

# ISEでのNTP認証の設定

## 内容

---

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[コンフィギュレーション](#)

[はじめる前に](#)

[GUIの手順](#)

[CLIの手順](#)

[ルータの設定](#)

[確認](#)

[トラブルシューティング](#)

[参照不具合](#)

[関連情報](#)

---

## はじめに

このドキュメントでは、Cisco Identity Services Engine(ISE)でNTP認証を設定し、NTP認証の問題をトラブルシューティングする方法について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- Cisco ISE CLI の設定
- ネットワークタイムプロトコル(NTP)の基礎知識

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

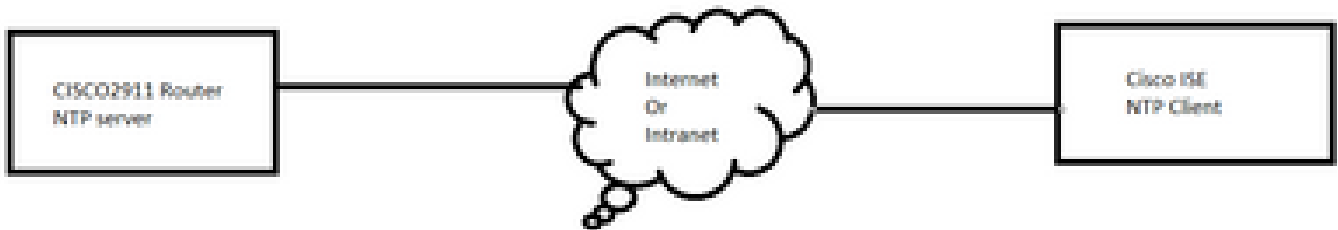
- ISE 2.7スタンドアロンノード
- CISCO2911/K9バージョン15.2(1)T2

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま

す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 設定

### ネットワーク図




## コンフィギュレーション


### はじめる前に

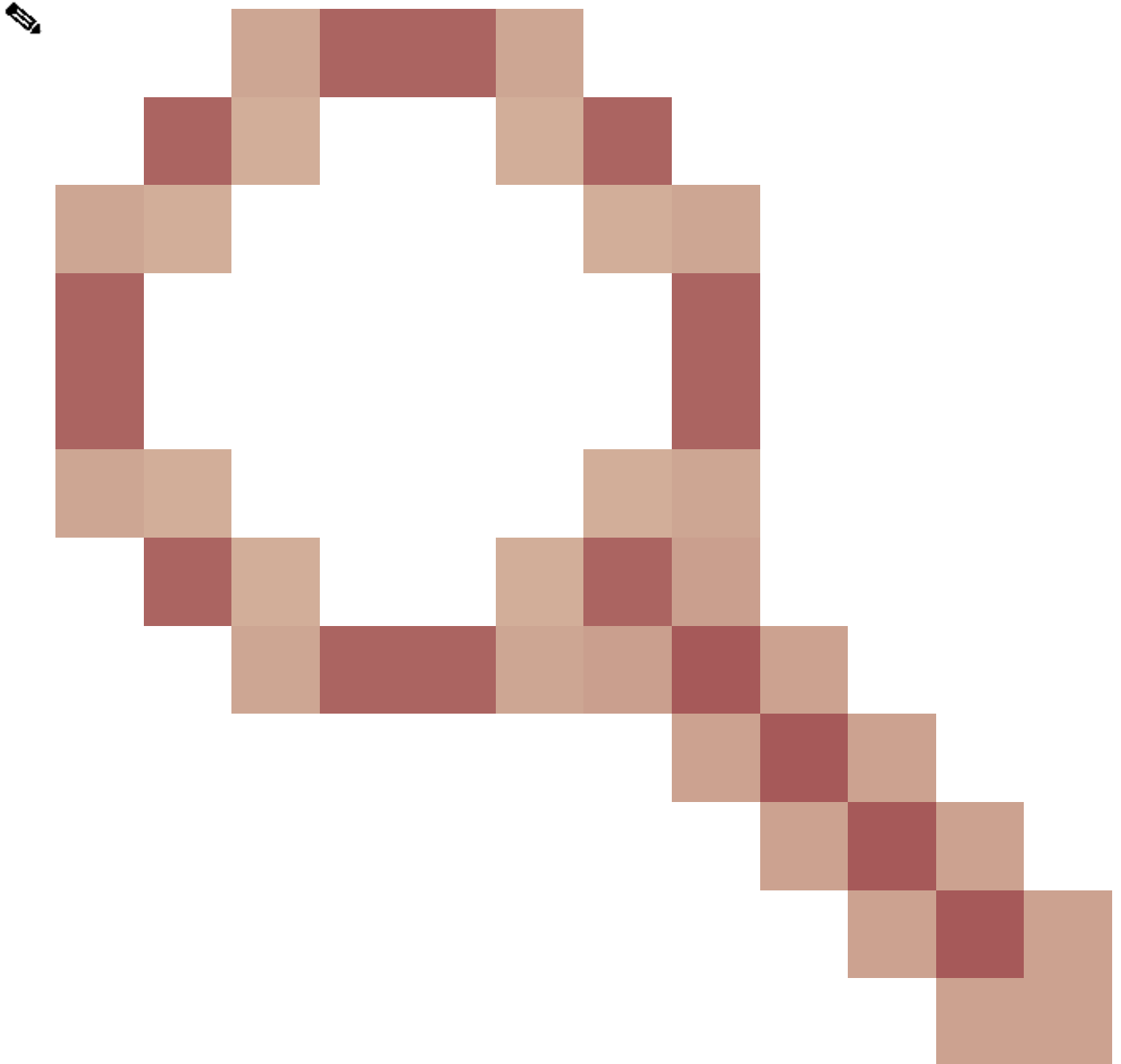
ISEアクセスには、スーパー管理者またはシステム管理者のどちらかの管理者ロールが割り当てられている必要があります。

ISEとNTPサーバ間の中継パスでNTPポートがブロックされていないことを確認します。

NTPサーバがISEで設定されていることを前提としています。NTPサーバを変更する場合は、Administration > System > Settings > System Timeの順に移動します。簡単なビデオとして、[ISE NTP設定](#)を確認できます。

 注：分散導入の場合、すべてのノードに同じネットワークタイムプロトコル(NTP)サーバを選択します。ノード間でのタイムゾーンの問題を回避するには、各ノードのインストール時に同じNTPサーバ名を指定する必要があります。これにより、導入環境のさまざまなノードからのレポートとログが常にタイムスタンプと同期されます。

 注：タイムゾーンをGUIから変更することはできません。これはCLIを使用して実行できます。この場合、特定のノードに対してISEサービスを再起動する必要があります。初期設定ウィザードでタイムゾーンの入力を求められたときに、インストール時に優先タイムゾーン（デフォルトUTC）を使用することをお勧めします。CLIのclock timezoneコマンドを有効にする方法については、Cisco Bug ID [CSCvo49755](#)を参



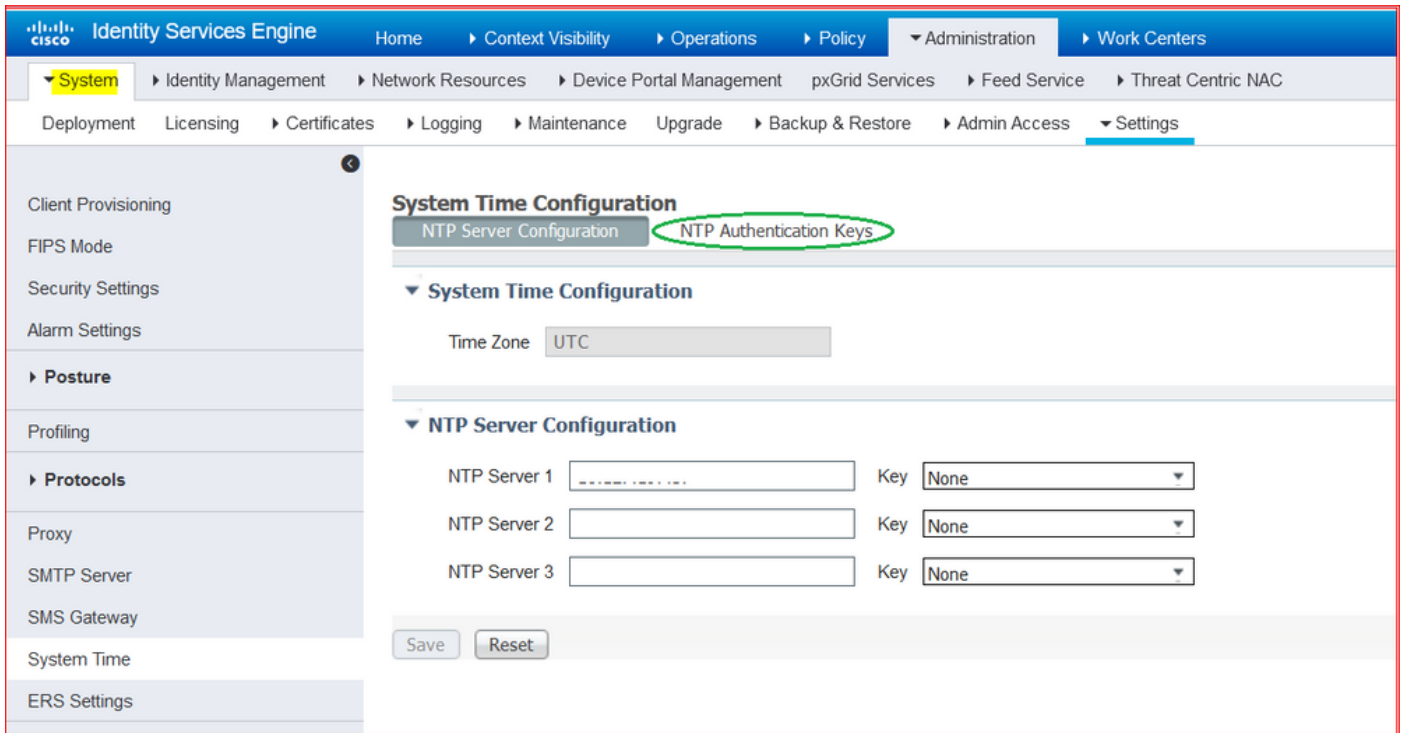
照してください。

導入環境にプライマリとセカンダリの両方のCisco ISEノードがある場合、各ノードのユーザーインターフェイスにログインし、システム時刻とNetwork Time Protocol(NTP)サーバ設定を構成する必要があります。

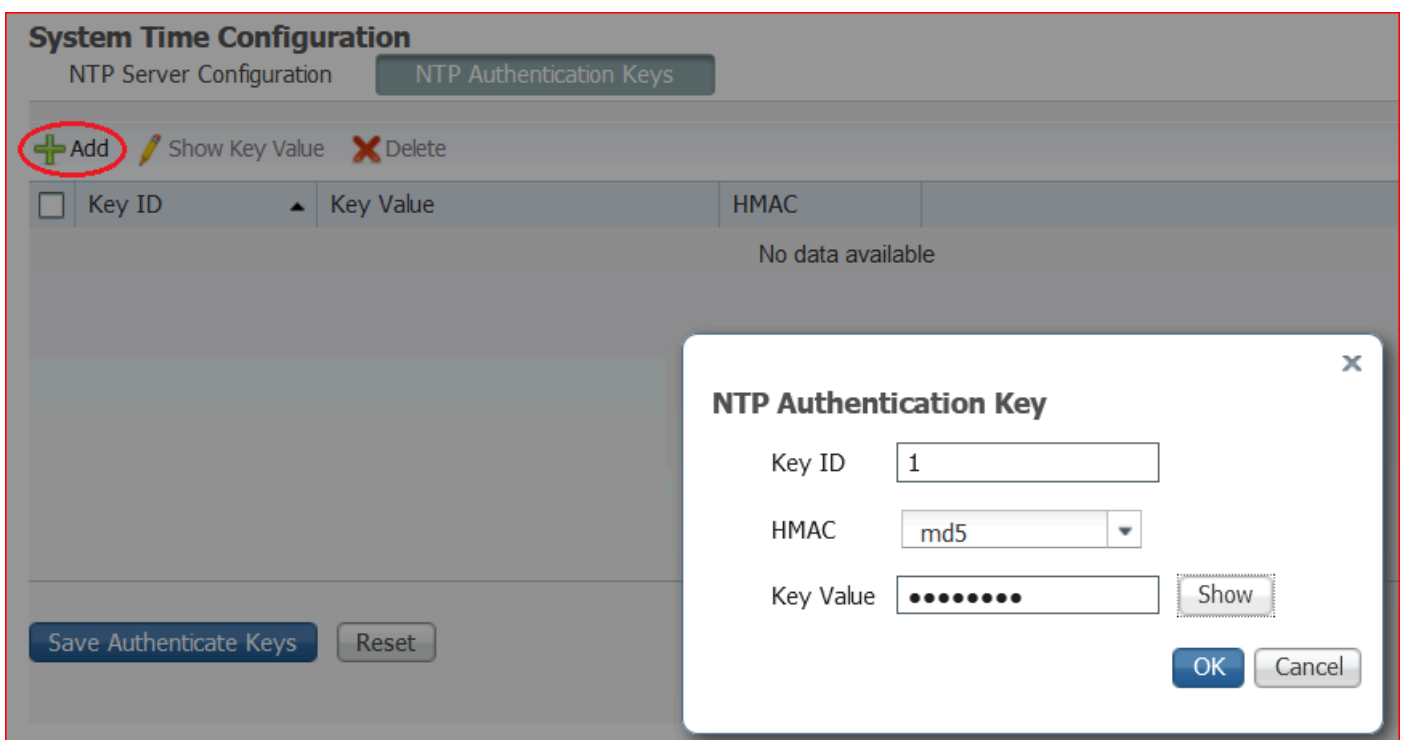
ISEのNTP認証は、GUIまたはCLIから設定できます。

#### GUIの手順

ステップ 1：次の図に示すように、Administration > System > Settings > System Timeの順に移動し、NTP Authentication Keysをクリックします。



ステップ 2 : ここで、1つ以上の認証キーを追加できます。Addをクリックすると、ポップアップが表示されます。ここで、キーIDフィールドは1 ~ 65535の数値をサポートし、キー値フィールドは最大15文字の英数字をサポートします。Key Valueは、ISEをクライアントとしてNTPサーバに認証するために使用される、実際のNTPキーです。また、キーIDはNTPサーバで設定されたものと一致している必要があります。HMACドロップダウンリストから、必要なHashed Message Authentication Code(HMAC)値を選択します。



ステップ 3 : OKをクリックしてから、Save Authentication Keysをクリックします。NTP Server Configurationタブに戻ります。

ステップ 4：キーのドロップダウンに、手順3で設定したキーIDが表示されます。複数のキーIDを設定している場合は、それぞれのキーIDをクリックします。次にSaveをクリックします。

**System Time Configuration**

NTP Server Configuration    NTP Authentication Keys

▼ System Time Configuration

Time Zone

▼ NTP Server Configuration

NTP Server 1	<input type="text" value="10.12.13.14"/>	Key	<input type="text" value="None"/>
NTP Server 2	<input type="text"/>	Key	<input type="text" value="None"/> 1 ←
NTP Server 3	<input type="text"/>	Key	<input type="text" value="None"/>

## CLIの手順

ステップ 1：NTP認証キーを設定します。

```
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
```

ステップ 2：NTPサーバを定義し、手順1で設定したキーIDを関連付けます。

```
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
```

## ルータの設定

ルータはNTPサーバとして動作します。これらのコマンドを設定して、ルータをNTP認証を使用するNTPサーバとして有効にします。

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

## 確認

ISEで次を実行します。

show ntpコマンドを使用します。NTP認証に成功した場合は、NTPサーバと同期するようにISEを確認する必要があります。

```
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
=====
^* 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#

## トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

1. NTP認証が機能しない場合、確認する最初のステップは、ISEとNTPサーバ間の到達可能性です。
2. キーIDの設定がISEとNTPサーバで一致していることを確認します。
3. NTPサーバでキーIDがtrusted-keyに設定されていることを確認します。
4. 2.4や2.6などの古いバージョンのISEでは、ntp trusted-keyコマンドがサポートされています。したがって、これらのISEバージョンでNTPキーをtrusted-keyとして設定してあることを確認します。
5. ISE 2.7では、NTP同期の動作が変更されています。以前のバージョンではntpdを使用していましたが、2.7以降のバージョンではchronyを使用します。Chronyにはntpdとは異なる要件があります。最も顕著なもの1つは、ntpdが最大10秒のルート分散を持つサーバと同期する一方で、ルート分散が3秒未満の場合にのみ同期することです。これにより、アップグレード前に同期できたNTPサーバは、明確な理由がなくても2.7で同期されなくなります。

この変更のため、Windows NTPサーバを使用するとNTP同期の問題が頻繁に発生します。これは、非常に長いルート分散 ( 3秒以上 ) がレポートされ、NTPサーバが不正確すぎるためです。

## 参照不具合

Cisco Bug ID [CSCvw78019](#)

Cisco Bug ID [CSCvw03693](#)

## 関連情報

- [Network Time Protocol \( NTP \) 問題のトラブルシューティングおよびデバッグ ガイド](#)

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。