

# Configure CSPC to Forward Syslog to Syslog Server

## Contents

---

[Introduction](#)

[Problem](#)

[Solution](#)

[Using rsyslog](#)

---

## Introduction

This document describes how to configure the CSPC to forward syslogs to a syslog server.

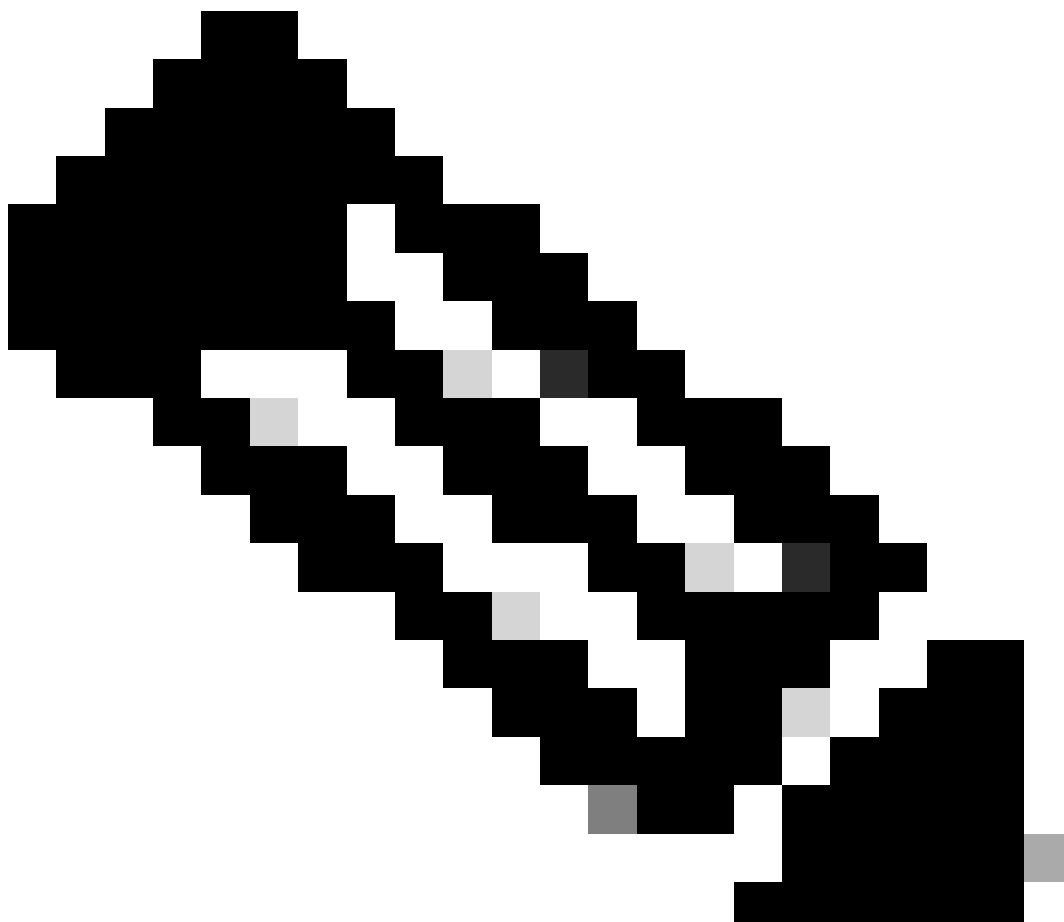
## Problem

Although the BCS and NP support syslog analysis, some people already have another solution and like to use a syslog server like Splunk. But in this case, you require the CSPC to forward the syslogs from CSPC to the syslog server.

## Solution

Determine which protocol (TCP/UDP) and which IP/port you need to use. The default port is 514.

---



**Note:** Syslog server must be reachable from the CSPC.

---

## Using rsyslog

1. Back up `/etc/rsyslog.conf`.

```
cp /etc/rsyslog.conf /etc/rsyslog.confbkup<date>
```

2. Add a forwarding rule.

```
# ### begin forwarding rule ###  
# The statement between the begin ... end define a SINGLE forwarding  
# rule. They belong together, do NOT split them. If you create multiple  
# forwarding rules, duplicate the whole block!  
# Remote Logging (we use TCP for reliable delivery)  
#
```

```
# An on-disk queue is created for this action. If the remote host is
# down, messages are spooled to disk and sent when it is up again.
#$WorkDirectory /var/lib/rsyslog # where to place spool files
#$ActionQueueFileName fwdRule1 # unique name prefix for spool files
#$ActionQueueMaxDiskSpace 1g # 1gb space limit (use as much as possible)
#$ActionQueueSaveOnShutdown on # save messages to disk on shutdown
#$ActionQueueType LinkedList # run asynchronously
#$ActionResumeRetryCount -1 # infinite retries if host is down
# remote host is: name/ip:port, e.g. 192.168.0.1:514, port optional
#*. * @@remote-host:514
Add here
# ### end of the forwarding rule ###
```

### 2.1. Example for TCP:

```
*. * @@138.25.253.132:514
```

### 2.2. Example for UDP:

```
*. * @138.25.253.132:514
```

### 3. Restart **rsyslog**.

```
service rsyslog restart
```



**Note:** If you configure the wrong protocol, an error message appears **rsyslogd: cannot connect to : Connection refused ...** . If this error occurs, modify (go to steps 2.1 and 2.2).

---

We can generate syslogs for testing purposes with:

```
logger "Your message for testing here"
```

4. Confirm if syslogs are being received.