

# Cómo dirigir la integración S A y ESA debido al intercambio de claves/al error del algoritmo de la cifra.

## Contenido

[Introducción](#)

[Problema](#)

[Solución](#)

[Información Relacionada](#)

## Introducción

Este documento abarca cómo dirigir el dispositivo de la Administración de seguridad (S A) y enviar por correo electrónico los errores de la integración del dispositivo de seguridad (ESA) dando por resultado los errores: "(3, "no podrían encontrar el intercambio de claves que correspondía con algorithm.") o el "EOF inesperado encendido para conectar" y los síntomas adicionales.

### Antecedentes

La conexión S A al ESA mientras que primero integra, S A ofrece las cifras/los algoritmos siguientes del intercambio de claves al ESA:

```
kex_algorithms string: diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521
encryption_algorithms_client_to_server string: aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se
encryption_algorithms_server_to_client string: aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se
```

Después de la conexión S A y ESA se establece, el S A ofrece las cifras/los algoritmos siguientes del intercambio de claves al ESA:

```
kex_algorithms string: curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1
encryption_algorithms_client_to_server string [truncated]: aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-gcm@openssh.com,aes256-gcm@openssh.com,chacha20-poly1305@openssh.com,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,arcfour,rijndael-cbc@lysator.liu.se
encryption_algorithms_server_to_client string [truncated]: aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-gcm@openssh.com,aes256-gcm@openssh.com,chacha20-poly1305@openssh.com,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,arcfour,rijndael-cbc@lysator.liu.se
```

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

# Problema

El problema existe al integrar el S A al ESA del EL GUI > el dispositivo de la Administración > centralizaron los dispositivos del > Security (Seguridad) de los servicios o CLI > applianceconfig. El problema indicará un error en la conexión, esto es debido al ESA que falta algunos de los algoritmos del kex/de los algoritmos de la cifra.

1. (3, 'Could not find matching key exchange algorithm.')
2. Error - Unexpected EOF on connect.

# Solución

Para resolver esto, la configuración de la cifra del ssh ESA necesita ser comprada de nuevo a los valores predeterminados proporcionados:

```
lab.esa.com> sshconfig
```

```
Choose the operation you want to perform:
- SSHD - Edit SSH server settings.
- USERKEY - Edit SSH User Key settings
- ACCESS CONTROL - Edit SSH whitelist/blacklist
[]> sshd
```

**ssh server config settings:**

**Public Key Authentication Algorithms:**

```
rsa1
ssh-dss
ssh-rsa
```

**Cipher Algorithms:**

```
aes128-ctr
aes192-ctr
aes256-ctr
aes128-cbc
3des-cbc
blowfish-cbc
cast128-cbc
aes192-cbc
aes256-cbc
rijndael-cbc@lysator.liu.se
```

**MAC Methods:**

```
hmac-md5
hmac-sha1
umac-64@openssh.com
hmac-ripemd160
hmac-ripemd160@openssh.com
hmac-sha1-96
hmac-md5-96
```

**Minimum Server Key Size:**

```
1024
```

**KEX Algorithms:**

```
diffie-hellman-group-exchange-sha256
diffie-hellman-group-exchange-sha1
diffie-hellman-group14-sha1
diffie-hellman-group1-sha1
ecdh-sha2-nistp256
ecdh-sha2-nistp384
```

ecdh-sha2-nistp521

La salida del CLI > sshconfig > sshd en la configuración gradual:

```
[ ]> setup
```

Enter the Public Key Authentication Algorithms do you want to use

```
[rsal,ssh-dss,ssh-rsa]>
```

Enter the Cipher Algorithms do you want to use

```
[aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se]>
```

Enter the MAC Methods do you want to use

```
[hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96]>
```

Enter the Minimum Server Key Size do you want to use

```
[1024]>
```

Enter the KEX Algorithms do you want to use

```
[diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521]>
```

## Información Relacionada

- [Dispositivo de seguridad del correo electrónico de Cisco - Guías del usuario final](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)
- [El mejor practica para la cuarentena centralizada del virus y del brote de la directiva](#)
- [El Guía exhaustiva para la cuarentena del Spam ESA puso con el S A](#)