



Before Contacting Technical Support

This chapter describes the steps to take before calling for technical support.



Note

If you purchased Cisco support through a Cisco reseller, contact the reseller directly. If you purchased support directly from Cisco, contact Cisco Technical Support.

Cisco Support Communities

For additional information, visit one of the following support communities:

- [Cisco Support Community for Server Networking](#)
- [Cisco Communities: Nexus 1000V](#)

Gathering Information for Technical Support

At some point, you might need to contact your customer support representative or Cisco TAC for some additional assistance. This section outlines the steps that you should perform before you contact your next level of support.



Note

Do not reload the module or the switch at least until you have completed [Step 1](#). Some logs and counters are kept in volatile storage and will not survive a reload.

Step 1

Collect the switch information and configuration before and after the issue has been resolved.

On the VSM, generate the technical support by entering the **show tech-support detail > tech-support** command. Use SCP/SFTP/FTP to get the file from the VSM.

On the VEM, generate the support directory by entering the following commands in a PowerShell window:

- **set-ExecutionPolicy Unrestricted**
- **cd c:\program files (x86)\Cisco\Nexus1000V\support**
- **vem-support.ps1**

Add the directory to a zip file to send to technical support.

- Step 2** Capture the exact error codes that you see in CLI message logs by entering one of these commands:
- **show logging log** (displays the error messages)
 - **show logging last *number*** (displays the last lines of the log)
- Step 3** Answer the following questions before calling for technical support:
- On which switch or port is the problem occurring?
 - Which Cisco Nexus 1000V software, driver versions, operating systems versions, and storage device firmware are in your fabric?
 - Which Microsoft Hyper-V and Microsoft SCVMM software are you running?
 - What is the network topology?
 - Were any changes being made to the environment (VLANs, adding modules, upgrades) prior to or at the time of this event?
 - Are there other similarly configured devices that could have this problem, but do not?
 - Where was this problematic device connected (which switch and interface)?
 - When did this problem first occur?
 - When did this problem last occur?
 - How often does this problem occur?
 - How many devices have this problem?
 - Were any traces or debug output captured during the problem time? What troubleshooting steps have you attempted? Which, if any, of the following tools were used:
 - Ethalyzer, local or remote SPAN
 - CLI debug commands
 - traceroute, ping
- Step 4** Is your problem related to a software upgrade attempt?
- What was the original Cisco Nexus 1000V version?
 - What is the new Cisco Nexus 1000V version?
-

Obtaining a File of Core Memory Information

Cisco customer support engineers often use files from your system for analysis. One file that contains memory information is referred to as a core dump. The file is sent to a TFTP server or to a Flash card in slot0: of the local switch. You should set up your switch to generate this file under the instruction of your customer support representative and send it to a TFTP server so that it can be e-mailed to them.

This example shows how to generate a file of core memory information, or a core dump.

```
n1000v# system cores tftp://10.91.51.200/jsmith_cores
n1000v# show system cores
Cores are transferred to tftp://10.91.51.200/jsmith_cores
```



Note

The filename (indicated by `jsmith_cores`) must exist in the TFTP server directory.

Copying Files

You might be required to move files to or from the switch. These files might include log, configuration, or firmware files.

The Cisco Nexus 1000V always acts as a client, so that an ftp/scp/tftp session always originates from the switch and either pushes files to an external system or pulls files from an external system.

```
File Server: 172.22.36.10
File to be copied to the switch: /etc/hosts
```

The **copy** CLI command supports four transfer protocols and 12 different sources for files.

```
n1000v# copy ?
 bootflash: Select source filesystem
 core: Select source filesystem
 debug: Select source filesystem
 ftp: Select source filesystem
 licenses Backup license files
 log: Select source filesystem
 modflash: Select source filesystem
 nvram: Select source filesystem
 running-config Copy running configuration to destination
 scp: Select source filesystem
 sftp: Select source filesystem
 slot0: Select source filesystem
 startup-config Copy startup configuration to destination
 system: Select source filesystem
 tftp: Select source filesystem
 volatile: Select source filesystem
```

Use the following syntax to use secure copy (scp) as the transfer mechanism:

```
"scp://[username@]server[/path]"
```

This example shows how to copy `/etc/hosts` from 172.22.36.10 using the user `user1`, where the destination would be `hosts.txt`:

```
n1000v# copy scp://user1@172.22.36.10/etc/hosts bootflash:hosts.txt
user1@172.22.36.10's password:
hosts 100% |*****| 2035 00:00
```

This example shows how to back up the startup configuration to an SFTP server:

```
n1000v# copy startup-config sftp://user1@172.22.36.10/test/startup-configuration.bak1
Connecting to 172.22.36.10...
User1@172.22.36.10's password:
n1000v#
```



Tip

Backing up the startup configuration to a server should be done on a daily basis before you make any changes. A short script could be written to be run on the Cisco Nexus 1000V to perform a save and then a backup of the configuration. The script needs to contain two commands only: **copy running-configuration startup-configuration** and then **copy startup-configuration tftp://server/name**. To execute the script, enter the **run-script filename** command.