

# 在ISE中配置NTP身份驗證

## 目錄

---

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[網路圖表](#)

[組態](#)

[開始之前](#)

[路由器上的配置](#)

[驗證](#)

[疑難排解](#)

[參考缺陷](#)

[相關資訊](#)

---

## 簡介

本文檔介紹如何在思科身份服務引擎(ISE)上配置NTP身份驗證並排除NTP身份驗證問題。

作者：Ankush Kaidalwar，思科TAC工程師。

## 必要條件

### 需求

建議您瞭解以下主題：

- Cisco ISE CLI配置
- 網路時間協定(NTP)基礎知識

### 採用元件

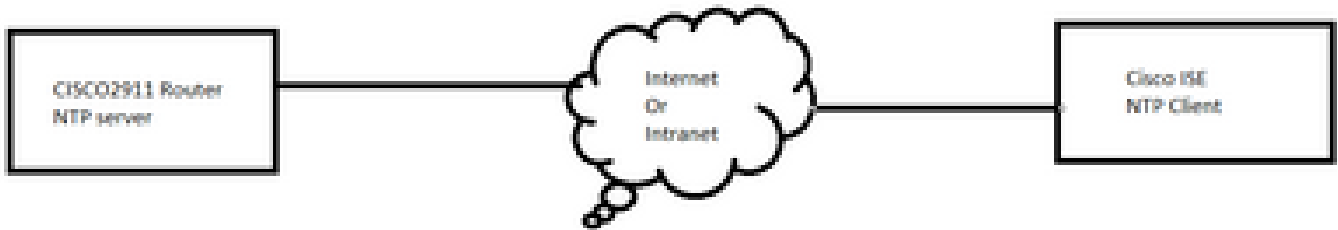
本文中的資訊係根據以下軟體和硬體版本：

- ISE 2.7獨立節點
- CISCO2911/K9版本15.2(1)T2

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

# 設定

## 網路圖表




## 組態


### 開始之前

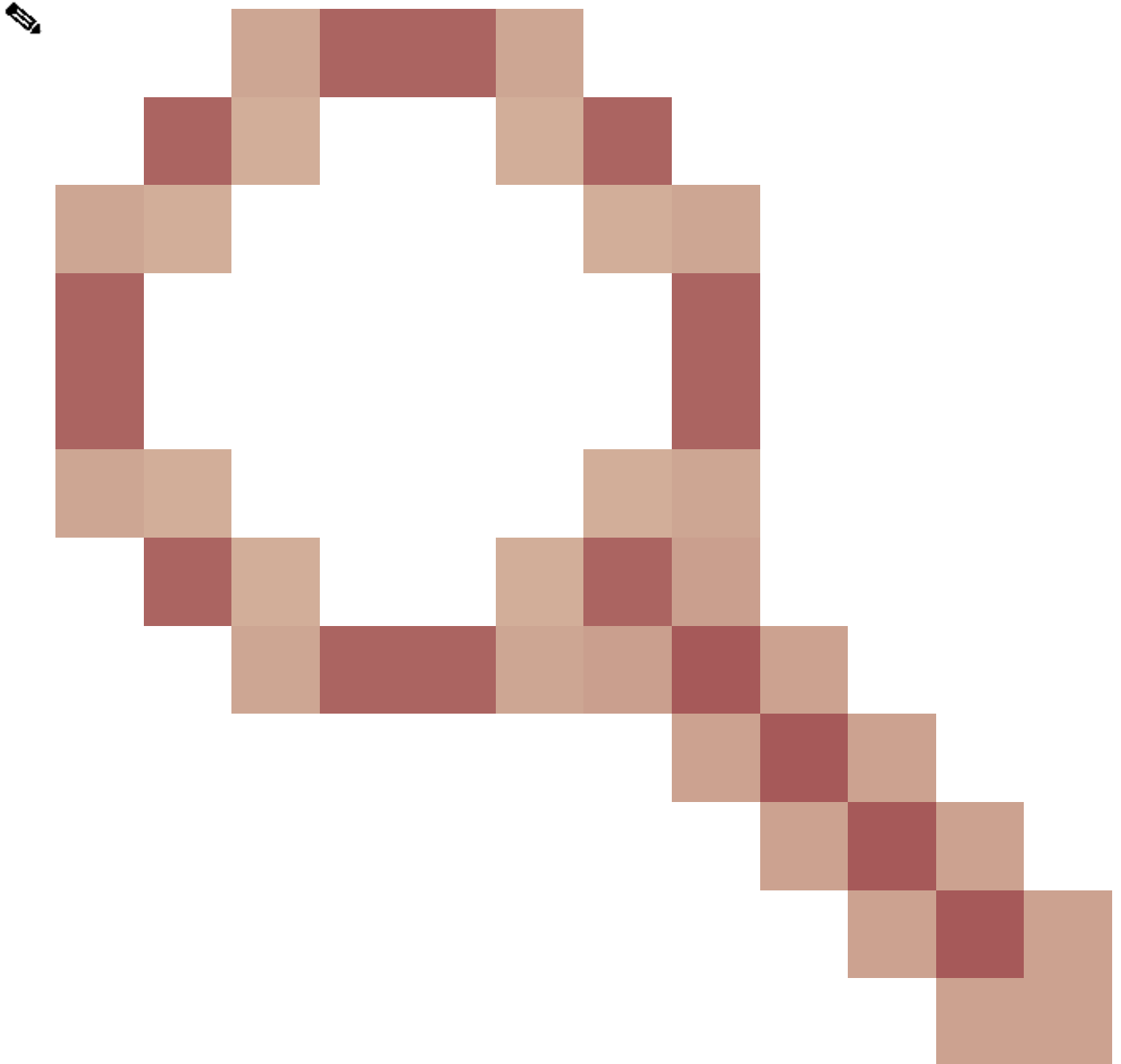
您必須分配超級管理員或系統管理員角色才能訪問ISE。

確保NTP埠在ISE和NTP伺服器之間的傳輸路徑中未被阻止。

假設您在ISE上配置了NTP伺服器。如果要更改NTP伺服器，請導航到管理>系統>設定>系統時間。有關短片，請參閱<https://www.youtube.com/watch?v=BI7loWfb6TE>

 注意：如果是分散式部署，請為所有節點選擇相同的網路時間協定(NTP)伺服器。為了避免節點之間的時區問題，必須在安裝每個節點時提供相同的NTP伺服器名稱。這可確保來自部署中各個節點的報告和日誌始終與時間戳同步。

 註：不能從GUI更改時區。您可以通過CLI執行此操作，CLI需要為該特定節點重新啟動ISE服務。當初始設定嚮導提示您輸入時區時，建議您在安裝時使用首選時區（預設UTC）。請參閱思科錯誤ID [CSCvo49755](https://www.cisco.com/cisco/webbugtool/bugdetails.do?bugid=CSCvo49755)



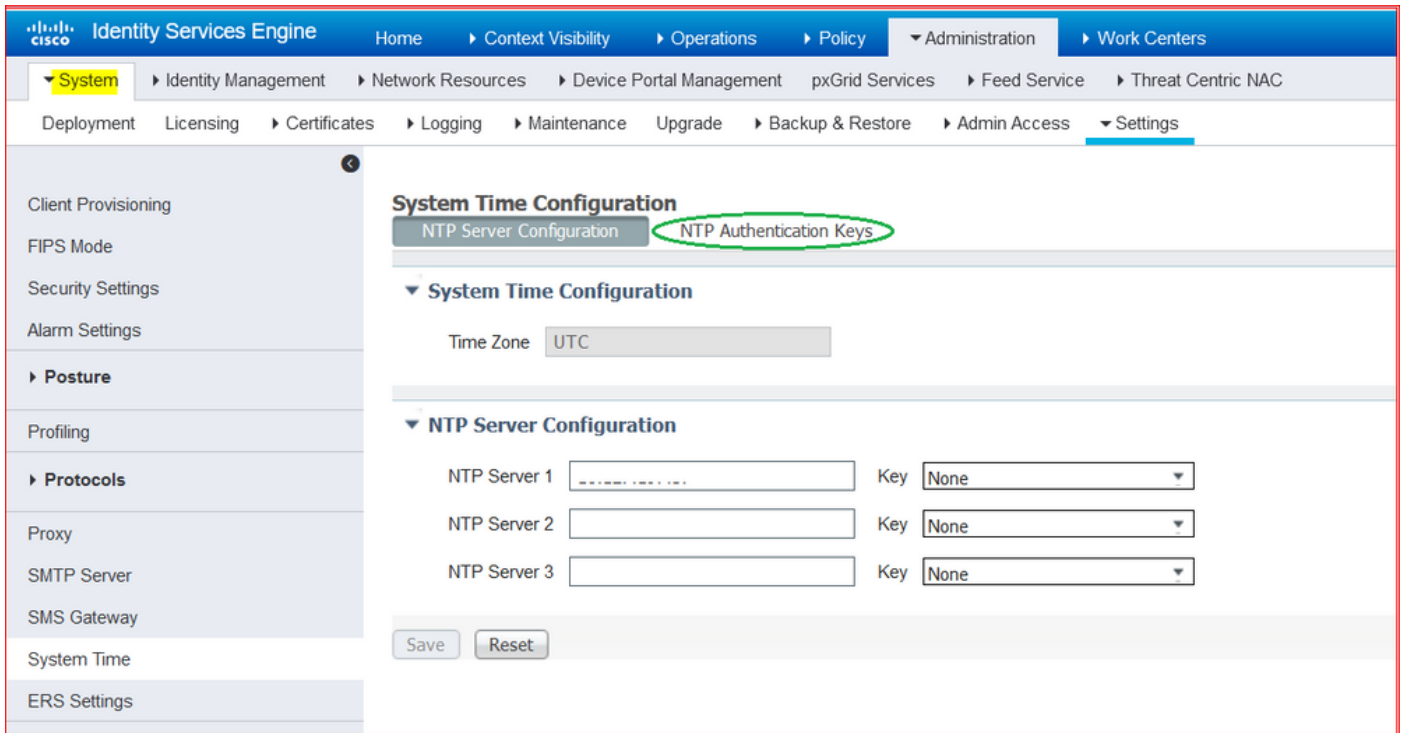
與啟用CLI `clock timezone`命令相關。

如果您在部署中同時擁有主要和輔助思科ISE節點，您必須登入到每個節點的使用者介面並配置系統時間和網路時間協定(NTP)伺服器設定。

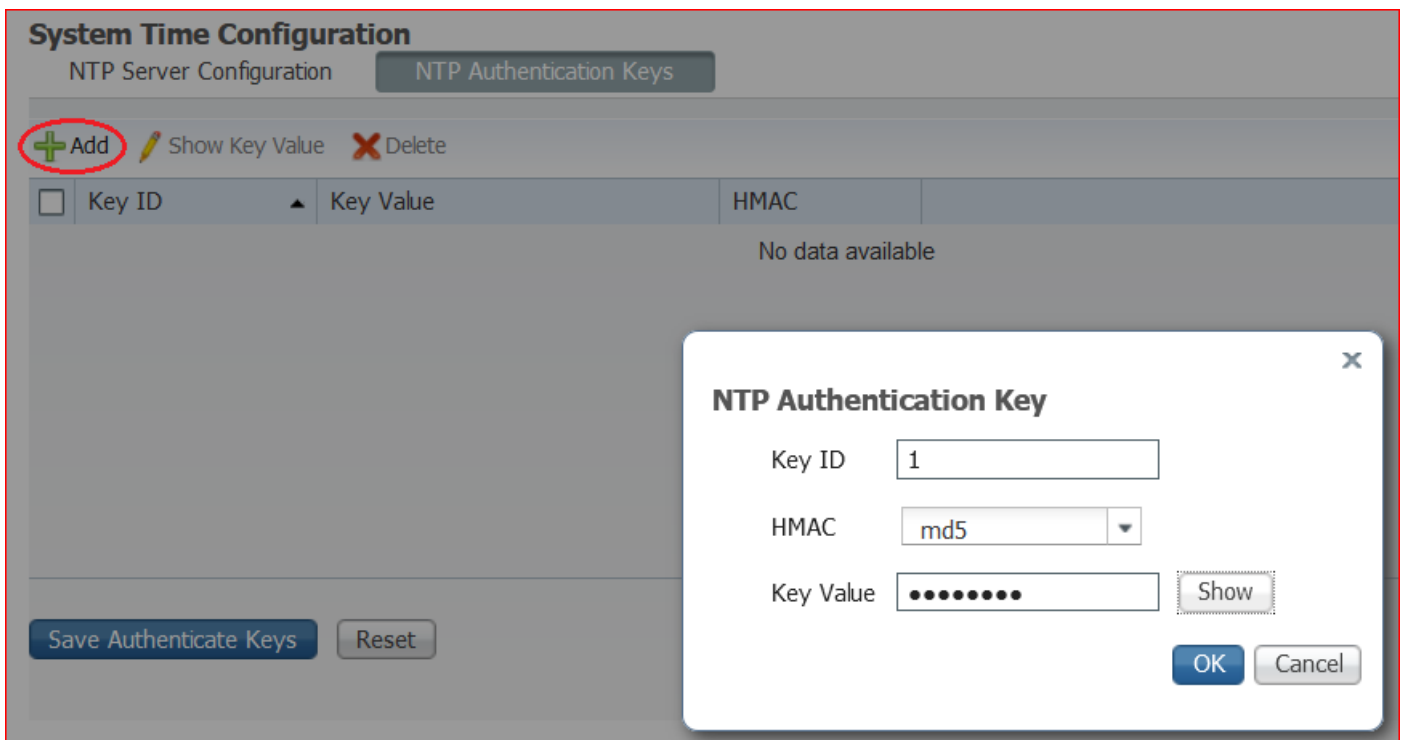
您可以在ISE中通過GUI或CLI配置NTP身份驗證。

#### GUI步驟

步驟 1. 導覽至Administration > System > Settings > System Time，然後按一下NTP Authentication Keys。 ，如下圖所示。



步驟 2. 您可以在此處新增一個或多個身份驗證金鑰。按一下「Add」，系統會顯示一個快顯視窗。此處，Key ID欄位支援1到65535之間的數值，Key Value欄位支援最多15個字母數字字元。Key Value是用於將ISE作為NTP伺服器的客戶端進行身份驗證的實際NTP金鑰。此外，金鑰ID必須與NTP伺服器上配置的金鑰ID匹配。從HMAC下拉選單中選擇所需的雜湊消息身份驗證代碼(HMAC)值。



步驟 3. 按一下OK ( 確定 ) ，然後按一下Save Authentication Keys。您將返回NTP Server Configuration選項卡。

步驟 4. 現在，在金鑰下拉選單中，可以看到您在步驟3中配置的金鑰ID。如果配置了多個金鑰

ID，請按一下相應的金鑰ID。然後按一下「Save」。

**System Time Configuration**

NTP Server Configuration    NTP Authentication Keys

▼ **System Time Configuration**

Time Zone

▼ **NTP Server Configuration**

NTP Server 1	<input type="text" value="10.10.10.10"/>	Key	<input type="text" value="None"/>
NTP Server 2	<input type="text"/>	Key	<input type="text" value="1"/>
NTP Server 3	<input type="text"/>	Key	<input type="text" value="None"/>

## CLI步驟

### 步驟 1. 配置NTP身份驗證金鑰。

```
admin(config)# ntp authentication-key ?
<1-65535> Key number >>> This is the Key ID
admin(config)# ntp authentication-key 1 ? >>> Here you can choose the HMAC value
md5 MD5 authentication
sha1 SHA1 authentication
sha256 SHA256 authentication
sha512 SHA512 authentication
admin(config)# ntp authentication-key 1 md5 ? >>> You can choose either to paste the hash of the actual
hash Specifies an ENCRYPTED (hashed) key follows
plain Specifies an UNENCRYPTED plain text key follows

admin(config)# ntp authentication-key 1 md5 plain Ntp123 >>> Ensure there are no spaces given at the end
```

### 步驟 2. 定義NTP伺服器並關聯步驟1中配置的金鑰ID。

```
admin(config)# ntp server IP/HOSTNAME ?
key Peer key number
<cr> Carriage return.

admin(config)# ntp serve IP/HOSTNAME key ?
```

<1-65535>

```
admin(config)# ntp serve IP/HOSTNAME key 1 ?  
<cr> Carriage return.
```

```
admin(config)# ntp serve IP/HOSTNAME key 1
```

## 路由器上的配置

路由器充當NTP伺服器。配置這些命令，使路由器成為具有NTP身份驗證的NTP伺服器。

```
ntp authentication-key 1 md5 Ntp123 >>> The same key that you configured on ISE  
ntp authenticate  
ntp master STRATUM
```

## 驗證

在ISE上：

使用show ntp命令。如果NTP身份驗證成功，您必須看到要與NTP伺服器同步的ISE。

```
admin# sh ntp  
Configured NTP Servers:  
NTP_SERVER_IP  
  
Reference ID : 0A6A23B1 (NTP_SERVER_IP)  
Stratum : 3  
Ref time (UTC) : Fri Mar 26 09:14:31 2021  
System time : 0.000008235 seconds fast of NTP time  
Last offset : +0.000003193 seconds  
RMS offset : 0.000020295 seconds  
Frequency : 10.472 ppm slow  
Residual freq : +0.000 ppm  
Skew : 0.018 ppm  
Root delay : 0.000571255 seconds  
Root dispersion : 0.000375993 seconds  
Update interval : 519.3 seconds  
Leap status : Normal >>> If there is any issue in NTP synchronization, it shows "Not synchronised".  
  
210 Number of sources = 1  
MS Name/IP address Stratum Poll Reach LastRx Last sample  
=====
```

MS	Name/IP address	Stratum	Poll	Reach	LastRx	Last sample
^*	NTP_SERVER_IP	2	9	377	100	+3853ns[+7046ns] +/- 684us

```
-----  
M indicates the mode of the source.  
^ server, = peer, # local reference clock.  
  
S indicates the state of the sources.  
* Current time source, + Candidate, x False ticker, ? Connectivity lost, ~ Too much variability
```

Warning: Output results can conflict at the time of changing synchronization.

admin#

## 疑難排解

本節提供的資訊可用於對組態進行疑難排解。

1. 如果NTP身份驗證不起作用，首先要確保ISE和NTP伺服器之間的可達性。
2. 確保ISE和NTP伺服器上的金鑰ID配置匹配。
3. 確保在NTP伺服器上將金鑰ID配置為trusted-key。
4. 舊版ISE（如2.4和2.6）支援ntp trusted-key命令。因此，請確保已在這些ISE版本上將NTP金鑰配置為trusted-key。
5. ISE 2.7引入了NTP同步行為的更改。雖然以前的版本使用ntpd，但2.7及更高版本使用的是編年史。Chrony的要求與ntpd不同。其中最明顯的一個問題是，當ntpd與根色散高達10秒的伺服器同步時，僅在根色散低於3秒時進行同步。這會導致能夠同步升級前的NTP伺服器在2.7上不同步，而沒有任何明顯原因。

由於此更改，如果您使用Windows NTP伺服器報告非常大的根色散（3秒或更多），NTP同步問題將頻繁出現，這會導致計時器忽略NTP伺服器時太不準確。

## 參考缺陷

思科錯誤 ID [CSCvw78019](#)

思科錯誤 ID [CSCvw03693](#)

## 相關資訊

- [網路時間通訊協定 \(NTP\) 問題疑難排解和偵錯指南](#)

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。