

MACSEC

<https://www.cisco.com/c/en/us/td/docs/dcn/nx-os/nexus9000/102x/configuration/Security/cisco-nexus-9000-nx-os-security-configuration-guide-102x/m-configuring-macsec.html>

I MKA policyn kan `should-secure` eller `must-secure` specificeras. Should-secure innebär att länken kan gå upp och trafik skyfflas utan eller innan MACSEC förhandlas. Must-secure innebär att MACSEC måste etableras innan länken går upp och trafik kan skyfflas över den.

Konfigurationsexempel

1 Aktivera feature

```
feature macsec
```

2. Skapa PSK

```
key chain 1 MACSEC_KEY no-show
```

```
key 1000
```

```
key-octet-string 64_TECKEN_HEX cryptographic-algorithm AES_256_CMAC
```

```
send-lifetime 00:00:00 May 13 2024 duration 2147483646
```

3. Konfigurera MACsec policy (MKA)

```
macsec policy MKA_POLICY
```

```
cipher-suite GCM-AES-256
```

```
key-server-priority 0
```

```
security-policy should-secure
```

```
window-size 1000
```

```
sak-expiry-time 300
```

4. Konfigurera på interface

```
interface Ethernet1/12
```

```
macsec keychain MACSEC_KEY policy MKA_POLICY
```

Verifying

- show key chain name
- show macsec mka session [interface type slot/port] [detail]
- show macsec mka session details
- show macsec mka summary
- show macsec policy [policy-name]
- show running-config macsec

Revision #1

Created 26 April 2025 11:50:25 by Jehrlander

Updated 26 April 2025 11:50:33 by Jehrlander