

Подготовка к промышленной эксплуатации

По окончании тестирования, для подготовки сервера к выводу в эксплуатацию, необходимо проверить и сделать следующее:

1. Если не планируется использование веб-интерфейса, отключить его

```
http_enable_paths=rest,action,shared,embed_player,empty
```

2. Убедиться, что пароли пользователей admin и demo изменены на безопасные

3. Расширить диапазон медиапортов, проверить, что диапазон не пересекается с [другими портами](#), используемыми в работе сервера

```
media_port_from      =20001
media_port_to         =40000
```

4. Проверить [диапазон динамических портов Linux](#) и при необходимости изменить его

5. Настроить firewall, открыв нужные порты:

- iptables

iptables setup script example [Expand source](#)

```
#!/bin/bash
#
export IPT="iptables"

# WAN interface
export WAN=eth0

# Clean iptables chains
$IPT -F
$IPT -F -t nat
$IPT -F -t mangle
$IPT -X
$IPT -t nat -X
$IPT -t mangle -X

# Set default policy
$IPT -P INPUT ACCEPT
$IPT -P OUTPUT ACCEPT
$IPT -P FORWARD ACCEPT

# Allow loopback traffic
$IPT -A INPUT -i lo -s 127.0.0.0/8 -d 127.0.0.0/8 -j ACCEPT
$IPT -A OUTPUT -o lo -s 127.0.0.0/8 -d 127.0.0.0/8 -j ACCEPT
```

```

# Allow outgoing connections
$IPT -A OUTPUT -o $WAN -j ACCEPT

# Set up already initiated connections rules
$IPT -A INPUT -p all -m state --state ESTABLISHED,RELATED -j ACCEPT
$IPT -A OUTPUT -p all -m state --state ESTABLISHED,RELATED -j ACCEPT
$IPT -A FORWARD -p all -m state --state ESTABLISHED,RELATED -j ACCEPT

# Drop all invalid packets
$IPT -A INPUT -m state --state INVALID -j DROP
$IPT -A FORWARD -m state --state INVALID -j DROP

$IPT -A INPUT -p tcp ! --syn -m state --state NEW -j DROP
$IPT -A OUTPUT -p tcp ! --syn -m state --state NEW -j DROP

# Allow pings
$IPT -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT
$IPT -A INPUT -p icmp --icmp-type destination-unreachable -j ACCEPT
$IPT -A INPUT -p icmp --icmp-type time-exceeded -j ACCEPT
$IPT -A INPUT -p icmp --icmp-type echo-request -j ACCEPT

# Open SSH port
$IPT -A INPUT -p tcp --dport 22 -j ACCEPT

# Open WCS ports
$IPT -A INPUT -p tcp --dport 80 -j ACCEPT
$IPT -A INPUT -p tcp --dport 443 -j ACCEPT
$IPT -A INPUT -p tcp --dport 8888 -j ACCEPT
$IPT -A INPUT -p tcp --dport 8443 -j ACCEPT
$IPT -A INPUT -p tcp --dport 1935 -j ACCEPT
$IPT -A INPUT -p udp --dport 1935 -j ACCEPT
$IPT -A INPUT -p tcp --dport 554 -j ACCEPT
$IPT -A INPUT -p tcp --dport 8080 -j ACCEPT
$IPT -A INPUT -p tcp --dport 8081 -j ACCEPT
$IPT -A INPUT -p tcp --dport 8084 -j ACCEPT
$IPT -A INPUT -p tcp --dport 8082 -j ACCEPT
$IPT -A INPUT -p tcp --dport 8445 -j ACCEPT
$IPT -A INPUT -p tcp --dport 8444 -j ACCEPT
$IPT -A INPUT -p tcp --dport 20001:40000 -j ACCEPT
$IPT -A INPUT -p udp --dport 20002:40000 -j ACCEPT

$IPT -A INPUT -j DROP
$IPT -A FORWARD -j DROP

# Store rules to the file
/sbin/iptables-save > /etc/sysconfig/iptables

```

- firewallld

firewalld setup script example [Expand source](#)

```

#!/bin/bash
#
systemctl start firewalld
firewall-cmd --permanent --zone=public --add-port=8888/tcp
firewall-cmd --permanent --zone=public --add-port=8443/tcp

```

```
firewall-cmd --permanent --zone=public --add-port=1935/tcp
firewall-cmd --permanent --zone=public --add-port=1935/udp
firewall-cmd --permanent --zone=public --add-port=554/tcp
firewall-cmd --permanent --zone=public --add-port=8080/tcp
firewall-cmd --permanent --zone=public --add-port=8081/tcp
firewall-cmd --permanent --zone=public --add-port=8084/tcp
firewall-cmd --permanent --zone=public --add-port=8082/tcp
firewall-cmd --permanent --zone=public --add-port=8445/tcp
firewall-cmd --permanent --zone=public --add-port=8444/tcp
firewall-cmd --permanent --zone=public --add-port=34001-35000/tcp
firewall-cmd --permanent --zone=public --add-port=30000-33000/udp
firewall-cmd --permanent --zone=public --add-port=30000-33000/tcp
firewall-cmd --reload
```

6. Увеличить максимальное число [одновременно открытых файлов](#)

7. Проверить [настройки REST клиента](#)

8. Отключить клиентские логи в файле flashphoner.properties

```
enable_extended_logging=false
```

9. Ограничить вывод в серверный лог в файле log4j.properties

```
log4j.rootLogger=error, stdout, fAppender
```

10. Очистить логи сервера

```
sudo rm -rf /usr/local/FlashphonerWebCallServer/logs/*
```

11. Проверить объем памяти, [выделенной под Java heap](#)

12. Обновить JDK до 12 или 14 и настроить [сборщик мусора ZGC](#)

13. Настроить [использование библиотеки jemalloc](#) для распределения нативной памяти (не Java heap)