Certificate Services System Certificate, CN = ESCISE2.ccv.local
verify return:1
```

---  
Certificate chain

- 0 s:OU = Certificate Services System Certificate, CN = ESCISE2.ccv.local  
i:CN = Certificate Services Endpoint Sub CA - ESCISE2
- 1 s:CN = Certificate Services Endpoint Sub CA - ESCISE2  
i:CN = Certificate Services Node CA - ESCISE2
- 2 s:CN = Certificate Services Node CA - ESCISE2  
i:CN = Certificate Services Root CA - ESCISE2
- 3 s:CN = Certificate Services Root CA - ESCISE2  
i:CN = Certificate Services Root CA - ESCISE2

---  
Server certificate

-----BEGIN CERTIFICATE-----

```
MIIF3jCCA8agAwIBAgIQUKVBBihpQhWBK5cZEjFpeDANBgkqhkiG9w0BAQsFADA5
MTcwNQYDVQQDDDC5DZXJ0aWZpY2F0ZSBTZXJ2aWNlcyBFbWVud2ludCBTdWIgQ0Eg
LSBFU0NlU0UyMB4XDTEwMTEwXDI1MTEzMDE3Mjc1M1owTjEwMjE0MDEyMDE3MjE0
MDE3MDE3MDE3MDE3MDE3MDE3MDE3MDE3MDE3MDE3MDE3MDE3MDE3MDE3MDE3MDE3
A1UECwnQ2VydG1maWNhdGUU2VydmljZXZlbnR1eXN1eXN1eXN1eXN1eXN1eXN1eXN1
GAYDVQQDBBFU0NlU0UyLmNjdi5sb2NhbDCCAiIwdQYJKoZIhvcNAQEBBQADggIP
ADCCAg0CgIBANE1Ukx/7QnUdrCIXJLUXgOXWTvOFTNme4L16yDFsLvytGjFqYfR
RCRM/kzRVjDk8f/cSSP9T+5pR/JA+PbOZqkAWWDJVAQh1ndqL0kX7UaCCodKUWon
DafVimPjKqV1RScd8bwVDxAr7gYou3S4BcCe00s1x5pL1WyZw6F6MPze2F388kSR
GuSRsn40ZM4JjDDeaxSBrS789f7zACw4eMZIfRDk0RL9qzMtoghIU089/1VuacUb
WYrF0e0mThUWg7wk7dFv4bozyWeHjdqsbEtb0Geme8ZWPX5ZYddSKjWhOrNUXeQV
NvDBUXhb5NpSsKYMocqnvIv+JYzkIV6ukksX9xqI5bL3/vik/CyPVMexIOJo64dK
S0vMjrcnmpNznoLzEv3mgvgp9mJhcTROg86wlyOrOzjOoMCGGLrhpgxuLeVatFKv
GLWjsmrWcLk/FOAe4H+tb6/+yO7KNXTSX+nP1z5epDA8stzvLxm1ylw65XdeEBho
m0qgGEKx5y/I/2b+myi24ZYrqsV64KpohCisIvZxbCG/2q77SP7ml8v8+BidpMaW
LZr20tD2XRJeyhPypRBYwV4QDBWpn+mCAFgpNd3KC36zAn138c2WW1Hs0PKhReMX
vNn+SwtKmyIbM09Oeww5zRSdMU90zPcFkY0qvrBUD31Gf5fAiWqImkVAgMBAAGj
gcwgckwaAYDVR0jBGEwX4Uuxz+SV+KtR/CpwGiyNg+mp/xxiAqhNaQzMDExLzAt
BgNVBAMMJkNlcnRpZmljYXR1IFNlcnZpY2VzIE5vZGUGQ0EgLSBFU0NlU0UyYghAx
lcB30YJL0Kwj6XolaV7SMB0GA1UdDgQWBRRigvgT63FOqKmS9m9COhW3ahdv8jAO
BgNVHQ8BAf8EBAMCBeAwIAVDVR01AQH/BBYwFAYIKwYBBQUHAWEGCCsGAQUFBwMC
MAwGA1UdEwEB/wQCMAAwDQYJKoZIhvcNAQELBQADggIBADwnDKtdHj/y3Pj4ADDV
57RrdHsiU/EkkWGLzmP/aMKJ9rY7f6eUDlig6b6gpJ8B0MnTPI9VfVduc++oZDEt
CrIMMwFexnbnhPWJfzjSNJpNAMIgFUeiPuoxBJYkjFzhiXtat0fOmdm5RbEu5W1a
f7EEbd/XOIRTMyIxqubXQct6pE61y9gBPuQU9Hvd5QpcLX77LSfEroJhkD4dmuRs
o4uj0wWKFtXW+yLWhwjkiieoBuREEU8Gvtk+iq+11mThfpeP32fV2IO/WIo4SKh0
ILkzS206rbSxxatKDQ6jZds3a5YKyFtR55r7VndmX0I4sqXI9dFQjTPVfW7TEbK
GPds+vMe4J9g4c1KGRhiXNiNzfb5S3eWzOL/2o9ZgWS1u7R7GVXK1YrvSHMieL3t
n/p+ov8cogr0o06jXFItZ+Rsnp11Kbq+DrsoCE/i26QgkTKBruMfhz6P8k/2aLqQ
MwJp0dhH1SfMkWCAGQpapoX3lpK36FUTA3sZL2mdN/XyK5UutLbLJx87elwunp
w6Cxz5MA97NXOUZIUqThnTG7Ibu8pzwl1XZyt1f1T50luCoY2CkVbU93rqfD4zyr
WyK2a0BmizcKXD+F8Yti4fm4Kvl0bpWihUNPPMTmgwJMUOW+zdC7b7g13j5rnE9X
lyFJ3uHTohidxEtXi4XsiCn5
```

-----END CERTIFICATE-----

subject=OU = Certificate Services System Certificate, CN = ESCISE2.ccv.local

수집할 데이터

네트워크 문제의 경우:

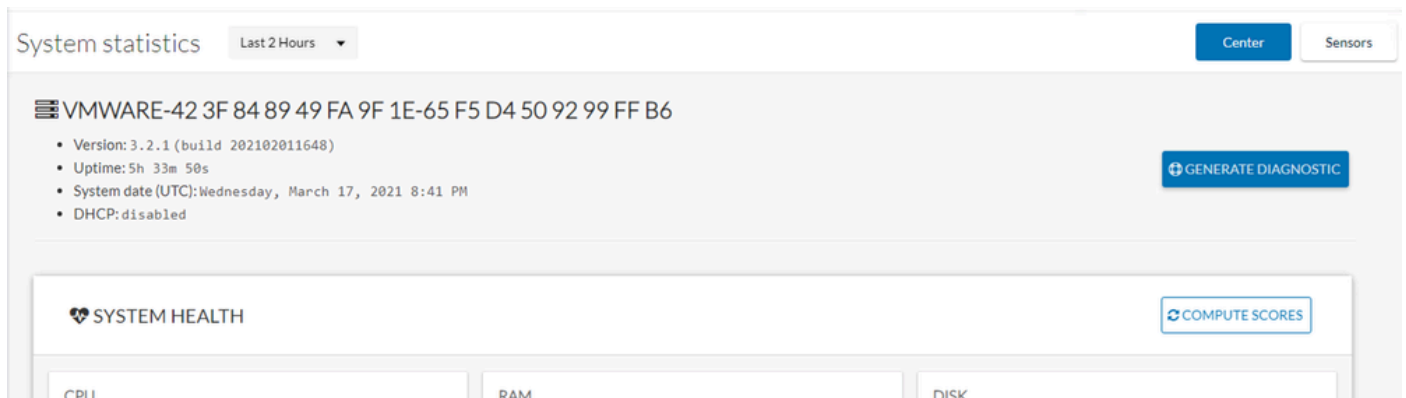
- 아키텍처:

센터와 ISE 간의 세부 정보를 보여 주는 체계가 유용합니다.

- 방화벽 규칙
- 고정 경로
- 게이트웨이 컨피그레이션
- VLAN 컨피그레이션

- 모든 ISE 문제에 대해 수집할 로그:

데이터 손실을 방지하기 위해 센터 진단 파일을 수집하는 것으로 시작할 수 있습니다.



그런 다음 다음 다음 다음 절차를 사용하여 센터에 고급 로그를 활성화합니다.

폴더에 두 개의 파일을 만듭니다/data/etc/sbs.

첫 번째 파일의 이름은 listener.conf 다음과 같이 지정해야 합니다.

(loglevel 앞에 있는 선행 공백을 참고하십시오.)

```
root@Center:~# cat /data/etc/sbs/listener.conf
configlog:
loglevel: debug
root@Center:~#
```

두 번째 파일은 이름이 지정되어야 하며pxgrid-agent.conf 다음 내용을 포함해야 합니다.

(loglevel 앞에 있는 선행 공백을 참고하십시오.)

```
root@Center:~# cat /data/etc/sbs/pxgrid-agent.conf
configlog:
loglevel: debug
```

두 파일이 모두 생성되면 센터를 재부팅하거나 및 서비스를sbs-burrow 다시 pxgrid-agent 시작합니다.

Restart service using the command:

```
#systemctl restart sbs-burrow
#systemctl restart pxgrid-agent
```

그런 다음 pxGrid 로그를 수집합니다(중앙에서 로그를 내보내려면 파일 전송 툴 사용).

```
root@Center:~# journalctl -u pxgrid-agent > /data/tmp/pxgridLogs.log
```

Center와 ISE 간의 통신 흐름을 분석하기 위한 tcpdump 캡처를 수집합니다.

```
root@Center:~# tcpdump -i eth0 -n host CCV_IP and host ISE_IP -w /data/tmp/ccv_ise.pcap
```

- ISE에서 디버그를 활성화하고 지원 번들을 수집합니다.

ISE에서 디버그를 활성화하려면 로 Administration > System > Logging > Debug Log Configuration 이동합니다. 로그 레벨을 다음으로 설정합니다.

페르소나	구성 요소 이름	로그 레벨	확인할 파일	
PAN(선택 사항)	프로 파 일러	디버그	profiler.log	
pxGrid 프로브가 활성화된 PSN	프로 파 일러	디버그	profiler.log	

PxGrid	pxgrid	추적	pxgrid-server.log	
--------	--------	----	-------------------	--

예상 로그 메시지

센터에 있는 pxGrid-agent의 디버그 로그에는 에이전트 시작, 서비스 등록, Cisco Cyber Vision(CCV) ISE와의 단순(또는 스트리밍) STOMP(Text Oriented Messaging Protocol) 연결 설정, 자산/구성 요소에 대한 업데이트 작업 전송 등이 표시됩니다.

<#root>

Jul 11 13:05:02 center systemd[1]:

**Started Agent**

for interfacing with pxGrid.

```
Jul 11 13:05:02 center pxgrid-agent[5404]: pxgrid-agent Center type: standalone [caller=postgres.go:543]
Jul 11 13:05:03 center pxgrid-agent[5404]: pxgrid-agent RPC server listening to: '/tmp/pxgrid-agent.sock'
Jul 11 13:05:03 center pxgrid-agent[5404]: pxgrid-agent HTTP server listening to: '169.254.0.90:2027' [
Jul 11 13:05:03 center pxgrid-agent[5404]: pxgrid-agent Request path=/pxgrid/control/AccountActivate bo
Jul 11 13:05:03 center pxgrid-agent[5404]: pxgrid-agent
```

**Account activated**

[caller=pxgrid.go:58]

```
Jul 11 13:05:03 center pxgrid-agent[5404]: pxgrid-agent Request path=/pxgrid/control/ServiceRegister bo
```

"assetTopic": "/topic/com.cisco.endpoint.asset"

, "restBaseUrl": "https://Center:8910/"

```
Jul 11 13:05:04 center pxgrid-agent[5404]: pxgrid-agent
```

**Service registered**

, ID: c514c790-2361-47b5-976d-4a1b5ccfa8b7 [caller=pxgrid.go:76]

```
Jul 11 13:05:04 center pxgrid-agent[5404]: pxgrid-agent Request path=/pxgrid/control/ServiceLookup body=
Jul 11 13:05:05 center pxgrid-agent[5404]: pxgrid-agent Request path=/pxgrid/control/AccessSecret body=
Jul 11 13:05:06 center pxgrid-agent[5404]: pxgrid-agent
```

**Websocket connect url**

=wss://labise.aaalab.com:

8910

/pxgrid/ise/pubsub [caller=endpoint.go:129]

```
Jul 11 13:05:07 center pxgrid-agent[5404]: pxgrid-agent
```

**STOMP CONNECT host**

=10.48.78.177 [caller=endpoint.go:138]

```
Jul 11 13:06:59 center pxgrid-agent[5404]: pxgrid-agent
```

**STOMP SEND destination**

=/topic/com.cisco.endpoint.asset body={

"opType": "UPDATE"

, "asset": {"assetId": "01:80:c2:00:00:00", "assetName": "LLDP/STP bridges Multicast 0:0:0", "assetIpAddress"

```
Jul 11 13:10:04 center pxgrid-agent[5404]: pxgrid-agent Request path=/pxgrid/control/ServiceReregister
```



통합 후 필요한 메시지 형식 및 assetGroup 특성은 다음과 같이 값 없이 게시됩니다.

<#root>

```
Jan 25 11:05:49 center pxgrid-agent[1063977]: pxgrid-agent STOMP SEND destination=/topic/com.cisco.endpoint.asset body={"opType":"UPDATE","assetGroup":{"key":"assetGroup","value":""}, {"key":"assetCustomName","value":"test"}, {"key":"assetGroupPath","value":""}], "assetConnectedLinks": []}
```

메시지 형식이 필요합니다(표시된 대로 값이 있는 assetGroup). 이는 CyberVision Center에서 특성을 전송하는 것을 확인하며, ISE에 더 이상 반영되지 않을 경우 ISE와 추가로 조사해야 합니다.

<#root>

```
Jan 25 11:09:28 center pxgrid-agent[1063977]: pxgrid-agent STOMP SEND destination=/topic/com.cisco.endpoint.asset body={"opType":"UPDATE","assetGroup":{"key":"assetGroup","value":"test group"}, {"key":"assetCustomName","value":"test"}, {"key":"assetGroupPath","value":"test group"}}, "assetConnectedLinks": []}
```

관련 정보

- [CCV 및 ISE 솔루션 개요](#)
- [데모 랩: Cisco Cyber Vision을 사용하여 Cisco ISE를 사용한 동적 마이크로 세그멘테이션 제공](#)
- [데모 ISE 및 CCV](#)
- [ISE 통합 가이드](#)
- [Cisco 기술 지원 및 다운로드](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.