

# AES-codering configureren op IW URWB Mode-radio's

## Inhoud

---

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[CLI-configuratie van vloeibaarheidsparameters](#)

---

## Inleiding

Dit document beschrijft de configuratie van AES-parameters op IW9165- en IW9167-radio's in URWB-modus.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basisinstructies voor CLI-navigatie en -opdrachten
- Inzicht in IW URWB-mode radio's

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- IW9165- en IW9167-radio's

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

## Achtergrondinformatie

AES - Advanced Encryption Standard is een cryptografische encryptiestandaard voor veilige communicatie van gegevens. Het is een symmetrisch sleutelalgoritme, wat betekent dat dezelfde sleutel wordt gebruikt om zowel gegevens te versleutelen als te decoderen.

IW-radio's in de URWB-modus, gebruikt u de wachtwoordgroep parameter die op hen is geconfigureerd om alle gegevens van het besturingsvlak te coderen.

Daarom kunnen twee apparaten alleen met elkaar communiceren of andere apparaten in hetzelfde netwerk ontdekken als ze dezelfde wachtwoordzin delen.

De gegevens die over het gegevensvlak worden verzonden, zijn standaard niet gecodeerd. Dit kan worden gecodeerd door AES op de radio's in te schakelen.

Twee apparaten kunnen alleen met elkaar communiceren als ze allebei AES hebben ingeschakeld.

Sleutelrotatie op IW-radio's:

Er zijn andere extra beveiligingsparameters die op de IW-radio's kunnen worden geconfigureerd om de codering sterker te maken. Om WPA-standaarden te ondersteunen, kan sleutelrotatie worden ingeschakeld op de IW-radio's.

Dit werkt op het Key controller-protocol waarmee twee apparaten die met elkaar communiceren periodieke regeneratie van de nieuwe Pairwise Transient Key en Group Transient Key voor pakketversleuteling kunnen plannen.

De Pairwise Transient Key (PTK) beveiligt één-op-één of unicast verkeer, terwijl de Group Transient Key (GTK) groep- of uitzend-/multicastverkeer beveiligt.

Het inschakelen van deze functie verbetert de beveiliging door de hoeveelheid gegevens te verminderen die kan worden aangetast als er inderdaad een aanval is.

De sleutels die worden gebruikt voor codering zijn tijdelijk en draaien periodiek, daarom worden ze nergens opgeslagen. Alle andere geheimen en certificaten worden opgeslagen in een gecodeerd volume dat is beveiligd via Cisco TAM.

([https://www.cisco.com/c/dam/en\\_us/about/doing\\_business/trust-center/docs/trustworthy-technologies-datasheet.pdf](https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/trustworthy-technologies-datasheet.pdf))

Als u bij het uitvoeren van Fluidity-netwerken de rotatie van sleutels inschakelt, kunt u een verstoring van de communicatie ervaren, vooral als de rotatie tijdens het roamingproces plaatsvindt.

Daarom wordt het niet aanbevolen om naast Fluidity-implementaties te worden gebruikt.

Parameters voor AES-codering kunnen op de IW-apparaten alleen worden geconfigureerd via de CLI-toegang of via IoT OD-configuratie.

## CLI-configuratie van vloeibaarheidsparameters

Deze parameters kunnen worden geconfigureerd vanuit de activeringsmodus op de CLI van de apparaten.

### 1. Wachtwoordgroep configureren op de radio's:

Deze parameter wordt gebruikt voor de radio's om de gegevens van het controlevlak te coderen.

*Radio1#configure wireless passphrase URWB*

```
Cisco#configure wireless passphrase
WORD network passphrase (maximum 64 characters)
Cisco#configure wireless passphrase URWB
```

Draadloze wachtwoordgroep configureren

### 2. AES-codering op de radio's inschakelen:

Met deze parameter kunt u AES-codering per radio-interface inschakelen.

*Radio1#configure dot11Radio*

*crypto aes enable*

```
Cisco#configure dot11Radio 1 crypto aes
disable disable encryption
enable enable encryption
Cisco#configure dot11Radio 1 crypto aes enable
```

dot11Radio 1 configureren

### 3. Sleutelcontroller op de radio's inschakelen:

Deze parameter wordt gebruikt om het algoritme van de sleutelcontroller op de radio's in te schakelen. Dit is ook ingeschakeld per radio-interface en is vereist om AES-sleutelrotatie te gebruiken.

*Radio1#configure dot11Radio*

*crypto key-control enable*

```
Cisco#configure dot11Radio 1 crypto key-control
  disable      disable AES-based encryption key-control
  enable       enable AES-based encryption key-control
  key-rotation  set key rotation
Cisco#configure dot11Radio 1 crypto key-control enable
```

dot11Radio 1 crypto-sleutelbesturing

#### 4. Sleutelrotatie op de radio's inschakelen:

Deze parameter wordt gebruikt om sleutelrotatie op de radio's in te schakelen en is ingeschakeld per interface.

*Radio1#configure dot11Radio*

*crypto key-control key-rotation enable*

```
Cisco#configure dot11Radio 1 crypto key-control key-rotation
<1-65535> Key Rotation timeout (seconds)
  disable      disable key rotation
  enable       enable key rotation
```

dot11Radio crypto key-rotation configureren

#### 5. Configureer de belangrijkste rotatietimer op de radio's:

Deze parameter wordt gebruikt om het tijdsinterval te configureren waarmee nieuwe sleutels worden gegenereerd. De timerwaarde wordt in seconden toegevoegd en de parameter kan variëren van <1-65535>.

De standaardwaarde is ingesteld op 3600 seconden of elk uur.

*Radio1#configure dot11Radio*

*crypto key-control key-rotation <1 - 65535>*

```
Cisco#configure dot11Radio 1 crypto key-control key-rotation
<1-65535> Key Rotation timeout (seconds)
disable    disable key rotation
enable     enable key rotation
```

dot11Radio crypto key-rotation configureren

6. Het valideren van de parameters van het sleutelbesturingsalgoritme op de radio's:

De huidige configuratie op de radio met betrekking tot coderingsparameters kan worden gevalideerd met de onderstaande opdracht.

```
Radio1#show dot11Radio
```

*crypto*

```
Cisco#show dot11Radio 1 crypto

Passphrase:          d0a3c370a6b508acadf7143243890068ab602e7b1a43f1f4b9fca940b4eb6348
AES encryption:      enabled
AES key-control:     enabled
Key rotation:        enabled
Key rotation timeout: 6800(second)
Cisco#
```

Dot11Radio 1 crypto weergeven

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.