# Configurare la crittografia delle chiavi già condivise in un router

## Sommario



## Introduzione

In questo documento viene descritto come configurare la crittografia delle chiavi già condivise, nuove e correnti, in un router.

## Prerequisiti

### Requisiti

Nessun requisito specifico previsto per questo documento.

### Componenti usati

Le informazioni di questo documento si basano sulla seguente versione del software:

- Software Cisco IOS XE® versione 16.9

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

### Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

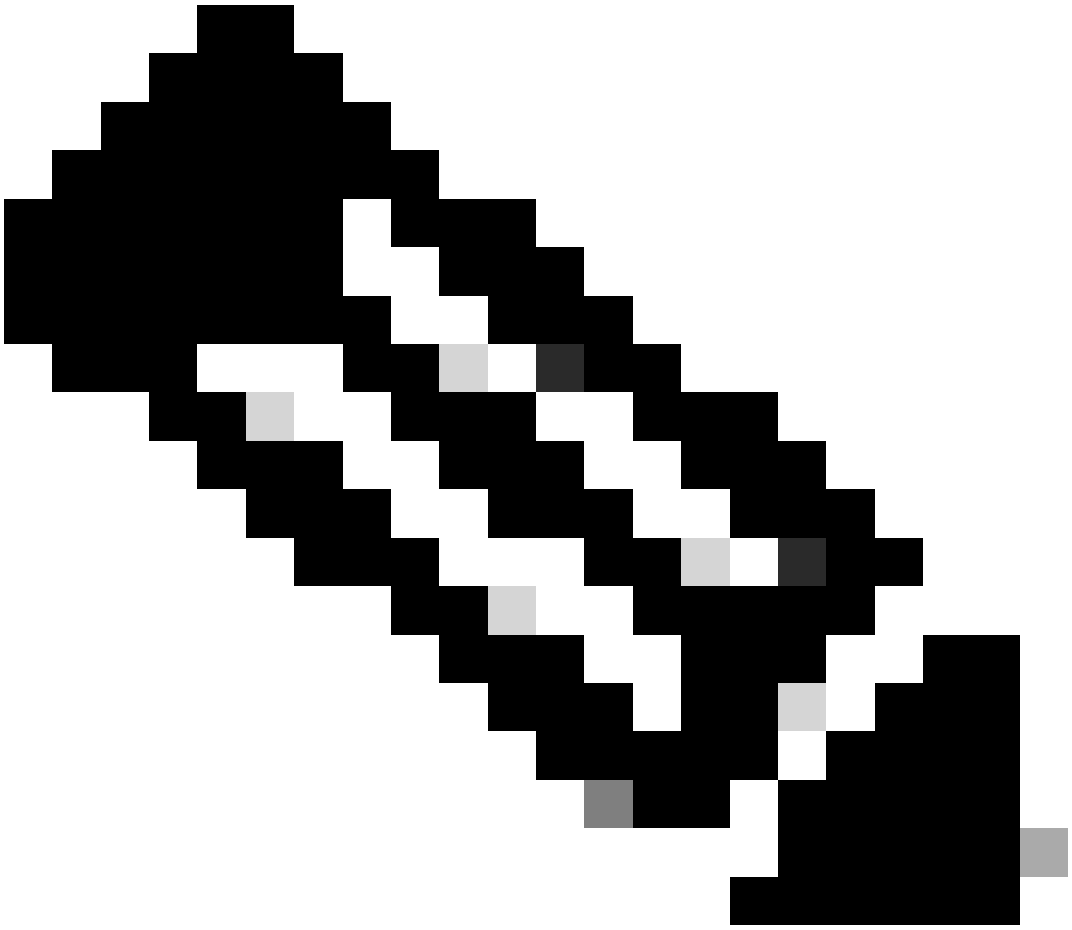
## Premesse

Il codice Cisco IOS versione 12.3(2)T introduce la funzionalità che consente al router di crittografare la chiave precondivisa ISAKMP (Internet Security Association and Key Management Protocol) in formato sicuro di tipo 6 in una memoria RAM non volatile, NVRAM (Non-Volatile RAM). La chiave precondivisa da crittografare può essere configurata come standard, sotto un anello di chiave ISAKMP, in modalità aggressiva, o come password di gruppo in un server Easy VPN (EzVPN) o in una configurazione client.

## Configurazione

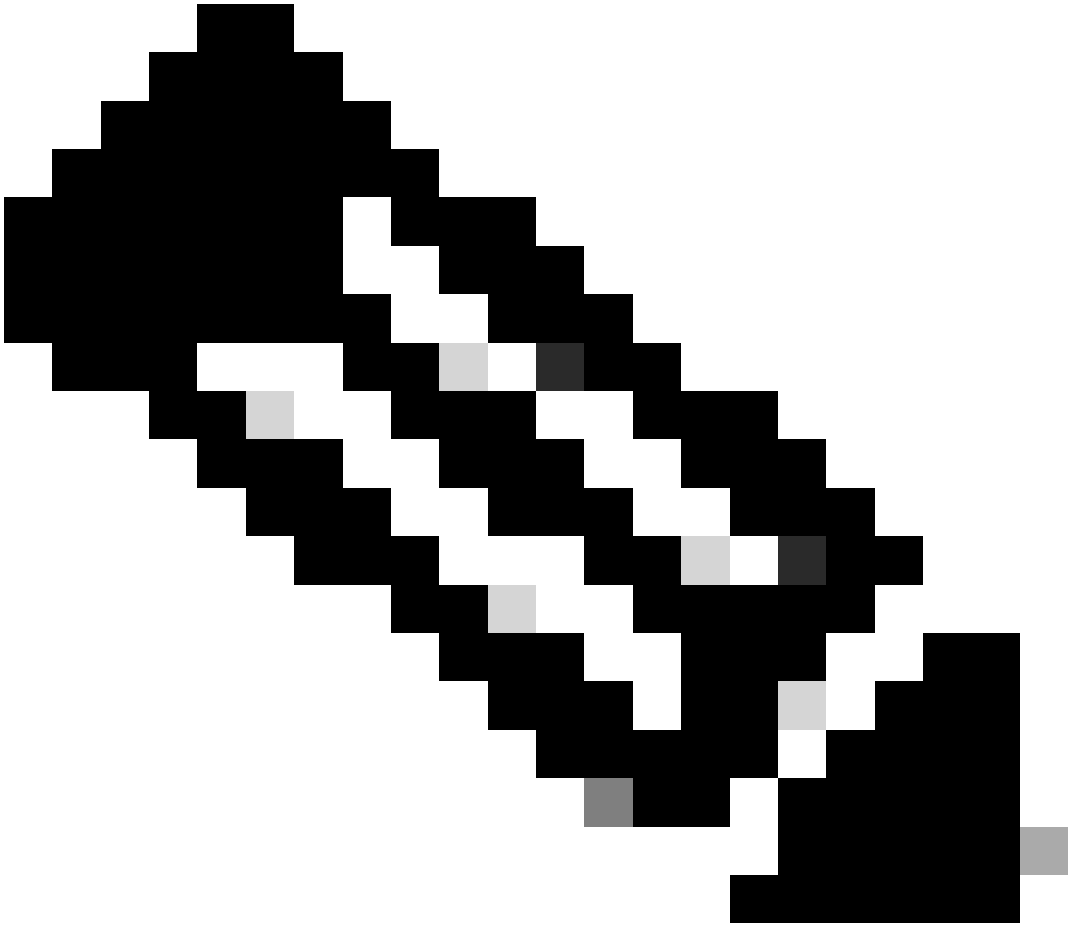
In questa sezione vengono presentate le informazioni che è possibile utilizzare per configurare le funzionalità descritte nel documento.

---



Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento Command Lookup Tool.

---



Nota: solo gli utenti Cisco registrati possono accedere alle informazioni e agli strumenti Cisco interni.

Questi due comandi sono stati introdotti per abilitare la crittografia a chiave già condivisa:

- key config-key password-encryption [primary key]
- crittografia password

La [chiave primaria] è la password/chiave utilizzata per crittografare tutte le altre chiavi nella configurazione del router con l'utilizzo della cifratura simmetrica AES (Advanced Encryption Standard). La chiave primaria non viene archiviata nella configurazione del router e non può essere visualizzata o ottenuta in alcun modo durante la connessione al router.

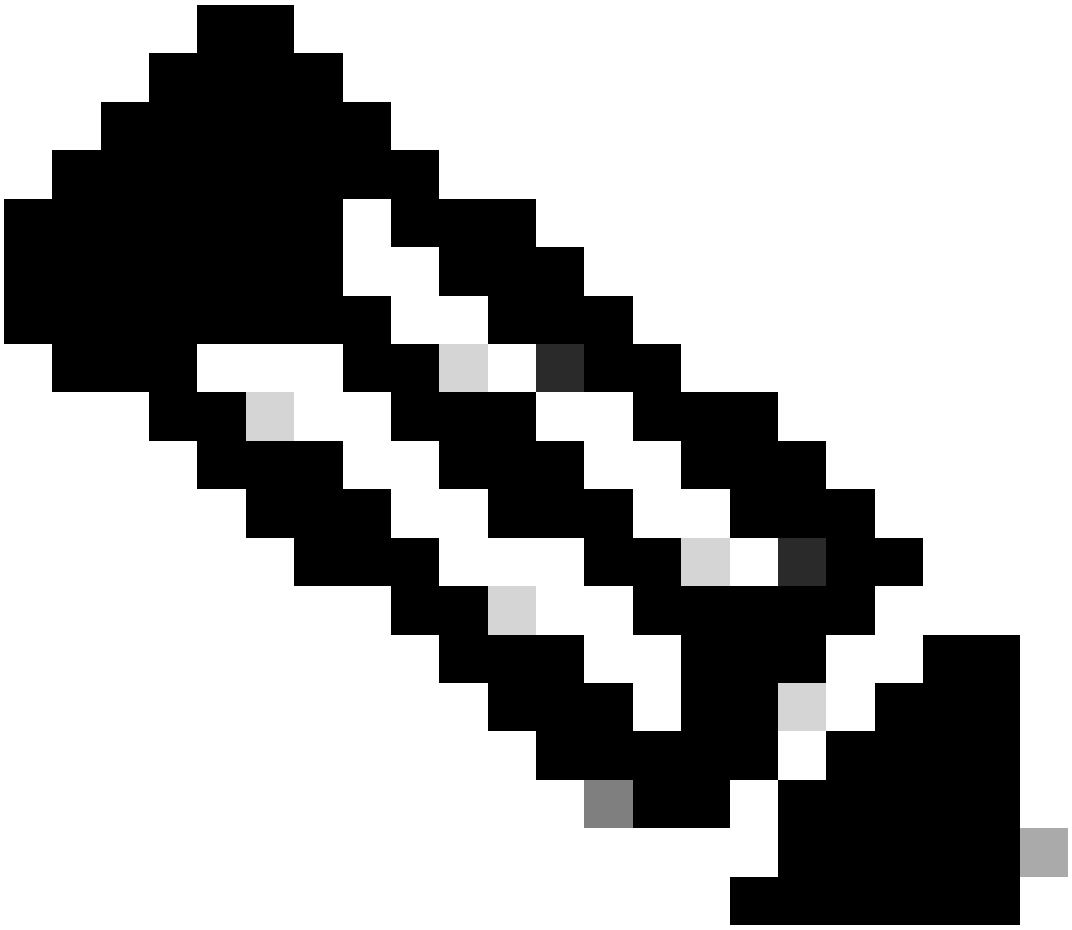
Dopo la configurazione, la chiave primaria viene utilizzata per crittografare le chiavi nuove o correnti nella configurazione del router. Se la [chiave primaria] non è specificata nella riga di comando, il router chiederà all'utente di immettere la chiave e di immetterla nuovamente per la verifica. Se esiste già una chiave, all'utente viene richiesto di immettere prima la vecchia chiave.

Le chiavi non vengono crittografate fino a quando non si esegue il comando password encryption.

La chiave primaria può essere modificata (sebbene ciò non sia necessario a meno che la chiave non sia stata in qualche modo compromessa) con il comando key config-key... di nuovo con il nuovo comando [primary-key].  Tutte le chiavi crittografate correnti nella configurazione del router vengono crittografate nuovamente con la nuova chiave.

È possibile eliminare la chiave primaria quando si esegue il comando no key config-key....  In questo modo, tuttavia, tutte le chiavi attualmente configurate nella configurazione del router verranno rese inutili. Verrà visualizzato un messaggio di avviso in cui viene descritto in dettaglio il problema e viene confermata l'eliminazione della chiave primaria. Poiché la chiave primaria non esiste più, le password di tipo 6 non possono essere decrittografate e utilizzate dal router.

---



Nota: per motivi di sicurezza, le password nella configurazione del router non vengono decrittografate né dalla rimozione della chiave primaria né dal aes comando di crittografia delle password. Una volta crittografate, le password non vengono decrittografate. È comunque possibile decrittografare le chiavi crittografate correnti della configurazione, a condizione che la chiave primaria non venga rimossa.

---

Inoltre, per visualizzare messaggi di tipo debug relativi a funzioni di crittografia della password, usare il comando **password logging** in modalità di configurazione.

## Configurazioni

Questo documento utilizza queste configurazioni sul router:

- Crittografa la chiave già condivisa corrente
- Aggiungi nuova chiave primaria in modo interattivo
- Modifica interattiva della chiave primaria corrente
- Elimina chiave primaria

**Crittografa la chiave già condivisa corrente**

```
    <#root>

Router#



show running-config



Building configuration...
.
.crypto isakmp policy 10
 authentication pre-share
crypto isakmp key cisco123 address 10.1.1.1
.
.
endRouter#



configure terminal



Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#



key config-key password-encrypt testkey123



Router(config)#



password encryption aes



Router(config)#



^Z
```

```
Router#
Router#



show running-config




Building configuration...
.
.
password encryption aes
.
.
crypto isakmp policy 10
 authentication pre-share
crypto isakmp key



6 FLgBaJHXdYY_AcHZZMgQ_RhTDJXHUBAAB



 address 10.1.1.1
.
.
end
```

**Aggiungi nuova chiave primaria in modo interattivo**

```
    <#root>


Router(config)#
```

```
key config-key password-encrypt



New key:



<enter key>



Confirm key:



<confirm key>



Router(config)#
```

**Modifica interattiva della chiave primaria corrente**

```
    <#root>

Router(config)#

key config-key password-encrypt

 Old key:
```

```
<enter current key>


New key:


<enter new key>


Confirm key:


<confirm new key>


Router(config)#
*Jan  7 01:42:12.299: TYPE6_PASS: Master key change heralded,
re-encrypting the keys with the new primary key
```

**Elimina chiave primaria**

```
    <#root>

Router(config)#


no key config-key password-encrypt


WARNING: All type 6 encrypted keys will become unusable
```

```
Continue with primary key deletion ? [yes/no]:

yes

Router(config)#
```

## Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

## Risoluzione dei problemi

Non sono attualmente disponibili informazioni specifiche per la risoluzione dei problemi per questa configurazione.

## Informazioni correlate

- **Pagina di supporto per IPsec**
- **Supporto tecnico Cisco e download**

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).