



コンフィギュレーションモードの Cisco ISE CLI コマンド

この章では、Cisco ISE コマンドラインインターフェイス (CLI) のコンフィギュレーション (config) モードで使用するコマンドについて説明します。この章では、コマンドごとに、その使用方法の簡単な説明、コマンドの構文、使用上のガイドライン、および使用例を示します。

- [EXEC モードでのコンフィギュレーションモードへの切り替え \(3 ページ\)](#)
- [コンフィギュレーションモードでの Cisco ISE の設定 \(4 ページ\)](#)
- [コンフィギュレーションサブモードでの Cisco ISE の設定 \(5 ページ\)](#)
- [CLI コンフィギュレーションコマンドのデフォルト設定 \(6 ページ\)](#)
- [backup interface \(7 ページ\)](#)
- [cdp holdtime \(12 ページ\)](#)
- [cdp run \(13 ページ\)](#)
- [cdp timer \(14 ページ\)](#)
- [clear screen \(15 ページ\)](#)
- [clock timezone \(16 ページ\)](#)
- [cls \(20 ページ\)](#)
- [conn-limit \(21 ページ\)](#)
- [dns cache \(22 ページ\)](#)
- [do \(23 ページ\)](#)
- [end \(27 ページ\)](#)
- [exit \(28 ページ\)](#)
- [hostname \(29 ページ\)](#)
- [icmp echo \(31 ページ\)](#)
- [identity-store \(32 ページ\)](#)
- [interface \(33 ページ\)](#)
- [ip address \(35 ページ\)](#)
- [ip default-gateway \(37 ページ\)](#)
- [ip domain-name \(38 ページ\)](#)

- ip host (40 ページ)
- ip mtu (43 ページ)
- ip name-server (44 ページ)
- ip route (46 ページ)
- ipv6 address (48 ページ)
- ipv6 address autoconfig (50 ページ)
- ipv6 address dhcp (52 ページ)
- ipv6 enable (54 ページ)
- ipv6 route (56 ページ)
- kron occurrence (58 ページ)
- kron policy-list (61 ページ)
- logging (63 ページ)
- max-ssh-sessions (65 ページ)
- ntp (66 ページ)
- ntp authenticate (67 ページ)
- ntp authentication-key (68 ページ)
- ntp server (70 ページ)
- ntp trusted-key (75 ページ)
- rate-limit (76 ページ)
- password-policy (77 ページ)
- repository (80 ページ)
- service (83 ページ)
- shutdown (85 ページ)
- snmp-server enable (86 ページ)
- snmp-server user (87 ページ)
- snmp-server host (90 ページ)
- snmp-server community (93 ページ)
- snmp-server contact (95 ページ)
- snmp-server location (96 ページ)
- snmp-server trap dskThresholdLimit (97 ページ)
- snmp engineid (98 ページ)
- synflood-limit (99 ページ)
- username (100 ページ)
- which (102 ページ)

EXEC モードでのコンフィギュレーションモードへの切り替え

EXEC モードで **configure** または **configure terminal (conf t)** コマンドを実行すると、コンフィギュレーションモードを開始できます。

Cisco ISE CLI から EXEC モードでコンフィギュレーション コマンドを直接入力することはできません。一部のコンフィギュレーション コマンドでは、コマンド コンフィギュレーションを完了するために、コンフィギュレーション サブモードを開始する必要があります。

コンフィギュレーションモードを終了するには、**exit**、**end**、または **Ctrl-z** コマンドを入力します。

コンフィギュレーションコマンドには **interface**、**Policy List**、**repository** が含まれます。

コンフィギュレーションモードで設定作業を実行できます。コンフィギュレーションの変更内容を保存して、システムのリロードや停電時に変更内容が失われないようにする必要があります。

コンフィギュレーションを保存すると、これらのコマンドは、次のいずれかのコマンドを実行した場合に限り、Cisco ISE サーバのリブート後もそのまま有効です。

- **copy running-config startup-config**
- **write memory**

コンフィギュレーションモードでの Cisco ISE の設定

コンフィギュレーション コマンドおよびコンフィギュレーション サブモード コマンドを入力して、Cisco ISE サーバの実際の設定をコンフィギュレーションモードで変更できます。

ステップ 1 `configure terminal` と入力してコンフィギュレーションモードを開始します。

```
ise/admin# configure terminal
Enter configuration commands, one per line. End with CNTL-Z.
ise/admin(config)# (configuration mode)
```

ステップ 2 疑問符 (?) を入力して、コンフィギュレーションモードのコマンドの一覧を表示します。

```
ise/admin(config)# ?
Configure commands:
cdp                CDP Configuration parameters
clock              Configure timezone
conn-limit         Configure a TCP connection limit from source IP
do                EXEC command
end                Exit from configure mode
exit              Exit from configure mode
hostname          Configure hostname
icmp              Configure icmp echo requests
interface         Configure interface
ip                Configure IP features
kron              Configure command scheduler
logging           Configure system logging
max-ssh-sessions  Configure number of concurrent SSH sessions
no                Negate a command or set its defaults
ntp               Specify NTP configuration
password-policy   Password Policy Configuration
rate-limit        Configure a TCP/UDP/ICMP packet rate limit from source IP
repository        Configure Repository
service           Specify service to manage
snmp-server       Configure snmp server
synflood-limit    Configure a TCP SYN packet rate limit
username          User creation
```

ステップ 3 コンフィギュレーションサブモードを開始します。コンフィギュレーションモードには数種類のコンフィギュレーションサブモードがあります。各サブモードに入ると、プロンプト階層のさらに深いレベルで操作できます。このレベルから、Cisco ISE コンフィギュレーションに直接コマンドを入力できます。

```
ise/admin(config)# interface GigabitEthernet 0
ise/admin(config-GigabitEthernet)#
```

ステップ 4 コンフィギュレーションモードと EXEC モードの両方を終了するには、コマンドプロンプトで **exit** を順に入力します。**exit** と入力すると、Cisco ISE はユーザのレベルを 1 段階戻し、前のレベルに戻します。もう一度 **exit** と入力すると、Cisco ISE はユーザを EXEC レベルに戻します。

```
ise/admin(config)# exit
ise/admin# exit
```

コンフィギュレーションサブモードでの Cisco ISE の設定

コンフィギュレーションサブモードで特定の設定のコマンドを入力できます。このプロンプトを終了してコンフィギュレーションプロンプトに戻る場合は **exit** コマンドまたは **end** コマンドを使用できます。

ステップ 1 **configure terminal** と入力してコンフィギュレーションモードを開始します。

```
ise/admin# configure terminal
Enter configuration commands, one per line. End with CNTL-Z.
ise/admin(config)# (configuration mode)
```

ステップ 2 コンフィギュレーションサブモードを開始します。

```
ise/admin# configure terminal
ise/admin(config)# interface GigabitEthernet 0
ise/admin(config-GigabitEthernet)# ?
Configure ethernet interface:
  backup    Configure NIC bonding feature
  do        EXEC command
  end       Exit from configure mode
  exit      Exit from this submode
  ip        Configure IP features
  ipv6     Configure IPv6 features
  no        Negate a command or set its defaults
  shutdown  Shutdown the interface
ise/admin(config-GigabitEthernet)#
```

ステップ 3 コマンドプロンプトで **exit** を入力して、コンフィギュレーションサブモードとコンフィギュレーションモードの両方を終了します。

```
ise/admin(config-GigabitEthernet)# exit
ise/admin(config)# exit
ise/admin#
```

CLI コンフィギュレーションコマンドのデフォルト設定

CLI コンフィギュレーションコマンドには、**default** 形式があることがあります。この形式は、コマンド設定をデフォルト値に戻します。ほとんどのコマンドはデフォルトでディセーブルに設定されているため、この場合はコマンドで **default** 形式を使用しても **no** 形式を使用しても同じ結果になります。

ただし、デフォルトでイネーブルに設定されていて、なおかつ変数が特定のデフォルト値に設定されているコマンドもあります。そのような場合に **default** 形式のコマンドを使用すると、コマンドがイネーブルになり、変数がデフォルト値に設定されます。

backup interface

高可用性のために単一の仮想インターフェイスに2つのイーサネットインターフェイスを設定（NIC ボンディング機能または NIC チーミング機能とも呼ばれる）するには、コンフィギュレーションサブモードで **backup interface** コマンドを使用します。NIC ボンディング設定を削除するには、このコマンドの **no** 形式を使用します。2つのインターフェイスをボンディングすると、2つの NIC は1つの MAC アドレスを持つ単一のデバイスとして認識されます。

Cisco ISE の NIC ボンディング機能は、ロードバランシングまたはリンク アグリゲーション機能をサポートしていません。Cisco ISE は、NIC ボンディングの高可用性機能だけをサポートします。

インターフェイスのボンディングでは、次の状況でも Cisco ISE サービスが影響を受けないことを保証します。

- 物理インターフェイスの障害
- スイッチ ポート接続の喪失（シャットダウンまたは障害）
- スイッチ ラインカードの障害

2つのインターフェイスをボンディングすると、インターフェイスの一方がプライマリ インターフェイスになり、もう一方はバックアップインターフェイスになります。2つのインターフェイスをボンディングすると、すべてのトラフィックは通常、プライマリインターフェイスを通過します。プライマリ インターフェイスが何らかの理由で失敗すると、バックアップインターフェイスがすべてのトラフィックを引き継いで処理します。ボンディングにはプライマリ インターフェイスの IP アドレスと MAC アドレスが必要です。

NIC ボンディング機能を設定する際に、Cisco ISE は固定物理 NIC を組み合わせて NIC のボンディングを形成します。ボンディングインターフェイスを形成するためにボンディングすることができる NIC について、次の表に概要を示します。

Cisco ISE の物理 NIC の名前	Linux 物理 NIC の名前	ボンディングされた NIC のロール	ボンディングされた NIC の名前
ギガビットイーサネット 0	Eth0	プライマリ	ボンド 0
ギガビットイーサネット 1	Eth1	バックアップ	
ギガビットイーサネット 2	Eth2	プライマリ	ボンド 1
ギガビットイーサネット 3	Eth3	バックアップ	

Cisco ISE の物理 NIC の名前	Linux 物理 NIC の名前	ボンディングされた NIC のロール	ボンディングされた NIC の名前
ギガビットイーサネット 4	Eth4	プライマリ	ボンド 2
ギガビットイーサネット 5	Eth5	バックアップ	

NIC ボンディング機能は、サポートされているすべてのプラットフォームとノードペルソナでサポートされています。サポートされるプラットフォームは次のとおりです。

- SNS-3400 シリーズ アプライアンス：ボンド 0 および 1（Cisco ISE 3400 シリーズ アプライアンスは最大 4 個の NIC をサポート）
- SNS-3500 シリーズ アプライアンス：ボンド 0、1、および 2
- VMware 仮想マシン：ボンド 0、1、および 2（6 つの NIC が仮想マシンで使用可能な場合）
- Linux KVM ノード：ボンド 0、1、および 2（6 つの NIC が仮想マシンで使用可能な場合）

構文の説明

backup interface	NIC ボンディング機能を設定します。
GigabitEthernet	バックアップ インターフェイスとして指定されるギガビットイーサネット インターフェイスを設定します。
0 ~ 3	バックアップ インターフェイスとして設定するギガビットイーサネット ポートの数。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

インターフェイス コンフィギュレーション サブモード (config-GigabitEthernet)#

コマンド履歴

リリース	変更内容
2.1.0.474	このコマンドが導入されました。

使用上のガイドライン

- Cisco ISE は最大 6 つのイーサネット インターフェイスをサポートするので、ボンドは 3 つ（ボンド 0、ボンド 1、ボンド 2）のみ設定できます。
- ボンドに含まれるインターフェイスを変更したり、ボンドのインターフェイスのロールを変更したりすることはできません。ボンディングできる NIC とボンドでの役割についての情報については、上記の表を参照してください。
- Eth0 インターフェイスは、管理インターフェイスとランタイム インターフェイスの両方として機能します。その他のインターフェイスは、ランタイムインターフェイスとして機能します。

- ボンドを作成する前に、プライマリ インターフェイス（プライマリ NIC）に IP アドレスを割り当てる必要があります。ボンド 0 を作成する前は、Eth0 インターフェイスに IPv4 アドレスを割り当てる必要があります。同様に、ボンド 1 と 2 を作成する前は、Eth2 と Eth4 インターフェイスに IPv4 または IPv6 アドレスをそれぞれ割り当てる必要があります。
- ボンドを作成する前に、バックアップ インターフェイス（Eth1、Eth3、および Eth5）に IP アドレスが割り当てられている場合は、バックアップ インターフェイスからその IP アドレスを削除します。バックアップ インターフェイスには IP アドレスを割り当てないでください。
- ボンドを 1 つのみ（ボンド 0）作成し、残りのインターフェイスをそのままにすることもできます。この場合、ボンド 0 は管理インターフェイスとランタイムインターフェイスとして機能し、残りのインターフェイスはランタイムインターフェイスとして機能します。
- ボンドでは、プライマリ インターフェイスの IP アドレスを変更できます。プライマリ インターフェイスの IP アドレスと想定されるので、新しい IP アドレスがボンディングされたインターフェイスに割り当てられます。
- 2 つのインターフェイス間のボンドを削除すると、ボンディングされたインターフェイスに割り当てられていた IP アドレスは、プライマリ インターフェイスに再び割り当てられます。
- デプロイメントに含まれる Cisco ISE ノードで NIC ボンディング機能を設定するには、そのノードをデプロイメントから登録解除し、NIC ボンディングを設定して、デプロイメントに再度登録する必要があります。
- ボンド（Eth0、Eth2、または Eth4 インターフェイス）のプライマリ インターフェイスとして機能する物理インターフェイスにスタティックルートが設定されている場合は、物理インターフェイスではなくボンディングされたインターフェイスで動作するようにスタティック ルートが自動的に更新されます。

例 1 : NIC ボンディングの設定

次の手順では、Eth0 と Eth1 インターフェイス間にボンド 0 を設定する方法を説明します。



- (注) バックアップ インターフェイスとして動作する物理インターフェイス（Eth1、Eth3、Eth5 インターフェイスなど）に IP アドレスが設定されている場合は、バックアップ インターフェイスからその IP アドレスを削除する必要があります。バックアップ インターフェイスには IP アドレスを割り当てないでください。

```
ise/admin# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ise/admin(config)# interface gigabitEthernet 0
ise/admin(config-GigabitEthernet)# backup interface gigabitEthernet 1
Changing backup interface configuration may cause ISE services to restart.
Are you sure you want to proceed? Y/N [N]: Y
```

```

Stopping ISE Monitoring & Troubleshooting Log Processor...
ISE PassiveID Service is disabled
ISE pxGrid processes are disabled
Stopping ISE Application Server...
Stopping ISE Certificate Authority Service...
Stopping ISE EST Service...
ISE Sxp Engine Service is disabled
Stopping ISE Profiler Database...
Stopping ISE Indexing Engine...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE AD Connector...
Stopping ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Profiler Database...
Starting ISE Application Server...
Starting ISE Indexing Engine...
Starting ISE Certificate Authority Service...
Starting ISE EST Service...
Starting ISE Monitoring & Troubleshooting Log Processor...
Starting ISE AD Connector...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
ise/admin(config-GigabitEthernet)#
    
```

例 2 : NIC ボンディングの設定の確認

NIC ボンディング機能が設定されているかどうかを確認するには、Cisco ISE CLI から **show running-config** コマンドを実行します。次のような出力が表示されます。

```

!
interface GigabitEthernet 0
  ipv6 address autoconfig
  ipv6 enable
  backup interface GigabitEthernet 1
  ip address 192.168.118.214 255.255.255.0
!
    
```

上記の出力では、「**backup interface GigabitEthernet 1**」は、ギガビットイーサネット 0 に NIC ボンディングが設定されていて、ギガビットイーサネット 0 がプライマリインターフェイス、ギガビットイーサネット 1 がバックアップインターフェイスとされていることを示します。また、ADE-OS 設定では、プライマリおよびバックアップのインターフェイスに効果的に同じ IP アドレスを設定していても、**running config** でバックアップインターフェイスの IP アドレスは表示されません。

また、**show interfaces** コマンドを実行して、ボンディングされたインターフェイスを表示できます。

```

ise/admin# show interface
bond0: flags=5187<UP,BROADCAST,RUNNING,PRIMARY,MULTICAST> mtu 1500
  inet 10.126.107.60 netmask 255.255.255.0 broadcast 10.126.107.255
  inet6 fe80::8a5a:92ff:fe88:4aea prefixlen 64 scopeid 0x20<link>
  ether 88:5a:92:88:4a:ea txqueuelen 0 (Ethernet)
  RX packets 1726027 bytes 307336369 (293.0 MiB)
  RX errors 0 dropped 844 overruns 0 frame 0
  TX packets 1295620 bytes 1073397536 (1023.6 MiB)
  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    
```

```
GigabitEthernet 0
  flags=6211<UP,BROADCAST,RUNNING,SUBORDINATE,MULTICAST> mtu 1500
  ether 88:5a:92:88:4a:ea txqueuelen 1000 (Ethernet)
  RX packets 1726027 bytes 307336369 (293.0 MiB)
  RX errors 0 dropped 844 overruns 0 frame 0
  TX packets 1295620 bytes 1073397536 (1023.6 MiB)
  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
  device memory 0xfab00000-fabfffff

GigabitEthernet 1
  flags=6147<UP,BROADCAST,SUBORDINATE,MULTICAST> mtu 1500
  ether 88:5a:92:88:4a:ea txqueuelen 1000 (Ethernet)
  RX packets 0 bytes 0 (0.0 B)
  RX errors 0 dropped 0 overruns 0 frame 0
  TX packets 0 bytes 0 (0.0 B)
  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
  device memory 0xfaa00000-faafffff
```

cdp holdtime

受信デバイスが Cisco ISE サーバからの Cisco Discovery Protocol パケットを廃棄するまでの保持時間を指定するには、コンフィギュレーション モードで **cdp holdtime** コマンドを使用します。

cdp holdtime *seconds*

デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

no cdp holdtime

構文の説明	holdtime	アドバタイズされた Cisco Discovery Protocol の保持時間を指定します。
	<i>seconds</i>	秒単位のアドバタイズされた保持時間値。値の範囲は、10 ~ 255 秒です。
コマンド デフォルト	CDP 保持時間のデフォルト値は、180 秒です。	
コマンド モード	コンフィギュレーション (config) #	
コマンド履歴	リリース	変更内容
	2.0.0.306	このコマンドが導入されました。

使用上のガイドライン Cisco Discovery Protocol パケットを存続可能時間、つまり保持時間の値とともに送信します。受信デバイスは、保持時間の経過後に、Cisco Discovery Protocol パケットの Cisco Discovery Protocol 情報を廃棄します。

cdp holdtime コマンドに指定できる引数は 1 つだけです。複数指定した場合は、エラーが発生します。

例

```
ise/admin(config)# cdp holdtime 60
ise/admin(config)#
```

cdp run

すべてのインターフェイスで Cisco Discovery Protocol を有効にするには、コンフィギュレーションモードで **cdp run** コマンドを使用します。

cdp run GigabitEthernet

Cisco Discovery Protocol を無効にするには、このコマンドの **no** 形式を使用します。

no cdp run

構文の説明

run	Cisco Discovery Protocol をイネーブルにします。 cdp run コマンドの no 形式を使用した場合は、Cisco Discovery Protocol が無効になります。
<i>GigabitEthernet</i>	(任意)。Cisco Discovery Protocol をイネーブルにする GigabitEthernet インターフェイスを指定します。
0-3	Cisco Discovery Protocol をイネーブルにする GigabitEthernet インターフェイス番号を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

コンフィギュレーション (config) #

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

このコマンドでは、1つのオプションの引数（インターフェイス名）を指定します。オプションのインターフェイス名を指定しない場合、このコマンドは、すべてのインターフェイス上で Cisco Discovery Protocol をイネーブルにします。



(注) このコマンドのデフォルトでは、すでに実行されているインターフェイスで動作します。インターフェイスの起動時に、最初に Cisco Discovery Protocol を停止します。次に、Cisco Discovery Protocol を起動します。

例

```
ise/admin(config)# cdp run GigabitEthernet 0
ise/admin(config)#
```

cdp timer

Cisco ISE サーバが Cisco Discovery Protocol アップデートを送信する頻度を指定するには、コンフィギュレーションモードで **cdp timer** コマンドを使用します。

cdp timer seconds

デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

no cdp timer

構文の説明	timer	指定した間隔で更新されます。
	<i>seconds</i>	Cisco ISE サーバが Cisco Discovery Protocol 更新を送信する頻度を秒単位で指定します。値の範囲は、5 ~ 254 秒です。
コマンド デフォルト	更新間隔値のデフォルトは 60 秒です。	
コマンド モード	コンフィギュレーション (config) #	
コマンド履歴	リリース	変更内容
	2.0.0.306	このコマンドが導入されました。

使用上のガイドライン Cisco Discovery Protocol パケットを存続可能時間、つまり保持時間の値とともに送信します。受信デバイスは、保持時間の経過後に、Cisco Discovery Protocol パケットの Cisco Discovery Protocol 情報を廃棄します。

cdp timer コマンドに指定できる引数は 1 つだけです。複数指定した場合は、エラーが発生します。

例

```
ise/admin(config)# cdp timer 60
ise/admin(config)#
```

clear screen

端末画面の内容をクリアするには、コンフィギュレーションモードで **clear screen** コマンドを使用します。

clear screen

構文の説明

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

コンフィギュレーション (config) #

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

clear screen は隠しコマンドです。 **clear screen** は Cisco ISE で使用できますが、コマンドラインで疑問符を入力して表示しようとした場合、CLI インタラクティブヘルプには表示されません。

例

次の例は、端末の内容をクリアする方法を示しています。

```
ise/admin(config)# clear screen
ise/admin#
```

clock timezone

時間帯を設定するには、コンフィギュレーションモードで **clock timezone** コマンドを実行します。

clock timezone タイムゾーン

時間帯を無効にするには、このコマンドの **no** 形式を使用します。

no clock timezone



(注) インストール後に Cisco ISE アプライアンス上で時間帯を変更すると、そのノード上で Cisco ISE アプリケーションを使用できなくなるため、ISE を再起動する必要があります。初期設定ウィザードで時間帯の設定を求めるプロンプトが表示されたら、優先する時間帯（デフォルト UTC）をインストール中に設定することをお勧めします。

構文の説明

timezone	システムの時間帯を設定します。
タイムゾーン	標準時に表示する時間帯の名前。最大 64 文字の英数字をサポートします。

プライマリ管理ノード（PAN）の自動フェールオーバー設定をイネーブルにしている場合は、時間帯を設定する前にディセーブルにしてください。時間帯を設定した後でイネーブルに戻すことができます。

コマンド デフォルト

協定世界時（UTC）

コマンド モード

コンフィギュレーション（config）#

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

システムの内部的には、UTCでの時刻が保持されます。特定の時間帯がわからない場合は、地域、国、都市を入力できます（システムに入力する共通の時間帯およびオーストラリアとアジアの時間帯については、表 4-1、4-2、4-3 を参照）。



(注) これ以外にも使用可能な時間帯がいくつかあります。**show timezones** を入力すると、使用可能なすべての時間帯のリストが Cisco ISE サーバに表示されます。該当地域の時間帯に最も適した時間帯を選択します。

展開内で PAN の自動フェールオーバー設定がイネーブルになっていると、次のメッセージが表示されます。


```
PAN Auto Failover is enabled, this operation is not
allowed! Please disable PAN Auto-failover first.
```

例

```
ise/admin(config)# clock timezone EST
ise/admin(config)# exit
ise/admin# show timezone
EST
ise/admin#
```

Cisco ISE ノードの時間帯の変更

インストール後に Cisco ISE アプライアンス上で時間帯を変更すると、そのノード上で Cisco ISE アプリケーションを使用できなくなります。ただし、初期設定ウィザードで時間帯の設定を求めるプロンプトが表示されたら、優先する時間帯（デフォルト UTC）をインストール中に設定できます。

時間帯の変更は、導入の異なる Cisco ISE ノードタイプに影響を与えます。

影響から回復するには、次の手順を使用します。

スタンドアロンまたはプライマリ Cisco ISE ノード

インストール後にタイムゾーンを変更するには、ノードのイメージを再作成する必要があります。

最新の設定のバックアップがあることを確認し、必要な証明書とキーをエクスポートします。

タイムゾーンを変更する場合は、次の操作を行います。

- プライマリ Cisco ISE ノードを再イメージ化します。
- インストール中に、適切なタイムゾーンを選択します。
- バックアップと証明書を復元します。
- Active Directory に再参加し、ISE プロファイラプローブ、LDAP などのノードごとの設定を適用します。

セカンダリ ISE ノード

プライマリ ノードの時間帯と同じになるようにセカンダリ ノードの時間帯を変更する場合、次の手順を実行します。

- 必要な証明書をエクスポートします。
- セカンダリ ノードの登録を解除します。
- ノードを再イメージ化します。
- 必要に応じて、必要な証明書をインポートします。
- ノードをプライマリノードにセカンダリノードとして再登録します。

- Active Directory に再参加し、ISE プロファイラプローブ、LDAP などのノードごとの設定を適用します。

共通の時間帯

表 1: 表 4-1 共通の時間帯 (続き)

略語または名前	時間帯名
欧州	
GMT、GMT0、GMT-0、GMT+0、UTC、Greenwich、Universal、Zulu	グリニッジ標準時 (UTC)
GB	英国
GB-Eire、Eire	アイルランド
WET	西ヨーロッパ時間 (UTC)
CET	中央ヨーロッパ標準時 (UTC + 1 時間)
EET	東ヨーロッパ時間 (UTC + 2 時間)
米国とカナダ	
EST、EST5EDT	東部標準時、UTC - 5 時間
CST、CST6CDT	中央標準時、UTC - 6 時間
MST、MST7MDT	山岳部標準時、UTC - 7 時間
PST、PST8PDT	太平洋標準時、UTC - 8 時間
HST	ハワイ標準時、UTC - 10 時間

オーストラリアのタイムゾーン



(注) オーストラリアの時間帯では、国と都市をスラッシュ (/) で区切って入力します (例: Australia/Currie)。

表 2:表 4-2 オーストラリアの時間帯（続き）

Australia			
Australian Capital Territory (ACT)	Adelaide	Brisbane	Broken_Hill
Canberra	Currie	Darwin	Hobart
Lord_Howe	Lindeman	Lord Howe Island (LHI)	Melbourne
North	New South Wales (NSW)	Perth	Queensland
South	Sydney	Tasmania	Victoria
West	Yancowinna		

アジアのタイムゾーン



(注) アジアの時間帯には、東アジア、南アジア、東南アジア、西アジア、および中央アジアがあります。地域と都市または国をスラッシュ (/) で区切って入力します (例: Asia/Aden)。

表 3:表 4-3 アジアの時間帯（続き）

Asia			
Aden	Almaty	Amman	Anadyr
Aqtau	Aqtobe	Ashgabat	Ashkhabad
Baghdad	Bahrain	Baku	Bangkok
Beirut	Bishkek	Brunei	Calcutta
Choibalsan	Chongqing	Colombo	Damascus
Dhakar	Dili	Dubai	Dushanbe
Gaza	Harbin	Hong_Kong	Hovd
Irkutsk	Istanbul	Jakarta	Jayapura
Jerusalem	Kabul	Kamchatka	Karachi
Kashgar	Katmandu	Kuala_Lumpur	Kuching
Kuwait	Krasnoyarsk		

cls

端末画面の内容をクリアするには、コンフィギュレーションモードで **cls** コマンドを使用します。

cls

構文の説明

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

コンフィギュレーション (config) #

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

cls は隠しコマンドです。 **cls** は Cisco ISE で使用できますが、コマンドラインで疑問符を入力して表示しようとした場合、CLI インタラクティブヘルプには表示されません。

例

次の例は、端末の内容をクリアする方法を示しています。

```
ise/admin(config)# cls
ise/admin#
```

conn-limit

送信元 IP アドレスからの着信 TCP 接続の制限を設定するには、コンフィギュレーションモードで **conn-limit** コマンドを使用します。この機能を削除するには、このコマンドの **no** 形式を使用します。

構文の説明	<1-2147483647>	TCP 接続の数。
	<i>ip</i>	(任意)。TCP 接続制限を適用する送信元 IP アドレス。
	<i>mask</i>	(任意)。TCP 接続制限を適用する送信元 IP マスク。
	<i>port</i>	(任意)。TCP 接続制限を適用する宛先ポート番号。
コマンドデフォルト	デフォルトの動作や値はありません。	
コマンドモード	コンフィギュレーション (config) #	
コマンド履歴	リリース	変更内容
	2.0.0.306	このコマンドが導入されました。

使用上のガイドライン この **conn-limit** コマンドは、TCP 接続が 99 を超える場合に使用します。100 未満の接続の場合は、次の警告が表示されます。

```
% Warning: Setting a small conn-limit may adversely affect system performance
```

例

```
ise/admin(config)# conn-limit 25000 ip 77.10.122.133 port 22
ise/admin(config)# end
ise/admin
```

dns cache

ホストの DNS 要求をキャッシュするには、コンフィギュレーションモードで **service cache enable** コマンドを使用します。この機能を有効にすると、DNS サーバの負荷が軽減されます。

service cache enable hosts ttl ttl

この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

構文の説明

ttl

キャッシュを有効にしながら、キャッシュ内のホストの存続可能時間 (TTL) 値を秒単位で設定できます。ttl のデフォルト設定はありません。ttl の有効な値の範囲は 1 ~ 2147483647 です。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

コンフィギュレーション (config) #

使用上のガイドライン

TTL 値は、否定応答に対して受け入れられます。DNS サーバで設定された TTL 値は、肯定応答に対して受け入れられます。DNS サーバで TTL が定義されていない場合は、コマンドで設定された TTL が受け入れられます。機能を無効にするとキャッシュも無効になります。

例

```
ise/admin(config)# service cache enable hosts ttl 10000
Enabling dns cache
ise/admin(config)# exit
```

do

コンフィギュレーションモードまたは任意のコンフィギュレーションサブモードから EXEC システムレベルのコマンドを実行するには、いずれかのコンフィギュレーションモードで **do** コマンドを使用します。

do EXEC commands

構文の説明

<i>EXEC commands</i>	EXEC システム レベルのコマンドを実行することを指定します (表 4: 表 4-4 do コマンドのコマンド オプション (続き) を参照)。
----------------------	---

表 4: 表 4-4 do コマンドのコマンド オプション (続き)

コマンド	説明
application configure	特定のアプリケーションを設定します。
application install	特定のアプリケーションをインストールします。
application remove	特定のアプリケーションを削除します。
application reset-config	アプリケーション コンフィギュレーションを工場出荷時のデフォルト設定にリセットします。
application reset-passwd	指定したユーザのアプリケーションパスワードをリセットします。
application start	特定のアプリケーションを起動またはイネーブルにします。
application stop	特定のアプリケーションを停止またはディセーブルにします。
application upgrade	特定のアプリケーションをアップグレードします。
backup	バックアップ (Cisco ISE と Cisco ADE OS) を実行して、そのバックアップをリポジトリに保存します。
backup-logs	Cisco ISE サーバに記録されているすべてのログをリモートの場所にバックアップします。
clock	Cisco ISE サーバのシステムクロックを設定します。

コマンド	説明
configure	設定モードを開始します。
copy	コピー元からコピー先に任意のファイルをコピーします。
debug	さまざまなコマンド状況（たとえば、バックアップと復元、コンフィギュレーション、コピー、リソースのロック、ファイル転送、ユーザ管理など）で、エラーまたはイベントを表示します。
delete	Cisco ISE サーバ上のファイルを削除します。
dir	Cisco ISE サーバのファイルを一覧表示します。
forceout	特定の Cisco ISE ノードユーザのすべてのセッションを強制的にログアウトします。
halt	Cisco ISE サーバをディセーブルにするか、シャットダウンします。
mkdir	新しいディレクトリを作成します。
nslookup	リモートシステムの IPv4 または IPv6 アドレス、あるいはホスト名を問い合わせます。
password	CLI アカウント パスワードを更新します。
patch	パッチバンドルをインストールする、またはアプリケーションのパッチをアンインストールします。
ping	リモートシステムの IPv4 アドレスまたはホスト名を特定します。
ping6	リモートシステムの IPv6 アドレスを特定します。
reload	Cisco ISE サーバを再起動します。
restore	復元を実行して、リポジトリからバックアップを取得します。
rmdir	既存のディレクトリを削除します。
show	Cisco ISE サーバに関する情報を提供します。

コマンド	説明
ssh	リモート システムとの暗号化されたセッションを開始します。
tech	Technical Assistance Center (TAC) コマンドを提供します。
terminal length	端末回線のパラメータを設定します。
terminal session-timeout	すべてのターミナルセッションに対して、無活動タイムアウトを設定します。
terminal session-welcome	すべてのターミナルセッションで表示される初期メッセージをシステムに設定します。
terminal terminal-type	現在のセッションの現在の回線に接続されている端末のタイプを指定します。
traceroute	リモート IP アドレスのルートを追跡します。
undebug	さまざまなコマンド状況（たとえば、バックアップと復元、コンフィギュレーション、コピー、リソースのロック、ファイル転送、ユーザ管理など）で、 debug コマンドの出力（エラーまたはイベントの表示）をディセーブルにします。
write	強制的にセットアップユーティリティを実行してネットワーク コンフィギュレーションをプロンプトするスタートアップコンフィギュレーションを消去し、実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーし、コンソールに実行コンフィギュレーションを表示します。

コマンドデフォルト デフォルトの動作や値はありません。

コマンドモード コンフィギュレーション (**config**) # または任意のコンフィギュレーション サブモード (**config-GigabitEthernet**) # と (**config-Repository**) #

コマンド履歴	リリース	変更内容
	2.0.0.306	このコマンドが導入されました。

使用上のガイドライン この **do** コマンドは、Cisco ISE サーバの設定中に、EXEC コマンド (**show**、**clear**、および **debug** コマンドを含む) を実行する場合に使用します。EXEC コマンドの実行後、システムは使用していたコンフィギュレーションモードに戻ります。

例

```
ise/admin(config)# do show run
Generating configuration...
!
hostname ise
!
ip domain-name cisco.com
!
interface GigabitEthernet 0
 ip address 172.23.90.113 255.255.255.0
 ipv6 address autoconfig
!
ip name-server 171.70.168.183
!
ip default-gateway 172.23.90.1
!
clock timezone EST
!
ntp server time.nist.gov
!
username admin password hash $1$JbbHvKVG$xMZ/XL4tH15Knf.FfcZZr. role admin
!
service sshd
!
backup-staging-url nfs://loc-filer02a:/vol/local1/private1/jdoe
!
password-policy
 lower-case-required
 upper-case-required
 digit-required
 no-username
 disable-cisco-passwords
 min-password-length 6
!
logging localhost
logging loglevel 6
!
--More--
ise/admin(config)#
```

end

現在のコンフィギュレーションセッションを終了して、EXEC モードに戻るには、コンフィギュレーションモードで **end** コマンドを使用します。

このコマンドには、キーワードおよび引数はありません。

end

コマンドデフォルト デフォルトの動作や値はありません。

コマンドモード コンフィギュレーション (config) #

コマンド履歴	リリース	変更内容
	2.0.0.306	このコマンドが導入されました。

使用上のガイドライン このコマンドは、現在のコンフィギュレーションモードやサブモードにかかわらず、EXEC モードに移行します。

このコマンドは、システム設定を終了し、EXEC モードに戻って、検証手順を実行する場合に使用します。

例

```
ise/admin(config)# end
ise/admin#
```

exit

コンフィギュレーションモードを終了して、CLI モード階層で次に高いモードに移行するには、コンフィギュレーションモードで **exit** コマンドを使用します。

exit

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト デフォルトの動作や値はありません。

コマンド モード コンフィギュレーション (config) #

コマンド履歴	リリース	変更内容
	2.0.0.306	このコマンドが導入されました。

使用上のガイドライン **exit** コマンドは、Cisco ISE サーバで現在のコマンドモードを終了して、CLI モード階層の次に高いコマンドモードに移行する場合に使用します。

たとえば、EXECモードに戻るには、コンフィギュレーションモードで **exit** コマンドを使用します。コンフィギュレーションサブモードで **exit** コマンドを使用すると、コンフィギュレーションモードに戻ります。最上位の EXEC モードで **exit** コマンドを使用すると、EXEC モードを終了して、Cisco ISE サーバから接続解除されます。

例

```
ise/admin(config)# exit
ise/admin#
```

hostname

システムのホスト名を設定するには、コンフィギュレーションモードで **hostname** コマンドを使用します。

hostname *hostname*

構文の説明	<i>hostname</i>	ホストの名前。19 文字までの英数字と下線 (_) をサポートします。ホスト名はスペース以外の文字で始める必要があります。
-------	-----------------	---

コマンドデフォルト デフォルトの動作や値はありません。

コマンドモード コンフィギュレーション (config) #

コマンド履歴	リリース	変更内容
	2.0.0.306	このコマンドが導入されました。

使用上のガイドライン



(注) 「hostname」コマンドの CLI 設定変更中に「Ctrl+C」を発行すると、一部のアプリケーションコンポーネントは古いホスト名を持ち、他のコンポーネントは新しいホスト名を使用する状態になる可能性があります。これにより、Cisco ISE ノードは機能していない状態になります。

この問題を回避するには、「hostname」コンフィギュレーションコマンドを再度実行して、ホスト名を目的の値に設定します。

hostname コマンドを使用して、現在のホスト名を変更できます。シングルインスタンスタイプのコマンドである **hostname** は、システムの設定時に一度だけ実行します。ホスト名には1つの引数を含める必要があります。引数がない場合、エラーが発生します。

このコマンドを使用して Cisco ISE サーバのホスト名を更新すると、次の警告メッセージが表示されます。

```
% Warning: Updating the hostname will cause any certificate using the old
%           hostname to become invalid. Therefore, a new self-signed
%           certificate using the new hostname will be generated now for
%           use with HTTPs/EAP. If CA-signed certs were used on this node,
%           please import them with the correct hostname. If Internal-CA
%           signed certs are being used, please regenerate ISE Root CA certificate.
%           In addition, if this ISE node will be joining a new Active Directory
%           domain, please leave your current Active Directory domain before
%           proceeding. If this ISE node is already joined to
%           an Active Directory domain, then it is strongly advised
%           to rejoin all currently joined join-points in order to
%           avoid possible mismatch between current and previous
%           hostname and joined machine account name.
```

例

```
ise/admin(config)# hostname new-hostname
% Changing the hostname will cause ISE services to restart
Continue with hostname change? Y/N [N]: y

Stopping ISE Monitoring & Troubleshooting Log Processor...
ISE Identity Mapping Service is disabled
ISE pxGrid processes are disabled
Stopping ISE Application Server...
Stopping ISE Certificate Authority Service...
Stopping ISE Profiler Database...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE AD Connector...
Stopping ISE Database processes...
ISE Database processes already running, PID: 9651
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Profiler Database...
Starting ISE Application Server...
Starting ISE Certificate Authority Service...
Starting ISE Monitoring & Troubleshooting Log Processor...
Starting ISE AD Connector...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
ise-1/admin#
```

icmp echo

インターネット制御メッセージプロトコル (ICMP) のエコー応答を設定するには、コンフィギュレーションモードで **icmp echo** コマンドを使用します。

icmp echo {*off* | *on*}

構文の説明	echo	ICMP エコー応答を設定します。
	<i>off</i>	ICMP エコー応答をディセーブルにします。
	<i>on</i>	ICMP エコー応答をイネーブルにします。
コマンドデフォルト	システムは ICMP エコー応答がオン (イネーブル) の場合と同様に動作します。	
コマンドモード	コンフィギュレーション (config) #	
コマンド履歴	リリース	変更内容
	2.0.0.306	このコマンドが導入されました。
使用上のガイドライン	ICMP エコー応答をオンまたはオフにするには、この icmp echo を使用します。	

例

```
ise/admin(config)# icmp echo off
ise/admin(config)#
```

identity-store

CLI 管理者を Active Directory ドメインに参加させるには、コンフィギュレーションモードで **identity-store** コマンドを使用します。Cisco ISE ノードが複数のドメインに参加している場合は、このコマンドを使用して参加できるドメインは1つだけです。各 CLI 管理者は個別に参加します。Cisco ISE が操作を完了するまで 5 分間待ってください。

このコマンドを使用して参加するドメインが、ISE ノードに参加していたドメインと同じである場合は、管理者コンソールでドメインに再参加する必要があります。管理 CLI ユーザはネットワーク管理者である必要があります。

例

```
identity-store active-directory domain-name <aDomainFQDN> user <adUserNameWithJoinPrivs>
```


interface

インターフェイスタイプを設定し、インターフェイス コンフィギュレーション モードを開始するには、**interface** コマンドをコンフィギュレーションモードで使用します。このコマンドには **no** 形式はありません。



- (注) VMware 仮想マシンで使用可能なインターフェイスの数は、仮想マシンに追加されるネットワーク インターフェイス (NIC) の数によって異なることがあります。

interface GigabitEthernet {0|1|2|3}

構文の説明

GigabitEthernet	ギガビットイーサネット インターフェイスを設定します。
0 ~ 3	設定するギガビットイーサネット ポートの数。



- (注) **interface** コマンドでギガビットイーサネット ポートの数を入力すると、**config-GigabitEthernet** コンフィギュレーション サブモードが開始されます (次の「構文の説明」を参照)。

構文の説明

backup	NIC ボンディング機能を設定して、物理インターフェイスに高可用性を提供します。
do	EXEC コマンド。このモードで EXEC コマンドを実行できます。
end	config-GigabitEthernet サブモードを終了し、EXEC モードに戻ります。
exit	config-GigabitEthernet コンフィギュレーション サブモードを終了します。
ip	ギガビットイーサネット インターフェイスの IP アドレスとネットマスクを設定します。
ipv6	DHCPv6 サーバから IPv6 アドレス自動設定および IPv6 アドレスを設定します。

no	このモードのコマンドを否定します。2つのキーワードを使用できます。 <ul style="list-style-type: none"> • ip : インターフェイスのIPアドレスとネットマスクを設定します。 • ipv6 : インターフェイスのIPv6アドレスを設定します。 • shutdown : インターフェイスをシャットダウンします。
shutdown	インターフェイスをシャットダウンします。

コマンド デフォルト デフォルトの動作や値はありません。

コマンド モード インターフェイス コンフィギュレーション (config-GigabitEthernet) #

コマンド履歴	リリース	変更内容
	2.0.0.306	このコマンドが導入されました。

使用上のガイドライン **interface** コマンドを使用して、インターフェイスを設定し、さまざまな要件をサポートすることができます。

例

```
ise/admin(config)# interface GigabitEthernet 0
ise/admin(config-GigabitEthernet)#
```

ip address

GigabitEthernet インターフェイスの IP アドレスとネットマスクを設定するには、インターフェイス コンフィギュレーションモードで **ip address** コマンドを使用します。

ip address *ip-address network mask*

IP アドレスを削除するか、IP プロセッシングを無効にするには、このコマンドの **no** 形式を使用します。

no ip address



(注) 複数のインターフェイスで、同じ IP アドレスを設定できます。この設定により、2 つのインターフェイス間の切り替えに必要なコンフィギュレーション手順を制限できます。

構文の説明

<i>ip-address</i>	IPv4 アドレス。
<i>network mask</i>	関連付けられた IP サブネットのマスク。

プライマリ管理ノード (PAN) の自動フェールオーバー設定をイネーブルにしている場合は、IP アドレスを設定する前にディセーブルにしてください。IP アドレスの設定後に PAN の自動フェールオーバー設定をイネーブルに戻すことができます。

コマンドデフォルト

イネーブル。

コマンドモード

インターフェイス コンフィギュレーション (config-GigabitEthernet) #

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン



(注) 「ip address」コマンドの CLI 設定変更中に「Ctrl+C」を発行すると、IP アドレスを変更する場合、一部のアプリケーション コンポーネントは古い IP アドレスを使用し、他のコンポーネントは新しい IP アドレスを使用する状態になる可能性があります。

これにより、Cisco ISE ノードは機能していない状態になります。これを回避するには、別の「ip address」コンフィギュレーション CLI を発行して、IP アドレスを目的の値に設定します。

アドレスとネットマスクを必ず1つずつ指定する必要があります。指定しない場合、エラーが発生します。

展開内で PAN の自動フェールオーバー設定がイネーブルになっていると、次のメッセージが表示されます。

```
PAN Auto Failover is enabled, this operation is not
allowed! Please disable PAN Auto-failover first.
```

例

```
ise/admin(config)# interface GigabitEthernet 1
ise/admin(config-GigabitEthernet)# ip address 209.165.200.227 255.255.255.224
Changing the hostname or IP may result in undesired side effects,
such as installed application(s) being restarted.
.....
To verify that ISE processes are running, use the
'show application status ise' command.
ise/admin(config-GigabitEthernet)#
```

ip default-gateway

IPアドレスを指定してデフォルトゲートウェイを定義または設定するには、コンフィギュレーションモードで **ip default-gateway** コマンドを使用します。

ip default-gateway *ip-address*

この機能を無効にするには、このコマンドの **no** 形式を使用します。

no ip default-gateway

構文の説明	default-gateway	IPアドレスを指定してデフォルトゲートウェイを定義します。
	<i>ip-address</i>	デフォルトゲートウェイのIPアドレス。
コマンドデフォルト	ディセーブル。	
コマンドモード	コンフィギュレーション (config) #	
コマンド履歴	リリース	変更内容
	2.0.0.306	このコマンドが導入されました。

使用上のガイドライン 複数の引数を指定した場合、または引数を指定していない場合はエラーが発生します。

例

```
ise/admin(config)# ip default-gateway 209.165.202.129
ise/admin(config)#
```

ip domain-name

Cisco ISE サーバがホスト名を完成させるために使用するデフォルトのドメイン名を定義するには、コンフィギュレーションモードで **ip domain-name** コマンドを使用します。

ip domain-name *domain-name*

この機能を無効にするには、このコマンドの **no** 形式を使用します。

no ip domain-name

構文の説明	domain-name	デフォルトのドメイン名を定義します。
	<i>domain-name</i>	ホスト名を完成させるために使用するデフォルトのドメイン名。2～64文字の英数字で指定します。
コマンド デフォルト	イネーブル。	
コマンド モード	コンフィギュレーション (config) #	
コマンド履歴	リリース	変更内容
	2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

(注) 「ip domain-name」コマンドの CLI 設定変更中に「Ctrl+C」を発行すると、IP ドメイン名を変更する場合、一部のアプリケーションコンポーネントは古いドメイン名を持ち、他のコンポーネントは新しいドメイン名を使用する状態になる可能性があります。

これにより、Cisco ISE ノードは機能していない状態になります。これを回避するには、別の「ip domain-name」コンフィギュレーション CLI を発行して、ドメイン名を目的の値に設定します。

入力した引数が多すぎる場合または不足している場合、エラーが発生します。

このコマンドで Cisco ISE サーバのドメイン名を更新する場合は、次の警告メッセージが表示されます。

```
% Warning: Updating the domain name will cause any certificate using the old
% domain name to become invalid. Therefore, a new self-signed
% certificate using the new domain name will be generated now for
% use with HTTPs/EAP. If CA-signed certs were used on this node,
% please import them with the correct domain name. If Internal-CA
% signed certs are being used, please regenerate ISE Root CA certificate.
% In addition, if this ISE node will be joining a new Active Directory
```

```
%          domain, please leave your current Active Directory domain before  
%          proceeding.
```

例

```
ise/admin(config)# ip domain-name cisco.com  
ise/admin(config)#
```

ip host

eth1、eth2、eth3 など eth0 以外のイーサネット インターフェイスにホストエイリアスと完全修飾ドメイン名 (FQDN) 文字列を関連付けるには、グローバルコンフィギュレーションモードで **ip host** コマンドを使用します。

Cisco ISE は認証プロファイルのリダイレクト URL を処理するときに、その IP アドレスを Cisco ISE ノードの FQDN に置き換えます。

ip host [*ipv4-address* | *ipv6-address*] [*host-alias* | *FQDN-string*]

ホストエイリアスと FQDN の関連付けを削除するには、このコマンドの **no** 形式を使用します。

no ip host [*ipv4-address* | *ipv6-address*] [*host-alias* | *FQDN-string*]

構文の説明		
	<i>ipv4-address</i>	ネットワーク インターフェイスの IPv4 アドレス。
	<i>ipv6-address</i>	ネットワーク インターフェイスの IPv6 アドレス。
	<i>host-alias</i>	ホストのエイリアスは、ネットワーク インターフェイスに割り当てる名前です。
	<i>FQDN-string</i>	ネットワーク インターフェイスの完全修飾ドメイン名 (FQDN)。

プライマリ管理ノード (PAN) の自動フェールオーバー設定をイネーブルにしている場合は、イーサネット インターフェイスのホスト エイリアスおよび FQDN を変更する前にディセーブルにしてください。ホスト エイリアスおよび FQDN の設定完了後に PAN の自動フェールオーバー設定をイネーブルに戻すことができます。

展開内で PAN の自動フェールオーバー設定がイネーブルになっていると、次のメッセージが表示されます。

```
PAN Auto Failover is enabled, this operation is not allowed! Please disable PAN Auto-failover first.
```

コマンド デフォルト	デフォルトの動作や値はありません。	
コマンド モード	コンフィギュレーション (config) #	
コマンド履歴	リリース	変更内容
	2.0.0.306	このコマンドが導入されました。

使用上のガイドライン サポートされている IPv6 アドレス形式は次のとおりです。

- 完全表記：コロンで区切られた4つの16進数桁の8つのグループ。たとえば、2001:0db8:85a3:0000:0000:8a2e:0370:7334 です。
- 短縮表記：1つのグループ内にある先行ゼロは除きます。ゼロのグループを2つの連続するコロンに置き換えます。たとえば、2001:db8:85a3::8a2e:370:7334 です。
- ドット区切りの4つの表記（IPv4 対応付けおよび IPv4 互換性 IPv6 アドレス）：たとえば、::ffff:192.0.2.128 です。

ip host コマンドを使用して、IP アドレスマッピング用にホストエイリアスと完全修飾ドメイン名 (FQDN) 文字列を追加します。eth1、eth2、eth3 などのイーサネットインターフェイスに一致する FQDN を検索する場合に使用します。ホストのエイリアスの定義を表示するには、**show running-config** コマンドを使用します。

ホストエイリアスか FQDN 文字列、またはその両方を指定できます。両方の値を指定する場合は、ホストエイリアスと FQDN 文字列の最初のコンポーネントが一致している必要があります。FQDN 文字列のみを指定すると、Cisco ISE は URL 内の IP アドレスを FQDN に置き換えます。ホストエイリアスのみを指定すると、Cisco ISE はホストエイリアスと設定されている IP ドメイン名を組み合わせる完全な FQDN を形成し、URL 内のネットワークインターフェイスの IP アドレスを FQDN に置き換えます。

例 1

```
ise/admin(config)# ip host 172.21.79.96 isel isel.cisco.com
Host alias was modified. You must restart ISE for change to take effect.
Do you want to restart ISE now? (yes/no) yes
Stopping ISE Monitoring & Troubleshooting Log Processor...
Stopping ISE Application Server...
Stopping ISE Profiler DB...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE Database processes...
Starting ISE Database processes...
Stopping ISE Database processes...
Starting ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Profiler DB...
Starting ISE Application Server...
Starting ISE Monitoring & Troubleshooting Log Processor...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
ise/admin(config)#
```

例 2

```
ise/admin(config)# ipv6 host 2001:db8:cc00:1::1 isel isel.cisco.com
Host alias was modified. You must restart ISE for change to take effect.
Do you want to restart ISE now? (yes/no) yes
Stopping ISE Monitoring & Troubleshooting Log Processor...

Stopping ISE Application Server...
Stopping ISE Profiler DB...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE Database processes...
Starting ISE Database processes...
Stopping ISE Database processes...
Starting ISE Database processes...
```

```

Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Profiler DB...
Starting ISE Application Server...
Starting ISE Monitoring & Troubleshooting Log Processor...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
ise/admin(config)#
    
```

ip mtu

インターフェイスで送信される IP パケットの最大伝送ユニット (MTU) サイズを設定するには、インターフェイス コンフィギュレーション モードで **ip mtu** コマンドを使用します。デフォルトの MTU サイズに戻すには、このコマンドの **no** 形式を使用します。

ip mtu bytes

no ip mtu bytes

構文の説明	mtu	ISE インターフェイスの MTU を設定します。
	bytes	MTU のバイト単位のサイズ (1300 ~ 1500)。デフォルトの MTU 値は 1500 です。

コマンドデフォルト MTU は 1500 として設定されます。

コマンドモード インターフェイス コンフィギュレーション (config-GigabitEthernet) #

コマンド履歴	リリース	変更内容
	2.4.0.357	このコマンドが導入されました。

使用上のガイドライン IP パケットがインターフェイスに設定された MTU を超過すると、Cisco ISE はそれをフラグメント化します。物理メディアのすべてのデバイスが動作するには、同じプロトコル MTU を持っている必要があります。

例

次の例は、インターフェイスで MTU を設定する方法を示しています。

```
ise/admin(config)# int GigabitEthernet 1
ise/admin(config-GigabitEthernet)# ip mtu ?
<1300-1500> Select MTU value in range of 1300 to 1500
```

次の例は、MTU の設定後に表示される出力を示しています。

```
ise/admin# show run | in mtu
ip mtu 1350
```

ip name-server

DNS クエリー実行時に使用するドメインネームサーバ (DNS) を設定するには、コンフィギュレーション モードで **ip name-server** コマンドを使用します。1 ~ 3 台の DNS サーバを設定できます。

ip name-server ip-address {ip-address*}

この機能を無効にするには、このコマンドの **no** 形式を使用します。

no ip name-server ip-address {ip-address*}



(注) このコマンドの **no** 形式を使用すると、設定からすべてのネームサーバが削除されます。このコマンドの **no** 形式と IP 名の 1 つを使用すると、そのネームサーバだけが削除されます。

構文の説明

name-server	ネームサーバの IP アドレスを設定します。
<i>ip-address</i>	ネームサーバのアドレス。
<i>ip-address*</i>	(任意)。追加のネームサーバの IP アドレス。 (注) IPv4/IPv6 アドレスの一方または両方を設定できます。IPv6 アドレスでネームサーバを追加する場合は、ISE eth0 インターフェイスが IPv6 アドレスで静的に設定されていることを確認してください。

展開内でプライマリ管理ノード (PAN) の自動フェールオーバー設定をイネーブルにしている場合は、**ip name-server** コマンドを実行する前にディセーブルにし、DNS サーバを設定した後でイネーブルに戻してください。

コマンド デフォルト デフォルトの動作や値はありません。

コマンド モード コンフィギュレーション (config) #

コマンド履歴	リリース	変更内容
	2.0.0.306	このコマンドが導入されました。

使用上のガイドライン **ip name-server** コマンドを使用して追加された最初のネームサーバは最初の位置に配置されません。システムはそのサーバを最初に使用して、IP アドレスを解決します。

IPv4 または IPv6 アドレスを使用してシステムにネームサーバを追加できます。1つのコマンドで、1～3つの IPv4 または IPv6 アドレスを設定できます。システムにすでに3台のネームサーバが設定されている場合、少なくとも1台を削除するまでネームサーバを追加できません。

1台のネームサーバを最初の位置に配置して、サブシステムがまずそのサーバを使用するようにするには、このコマンドの **no** 形式を使用してすべてのネームサーバを削除してから処理を進める必要があります。



- (注) AD接続のこの設定を変更した場合、変更を有効にするためにCisco ISEを再起動する必要があります。また、Cisco ISEで設定されているすべてのDNSサーバがすべての関連するAD DNSレコードを解決できる必要があります。DNS設定が変更された後、設定済みのAD参加ポイントが正しく解決されない場合、脱退処理を手動で実行してから、AD参加ポイントを再参加させる必要があります。

展開内でPANの自動フェールオーバー設定がイネーブルになっていると、次のメッセージが表示されます。

```
PAN Auto Failover is enabled, this operation is not
allowed! Please disable PAN Auto-failover first.
```

例 1

```
ise/admin(config)# ip name-server ?
<A.B.C.D>|<valid IPv6 format> Primary DNS server IP address
<A.B.C.D>|<valid IPv6 format> DNS server 2 IP address
<A.B.C.D>|<valid IPv6 format> DNS server 3 IP address

ise/admin(config)# ip name-server
```

例 2

IPネームサーバを設定した後に、次の出力が表示されます。

```
ise/admin# show run | in name-server
ip name-server 171.70.168.183 171.68.226.120
3201:db8:0:20:f41d:eee:7e66:4eba
ise/admin#
```

例 3

```
ise/admin(config)# ip name-server ?
ip name-server 10.126.107.120 10.126.107.107 10.106.230.244
DNS Server was modified. If you modified this setting for AD connectivity, you must
restart ISE for the change to take effect.
Do you want to restart ISE now? (yes/no)
```

ip route

スタティックルートを設定するには、コンフィギュレーションモードで **ip route** コマンドを使用します。スタティックルートを削除するには、このコマンドの **no** 形式を使用します。

ip route *prefix mask gateway ip-address*

no ip route *prefix mask*

構文の説明	<i>prefix</i>	宛先の IP ルート プレフィクス。
	<i>mask</i>	宛先のプレフィクス マスク。
	<i>ip-address</i>	ネットワークに到達するために使用可能なネクストホップの IP アドレス。
コマンド デフォルト	デフォルトの動作や値はありません。	
コマンド モード	コンフィギュレーション (config) #	
コマンド履歴	リリース	変更内容
	2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

スタティック ルートは手動で設定されます。これによって、柔軟性が低くなります（ネットワーク ポロジの変更に対応できません）が、安定性は非常に高くなります。スタティックルートでは、維持するためにルーティングの更新を送信される必要がないため、帯域幅使用率が最適化されます。また、ルーティング ポリシーの実施が容易になります。

ip route コマンドは個々の Cisco ISE ノードでのスタティックルートの定義に使用できるだけでなく、各インターフェイスのデフォルトルートを定義して、マルチインターフェイス IP ノードに固有の非対称 IP 転送の影響を軽減するために拡張されます。

単一のデフォルト ルートがマルチインターフェイス ノードに設定されている場合、ノードのいずれかの IP インターフェイスから受信したすべての IP トラフィックは、非対称 IP 転送を生成するデフォルト ゲートウェイのネクストホップにルーティングされます。Cisco ISE ノードに複数のデフォルトルートを設定すると、非対称転送の影響がなくなります。

次の例に、複数のデフォルト ルートを設定する方法を示します。

Cisco ISE ノード eth0、eth1、eth2、および eth3 インターフェイスの次のインターフェイス設定についてそれぞれ考えてみてください。

```
ISE InterfaceIPNetworkGateway
192.168.114.10 192.168.114.0 192.168.114.1
192.168.115.10 192.168.115.0 192.168.115.1
192.168.116.10 192.168.116.0 192.168.116.1
192.168.117.10 192.168.117.0 192.168.117.1
```

ip route コマンドは、ここでは各インターフェイスのデフォルトルートを定義するために使用されます。

```
ise/admin(config)# ip route 0.0.0.0 0.0.0.0 192.168.114.1
ise/admin(config)# ip route 0.0.0.0 0.0.0.0 192.168.115.1
ise/admin(config)# ip route 0.0.0.0 0.0.0.0 192.168.116.1
ise/admin(config)# ip route 0.0.0.0 0.0.0.0 192.168.117.1
ise/admin(config)# ip default-gateway 192.168.118.1
```



(注) 上記の「ip default-gateway」は、すべてのインターフェイスのラストリゾートのルートです。

show ip route コマンドでは、**ip route** コマンドを使用して作成したスタティックルート（デフォルトルートとデフォルト以外のルート）、および「ip default gateway」コマンドの使用により設定されたルートを含むシステムによって作成されたルートの出力が表示されます。これは、各ルートの発信インターフェイスを表示します。



(注) インターフェイスの IP アドレスを変更した場合、到達不能なゲートウェイのためにいずれかのスタティックルートが到達不能になると、そのスタティックルートは実行コンフィギュレーションから削除されます。到達不能になったルートはコンソールに表示されます。

例 2

```
ise/admin(config)# ip route 192.168.0.0 255.255.0.0 gateway 172.23.90.2
ise/admin(config)#
```

ipv6 address

IPv6 の一般的なプレフィックスに基づいてスタティック IPv6 アドレスを設定し、インターフェイスで IPv6 処理を有効にするには、インターフェイス コンフィギュレーションモードで **ipv6 address** コマンドを使用します。

ipv6 address *ipv6-address/prefix-length*

IPv6 アドレスを削除するか、IPv6 処理を無効にするには、このコマンドの **no** 形式を使用します。

no ipv6 address *ipv6-address/prefix-length*

構文の説明

<i>ipv6-address</i>	IPv6 アドレス。
<i>prefix-length</i>	IPv6 プレフィックスの長さ。プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す 0 ~ 128 の 10 進数値です。10 進値の前にスラッシュ記号を付ける必要があります。

プライマリ管理ノード（PAN）の自動フェールオーバー設定をイネーブルにしている場合は、IPv6 アドレスを設定する前にディセーブルにしてください。IPv6 アドレスの設定後に PAN の自動フェールオーバー設定をイネーブルに戻すことができます。

展開内で PAN の自動フェールオーバー設定がイネーブルになっていると、次のメッセージが表示されます。

```
PAN Auto Failover is enabled, this operation is not allowed! Please disable PAN Auto-failover first.
```

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

インターフェイス コンフィギュレーション (config-GigabitEthernet) #

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

サポートされている IPv6 アドレス形式は次のとおりです。

- 完全表記：コロンで区切られた 4 つの 16 進数桁の 8 つのグループ。たとえば、2001:0db8:85a3:0000:0000:8a2e:0370:7334 です。
- 短縮表記：1 つのグループ内にある先行ゼロは除きます。ゼロのグループを 2 つの連続するコロンに置き換えます。たとえば、2001:db8:85a3::8a2e:370:7334 です。
- ドット区切り表記（IPv4 マッピングおよび IPv4 互換の IPv6 アドレス）：::ffff:192.0.2.128 など

fe80 プレフィックスを使用してリンクローカルアドレスを割り当てます。インターフェイスにグローバルアドレスを割り当てると、リンクローカルアドレスが自動的に作成されます。



- (注) IPv6 アドレスを変更する場合、**ipv6 address** コマンドでの CLI 設定変更中に Ctrl+C を押すと、システムの一部のアプリケーション コンポーネントは古い IPv6 アドレスを使用し、他のコンポーネントは新しい IPv6 アドレスを使用する状態になる可能性があります。

これにより、Cisco ISE ノードは機能していない状態になります。これを回避するには、別の **ipv6 address** コマンドを実行して IPv6 アドレスを目的の値に設定します。

例 1

```
ise/admin(config)# interface GigabitEthernet 1
ise/admin(config-GigabitEthernet)# ipv6 address 2001:DB8:0:1::/64
Changing the IPv6 address may result in undesired side effects on any installed
application(s).
Are you sure you want to proceed? Y/N[N]: y
.....
Note: ISE Processes are initializing. Use 'show application status ise' CLI to verify
all processes are in running state.
ise/admin(config-GigabitEthernet)#
```

例 2

```
ise/admin(config)# interface GigabitEthernet 1
ise/admin(config-GigabitEthernet)# ipv6 address fe80::250:56ff:fe87:4763/64
ise/admin(config-GigabitEthernet)#
```

ipv6 address autoconfig

インターフェイスのステートレス自動設定を使用した IPv6 アドレスの自動設定を有効にし、インターフェイスで IPv6 処理を有効にするには、インターフェイス コンフィギュレーションモードで **ipv6 address autoconfig** コマンドを使用します。

IPv6 アドレス自動設定は、Linux ではデフォルトでイネーブルです。Cisco ADE 2.0 は、イネーブルになっている任意のインターフェイスの実行コンフィギュレーションで IPv6 アドレス自動設定を示します。

ipv6 address autoconfig

インターフェイスで IPv6 アドレスの自動設定を無効にするには、このコマンドの **no** 形式を使用します。

コマンド デフォルト	デフォルトの動作や値はありません。	
コマンド モード	インターフェイス コンフィギュレーション (config-GigabitEthernet) #	
コマンド履歴	リリース	変更内容
	2.0.0.306	このコマンドが導入されました。

使用上のガイドライン IPv6 ステートレス自動設定には、予測可能な IP アドレスを持つというセキュリティ面の落とし穴があります。この落とし穴は、プライバシーの拡張によって解決されます。**show interface** コマンドを使用して、プライバシー機能拡張が有効になっていることを確認できます。

例

```
ise/admin(config-GigabitEthernet)# ipv6 address autoconfig
ise/admin(config)#
```

IPv6 自動設定の設定

IPv6 ステートレス自動設定を有効にするには、インターフェイスコンフィギュレーションモードで **interface GigabitEthernet 0** コマンドを使用します。

```
ise/admin# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ise/admin(config)# interface GigabitEthernet 0
ise/admin(config)# (config-GigabitEthernet)# ipv6 address autoconfig
ise/admin(config)# (config-GigabitEthernet)# end
ise/admin#
```

IPv6 自動設定がイネーブルの場合、実行コンフィギュレーションは次のようなインターフェイス設定を表示します。

```
!
interface GigabitEthernet 0
```

```
ip address 172.23.90.116 255.255.255.0
ipv6 address autoconfig
!
```

インターフェイス設定を表示するには、**show interface GigabitEthernet 0** コマンドを使用できます。次の例では、インターフェイスに 3 個の IPv6 アドレスがあることを確認できます。最初のアドレス (3ffe 以降) は、ステートレス自動設定を使用して取得されます。

ステートレス自動設定が機能するには、そのサブネットで IPv6 ルート アドバタイズメントがイネーブルになっている必要があります。次のアドレス (fe80 以降) は、ホストの外部にスコープが存在しないリンクローカルアドレスです。

IPv6 自動設定または DHCPv6 設定に関係なくリンクローカルアドレスが常に表示されます。最後のアドレス (2001 以降) は、IPv6 DHCP サーバから取得されます。

```
ise/admin# show interface GigabitEthernet 0
eth0      Link encap:Ethernet  HWaddr 00:0C:29:AF:DA:05
          inet addr:172.23.90.116  Bcast:172.23.90.255  Mask:255.255.255.0
          inet6 addr: 3ffe:302:11:2:20c:29ff:feaf:da05/64 Scope:Global
          inet6 addr: fe80::20c:29ff:feaf:da05/64 Scope:Link
          inet6 addr: 2001:558:ff10:870:8000:29ff:fe36:200/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:77848 errors:0 dropped:0 overruns:0 frame:0
          TX packets:23131 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10699801 (10.2 MiB)  TX bytes:3448374 (3.2 MiB)
          Interrupt:59 Base address:0x2000
ise/admin#
```

プライバシー拡張機能の確認

show interface GigabitEthernet 0 コマンドを使用して、プライバシー機能拡張が有効になっていることを確認できます。2 つの自動設定アドレスが表示されます。1 つのアドレスはプライバシー拡張なしで、もう 1 つはプライバシー拡張ありです。

次の例では MAC は 3ffe:302:11:2:20c:29ff:feaf:da05/64 で、非 RFC3041 アドレスには MAC が含まれています。プライバシー拡張アドレスは 302:11:2:9d65:e608:59a9:d4b9/64 です。

出力は次のように表示されます。

```
ise/admin# show interface GigabitEthernet 0
eth0      Link encap:Ethernet  HWaddr 00:0C:29:AF:DA:05
          inet addr:172.23.90.116  Bcast:172.23.90.255  Mask:255.255.255.0
          inet6 addr: 3ffe:302:11:2:9d65:e608:59a9:d4b9/64 Scope:Global
          inet6 addr: 3ffe:302:11:2:20c:29ff:feaf:da05/64 Scope:Global
          inet6 addr: fe80::20c:29ff:feaf:da05/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:60606 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2771 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:9430102 (8.9 MiB)  TX bytes:466204 (455.2 KiB)
          Interrupt:59 Base address:0x2000
ise/admin#
```

ipv6 address dhcp

IPv6 (DHCPv6) サーバの Dynamic Host Configuration Protocol からインターフェイス上に IPv6 アドレスを取得するには、インターフェイス コンフィギュレーションモードで **ipv6 address dhcp** コマンドを使用します。インターフェイスからアドレスを削除するには、このコマンドの **no** 形式を使用します。

ipv6 address dhcp

コマンド デフォルト	デフォルトの動作や値はありません。	
コマンド モード	インターフェイス コンフィギュレーション (config-GigabitEthernet) #	
コマンド履歴	リリース	変更内容
	2.0.0.306	このコマンドが導入されました。

使用上のガイドライン 例

```
ise/admin# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ise/admin(config)# interface GigabitEthernet 1
ise/admin(config-GigabitEthernet)# ipv6 address dhcp
ise/admin(config-GigabitEthernet)# end
ise/admin#
```

IPv6DHCPがイネーブルの場合、実行コンフィギュレーションは次のようなインターフェイス設定を表示します。

```
!
interface GigabitEthernet 1
    ipv6 address dhcp
    ipv6 enable
!
```



(注) IPv6 ステータス自動設定および IPv6 アドレス DHCP は相互に排他的ではありません。同じインターフェイスに IPv6 ステータス自動設定および IPv6 アドレス DHCP の両方を指定できません。

どのIPv6アドレスが特定のインターフェイスで使用されているかを表示するには、**show interface** コマンドを使用します。

IPv6 ステータス自動設定および IPv6 アドレス DHCP の両方がイネーブルの場合、実行コンフィギュレーションは次のようなインターフェイス設定を表示します。

```
!
interface GigabitEthernet 1
    ipv6 address dhcp
```

```
    ipv6 address autoconfig  
    ipv6 enable  
!
```

ipv6 enable

インターフェイス上の IPv6 を有効にするには、インターフェイス コンフィギュレーションモードで **ipv6 enable** コマンドを使用します。

ipv6 enable

インターフェイスで GVRP を無効にするには、このコマンドの **no** 形式を使用します。

no ipv6 enable

コマンド デフォルト	デフォルトの動作や値はありません。	
コマンド モード	インターフェイス コンフィギュレーション (config-GigabitEthernet) #	
コマンド履歴	リリース	変更内容
	2.0.0.306	このコマンドが導入されました。

使用上のガイドライン **ipv6 enable** コマンドは、インターフェイスで IPv6 を有効化し、インターフェイス MAC アドレスに基づいてリンクローカルアドレスを自動生成する場合に使用します。

例 1

```
ise/admin(config)# interface GigabitEthernet 1
ise/admin(config-GigabitEthernet)# ipv6 enable
ise/admin(config-GigabitEthernet)#
```

例 2

デフォルトでは、**ipv6**が、すべてのインターフェイスで有効になっています。これを無効にするには、このコマンドの **no** 形式を使用します。

```
ise/admin# show interface gigabitEthernet 1
GigabitEthernet 1
flags=4163UP,BROADCAST,RUNNING,MULTICAST mtu 1500
inet6 fe80::20c:29ff:fe83:a610 prefixlen 64 scopeid 0x20 link
ether 00:0c:29:83:a6:10 txqueuelen 1000 (Ethernet)
RX packets 11766 bytes 1327285 (1.2 MiB)
RX errors 0 dropped 13365 overruns 0 frame 0
TX packets 6 bytes 508 (508.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
ise/admin# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ise/admin(config)# interface gigabitEthernet 1
ise/admin(config-GigabitEthernet)# no ipv6 enable
ise/admin(config-GigabitEthernet)# exit
ise/admin(config)# end
ise/admin# show interface gigabitEthernet 1
GigabitEthernet 1
flags=4163 UP,BROADCAST,RUNNING,MULTICAST mtu 1500
```

```
ether 00:0c:29:83:a6:10 txqueuelen 1000 (Ethernet)
RX packets 64 bytes 5247 (5.1 KiB)
RX errors 0 dropped 13365 overruns 0 frame 0
TX packets 3 bytes 258 (258.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

ipv6 route

IPv6 スタティックルートを手動で設定し、2台のネットワークデバイス間の明示的なパスを定義するには、グローバル コンフィギュレーションモードで **ipv6 route** コマンドを使用します。スタティック ルートは自動的に更新されないで、ネットワーク トポロジが変化した場合は手動でスタティック ルートを再設定する必要があります。

ipv6 route ipv6-address/prefix-length gateway route-specific gateway

IPv6 スタティックルートを削除するには、このコマンドの **no** 形式を使用します。

no ipv6 route ipv6-address/prefix-length gateway route-specific gateway

IPv6 アドレスを指定してデフォルト スタティック ルートを設定するには、グローバル コンフィギュレーションモードで **ipv6 route ::/0 gateway route-specific gateway** コマンドを使用します。IPv6 アドレスを指定してデフォルト スタティック ルートを無効にするには、このコマンドの **no** 形式を使用します。

構文の説明	<i>ipv6-address</i>	IPv6 アドレス。
	<i>prefix-length</i>	IPv6 プレフィックスの長さ。プレフィックス (アドレスのネットワーク部分) を構成するアドレスの上位連続ビット数を示す 0 ~ 128 の 10 進数値です。10 進値の前にスラッシュ記号を付ける必要があります。
	<i>route-specific gateway</i>	そのネットワークに到達するために使用できるネクストホップの IPv6 アドレス。
コマンド デフォルト	デフォルトの動作や値はありません。	
コマンド モード	グローバル コンフィギュレーション (config) #	
コマンド履歴	リリース	変更内容
	2.0.0.306	このコマンドが導入されました。

使用上のガイドライン サポートされている IPv6 アドレス形式は次のとおりです。

- 完全表記 : コロンで区切られた 4 つの 16 進数桁の 8 つのグループ。たとえば、2001:0db8:85a3:0000:0000:8a2e:0370:7334 です。
- 短縮表記 : 1 つのグループ内にある先行ゼロは除きます。ゼロのグループを 2 つの連続するコロンに置き換えます。たとえば、2001:db8:85a3::8a2e:370:7334 です。
- ドット区切り表記 (IPv4 マッピングおよび IPv4 互換の IPv6 アドレス) : ::ffff:192.0.2.128 など

show ipv6 route コマンドは、設定済みの IPv6 ルートを表示する場合に使用します。

例 1

```
ise/admin(config)# ipv6 route 2001:DB8:cc00:1::/64 gateway 2001:DB8::cc00:1::1
```

例 2


```
ise/admin(config)# ipv6 route ::/0 gateway 2001:db::5
```

::/0 はデフォルト ルート プレフィックスを示します。

kron occurrence

1つ以上のコマンドスケジューラ コマンドが特定の日時または一定間隔で実行されるようにスケジューリングするには、コンフィギュレーションモードで **kron occurrence** コマンドを使用します。このスケジュールを削除するには、このコマンドの **no** 形式を使用します。

kron occurrence *occurrence-name*

構文の説明	occurrence	コマンドスケジューラ コマンドをスケジューリングします。
	<i>occurrence-name</i>	オカレンスの名前。最大 80 文字の英数字をサポートします。（次の「注」と「構文の説明」を参照）。
 (注)	kron occurrence コマンドで <i>occurrence-name</i> を入力すると、 config-Occurrence コンフィギュレーション サブモードが開始されます（次の「構文の説明」を参照）。	
	構文の説明	at
	do	EXEC コマンド。このモードで EXEC コマンドを実行できます。
	end	kron-occurrence コンフィギュレーション サブモードを終了し、EXEC モードに戻ります。
	exit	kron-occurrence コンフィギュレーション モードを終了します。
	no	このモードのコマンドを否定します。
		3つのキーワードを使用できます。
		<ul style="list-style-type: none"> • at : 使用方法 : at [<i>hh:mm</i>] [<i>day-of-week</i> <i>day-of-month</i> <i>month day-of-month</i>]
		<ul style="list-style-type: none"> • policy-list : オカレンスによって実行されるポリシー リストを指定します。最大 80 文字の英数字をサポートします。
		<ul style="list-style-type: none"> • recurring : ポリシー リストの実行を繰り返します。

policy-list	オカレンスによって実行されるコマンドスケジューラ ポリシー リストを指定します。
recurring	繰り返して実行するオカレンスを指定します。 (注) kron オカレンスが繰り返されない場合、スケジュール バックアップの kron オカレンスの設定が実行後に削除されます。

コマンドデフォルト デフォルトの動作や値はありません。

コマンドモード コンフィギュレーション (config-Occurance) #

コマンド履歴	リリース	変更内容
	2.0.0.306	このコマンドが導入されました。

使用上のガイドライン **kron occurrence** および **policy-list** コマンドを使用して、1 つ以上のポリシーリストが同じ時間または間隔で実行されるようにスケジューリングします。

EXEC CLI コマンドを含むコマンドスケジューラ ポリシーを作成して、指定した時刻に Cisco ISE サーバで実行されるようにスケジューリングするには、**cli** コマンドとともに **kron policy-list** コマンドを使用します。



(注) **kron** コマンドを実行すると、一意の名前 (タイムスタンプの追加により) でバックアップバンドルが作成されるため、ファイルが互いに上書きされることはありません。



(注) **Administration > System > Backup and Restore** ページを使用して、GUI を介して設定またはモニタリングのバックアップをスケジューリングすることを推奨します。

例 1 : 週次バックアップ

```
ise/admin(config)# kron occurrence WeeklyBackup
ise/admin(config-Occurrence)# at 14:35 Monday
ise/admin(config-Occurrence)# policy-list SchedBackupPolicy
ise/admin(config-Occurrence)# recurring
ise/admin(config-Occurrence)# exit
ise/admin(config)#
```

例 2 : 日次バックアップ

```
ise/admin(config)# kron occurrence DailyBackup
```

```
ise/admin(config-Occurrence)# at 02:00
ise/admin(config-Occurrence)# exit
ise/admin(config)#
```

例 3 : 週次バックアップ

```
ise/admin(config)# kron occurrence WeeklyBackup
ise/admin(config-Occurrence)# at 14:35 Monday
ise/admin(config-Occurrence)# policy-list SchedBackupPolicy
ise/admin(config-Occurrence)# no recurring
ise/admin(config-Occurrence)# exit
ise/admin(config)#
```

kron policy-list

コマンドスケジューラポリシーの名前を指定し、kron-Policy List コンフィギュレーションサブモードを開始するには、コンフィギュレーションモードで **kron policy-list** コマンドを使用します。コマンドスケジューラポリシーを削除するには、このコマンドの **no** 形式を使用します。

kron policy-list *list-name*

構文の説明	policy-list	コマンドスケジューラポリシーの名前を指定します。
	<i>list-name</i>	ポリシーリストの名前。最大 80 文字の英数字をサポートします。



(注) **kron policy-list** コマンドで *list-name* を入力すると、config-Policy List コンフィギュレーションサブモードが開始されます（次の「構文の説明」を参照）。

構文の説明	cli	スケジューラによって実行されるコマンド。最大 80 文字の英数字をサポートします。
	do	EXEC コマンド。このモードで EXEC コマンドを実行できます。
	end	config-Policy List コンフィギュレーションサブモードを終了し、EXEC モードに戻ります。
	exit	このサブモードを終了します。
	no	このモードのコマンドを否定します。次の 1 つのキーワードを使用できます。 <ul style="list-style-type: none"> • cli : スケジューラによって実行されるコマンド。

コマンドデフォルト デフォルトの動作や値はありません。

コマンドモード コンフィギュレーション (config-Policy List) #

コマンド履歴	リリース	変更内容
	2.0.0.306	このコマンドが導入されました。

使用上のガイドライン EXEC CLI コマンドを含むコマンド スケジューラ ポリシーを作成して、指定した時刻に ISE サーバで実行されるようにスケジューリングするには、**cli** コマンドとともに **kron policy-list** コマンドを使用します。**kron occurrence** および **policy list** コマンドを使用して、1 つ以上のポリシーリストが同じ時間または間隔で実行されるようにスケジューリングします。



(注) **kron policy-list** コマンドを使用して、CLI から設定および動作データのバックアップをスケジューリングすることはできません。Cisco ISE 管理者ポータルからこれらのバックアップをスケジューリングできます。

例

```
ise/admin(config)# kron policy-list BackupLogs
ise/admin(config-Policy List)# cli backup-logs ScheduledBackupLogs repository
SchedBackupRepo encryption-key plain xyzabc
ise/admin(config-Policy List)# exit
ise/admin(config)#
```

logging

ログレベルを設定するには、コンフィギュレーションモードで **logging** コマンドを使用します。

logging loglevel {0|1|2|3|4|5|6|7}

この機能を無効にするには、このコマンドの **no** 形式を使用します。

no logging

構文の説明	loglevel	logging コマンドのログレベルを設定するコマンド。
	0 ~ 7	<p>ログメッセージをセットする目的のプライオリティレベル。プライオリティレベルは以下のとおりです（キーワードの番号を入力）。</p> <ul style="list-style-type: none"> • 0-emerg（緊急事態）：システムが使用不可。 • 1-alert（アラート）：ただちに処置が必要。 • 2-crit（クリティカル）：クリティカルな状態。 • 3-err（エラー）：エラー状態。 • 4-warn（警告）：警告状態。 • 5-notif（通知）：正常であるが、重要な状態。 • 6-inform：（デフォルト）情報メッセージ。 • 7-debug：デバッグメッセージ。
コマンドデフォルト	デフォルトの動作や値はありません。	
コマンドモード	コンフィギュレーション（config）#	
コマンド履歴	リリース	変更内容
	2.0.0.306	このコマンドが導入されました。
使用上のガイドライン	このコマンドには loglevel キーワードが必要です。	

例

```
ise/admin(config)# logging loglevel 0
ise/admin(config)#
```


max-ssh-sessions

分散展開のノードごとにコマンドラインインターフェイス（CLI）の最大同時セッション数を設定するには、コンフィギュレーションモードで **max-ssh-sessions** コマンドを使用します。

max-ssh-sessions {0|1|2|3|4|5|6|7|8|9|10}

構文の説明	1 ~ 10	同時 SSH セッションの数。デフォルトは 5 です。
-------	--------	-----------------------------

コマンドデフォルト	許可される最大同時 CLI セッション数のデフォルトは、Cisco ISE 管理者ポータルから 5 に設定されます。	
-----------	--	--

コマンドモード	コンフィギュレーション (config) #
---------	------------------------

コマンド履歴	リリース	変更内容
	2.0.0.306	このコマンドが導入されました。

使用上のガイドライン	<p>max-ssh-sessions パラメータはコマンドラインインターフェイスから設定可能ではありません。アクティブ CLI セッションの最大数は、プライマリ管理 ISE 管理者ポータルから複製されません。</p>
------------	---

CLI セッションの最大数を超えると、このセッションを閉じているコマンドラインインターフェイスに「最大アクティブ SSH セッション数に到達 (Maximum active ssh sessions reached)」メッセージが表示され、下部に「未接続：続行するには Enter または Space を押します (Not connected - press Enter or Space to connect)」というメッセージが表示されます。

コンソールから CLI にログインして **forceout username** コマンドを使用すると、ユーザをログアウトさせてアクティブな SSH セッションの数を削減できます。

コマンドラインインターフェイス（CLI）セッションの最大数を設定するためのナビゲーションパスは、Cisco ISE 管理者ポータルの [セッション (Session)] タブの次の場所にあります。
 [管理 (Administration)] > [システム (System)] > [管理者アクセス (Admin Access)] > [設定 (Settings)] > [アクセス (Access)]。

ntp

NTP 設定を指定するには、**authenticate**、**authentication-key**、**server**、および **trusted-key** コマンドと共にコンフィギュレーションモードで **ntp** コマンドを使用します。

ntp authenticate

ntp authentication-key <key id> **md5hash** | **plain**<key value>

ntp server {ip-address | hostname} key <peer key number>

ntp trusted-key <key>

no ntp server

構文の説明

authenticate	すべての時刻源の認証をイネーブルにします。
authentication-key	信頼できる時刻源の認証キーを指定します。
server	使用する NTP サーバを指定します。
trusted-key	信頼できる時刻源のキー番号を指定します。

コマンド デフォルト

なし

コマンド モード

コンフィギュレーション (config) #

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

ntp コマンドを使用して NTP 設定を指定します。

デバイスの NTP サービスを終了するには、**authenticate**、**authentication-key**、**server**、および **trusted-key** などのキーワードおよび引数を指定して **no ntp** を入力する必要があります。たとえば、以前に **ntp server** コマンドを実行した場合は、**server** とともに **no ntp** コマンドを使用します。

例

```
ise/admin(config)# ntp ?
  authenticate      Authenticate time sources
  authentication-key Authentication key for trusted time sources
  server             Specify NTP server to use
  trusted-key        Key numbers for trusted time sources
ise/admin(config)#
ise/admin(config)# no ntp server
ise/admin(config)# do show ntp
% no NTP servers configured
ise/admin(config)#
```

ntp authenticate

すべての時刻源の認証を有効にするには、**ntp authenticate** コマンドを使用します。NTP 認証キーのない時刻源は同期されません。

この機能を無効にするには、このコマンドの **no** 形式を使用します。

ntp authenticate

構文の説明	authenticate	すべての時刻源の認証をイネーブルにします。
コマンドデフォルト	なし	
コマンドモード	コンフィギュレーション (config) #	
コマンド履歴	リリース	変更内容
	2.0.0.306	このコマンドが導入されました。

使用上のガイドライン **ntp authenticate** コマンドを使用し、すべての時刻源の認証を有効にします。このコマンドは任意であり、このコマンドを指定しなくても認証は機能します。

一部のサーバのみが認証を必要とする混在モードで認証する場合、つまり一部のサーバのみ認証用に設定されているキーが必要な場合は、このコマンドを実行してはなりません。

例

```
ise/admin(config)# ntp authenticate
ise/admin(config)#
```

ntp authentication-key

時間源の認証キーを指定する場合は、コンフィギュレーション モードで一意的識別子およびキー値を指定して **ntp authentication-key** コマンドを使用します。

ntp authentication-key キー *id* **md5 hash** | **plain** キーの値

この機能を無効にするには、このコマンドの **no** 形式を使用します。

no ntp authentication-key

構文の説明

authentication-key	信頼できる時刻源の認証キーを設定します。
<i>key id</i>	このキーに割り当てる ID。1 から 65535 までの数値がサポートされます。
md5	認証キーの暗号化タイプ。
hash	認証のハッシュされたキー。暗号化タイプに続けて、暗号化された（ハッシュされた）キーを指定します。40 文字までで指定します。
plain	認証用のプレーン テキストのキー。暗号化タイプに続けて、暗号化されていないプレーン テキストキーを指定します。15 文字までで指定します。
<i>key value</i>	上記の md5 plain hash のいずれかに一致する形式のキー値。

コマンド デフォルト

なし

コマンド モード

コンフィギュレーション (config) #。

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

ntp authentication-key コマンドを使用して、NTP 認証の認証キーとともに時刻源を設定し、それに関連するキー ID、キー暗号化タイプ、およびキー値設定を指定します。このキーを信頼できるリストに追加してから **ntp server** コマンドに追加します。

信頼リストに追加されている NTP 認証キーのない時刻源は同期されません。



(注) **show running-config** コマンドはセキュリティのためにハッシュ形式に変換される Message Digest 5 (MD5) プレーン形式に入力されたキーを常に示します。たとえば、**ntp authentication-key 1 md5 hashee18afc7608ac7ecdbeefc5351ad118bc9ce1ef3** です。

例 1

```
ise/admin# configure
ise/admin(config)#
ise/admin(config)# ntp authentication-key 1 md5 plain SharedWithServe
ise/admin(config)# ntp authentication-key 2 md5 plain SharedWithServ
ise/admin(config)# ntp authentication-key 3 md5 plain SharedWithSer
```

例 2

```
ise/admin(config)# no ntp authentication-key 3
(Removes authentication key 3.)
```

例 3

```
ise/admin(config)# no ntp authentication-key
(Removes all authentication keys.)
```

ntp server

NTP サーバによるシステムのソフトウェアクロックの同期を許可するには、コンフィギュレーション モードで **ntp server** コマンドを使用します。それぞれ別個の行にキーを指定した最大 3 台のサーバを許可します。キーはオプションパラメータですが、NTP 認証にはキーが必要です。

Cisco ISE は、NTP サーバの公開キー認証もサポートしています。NTPv4 は、対称キー暗号化を使用し、公開キー暗号化に基づく新しい **Autokey** 方式も提供します。公開キー暗号化は、一般に、各サーバによって生成され公開されない非公開の値に基づいているため、対称キー暗号化よりも安全であると考えられます。**Autokey** では、すべてのキー配布および管理機能には公開値のみが含まれているため、キーの配布と保管が大幅に簡素化されます。IFF (**identify Friend** または **Foe**) 識別方式は最も広く使用されている方式なので、この方式を使用することを推奨します。

Cisco ISE には、常に有効で到達可能な NTP サーバが必要です。

キーはオプションパラメータですが、NTP サーバを認証する必要がある場合は、キーを設定する必要があります。

この機能を無効にするには、NTP サーバを削除して別のサーバを追加する場合のみ、このコマンドの **no** 形式を使用します。

ntp server {*ip-address* | *hostname*} {**autokey** | *key* <*peer key number*>}

構文の説明

server	システムによって、指定されたサーバと同期されます。
<i>ip-address</i> <i>hostname</i>	クロック同期を提供するサーバの IPv4 または IPv6 アドレスまたはホスト名。引数は 255 文字までの英数字で指定します。IPv6 アドレスで NTP サーバを追加する場合は、ISE eth0 インターフェイスが IPv6 アドレスで静的に設定されていることを確認してください。
autokey	NTP サーバに対して公開キー認証を使用する必要があることを指定します。このオプションを選択した場合、 crypto コマンドを使用して、Cisco ISE ノードに NTP サーバの公開キーをインポートする必要があります。

<i>key</i>	<p>(任意)。ピアのキー番号。最大 65535 桁までサポートします。</p> <p>このキーは、ntp authentication-key コマンドを使用してキー値で定義する必要があります。また、ntp trusted-key コマンドを使用して、信頼できるキーとして追加する必要があります。</p> <p>認証を実行するために、キーとキーの値は実際の NTP サーバに定義されているキーと同じ値にする必要があります。</p>
------------	--

コマンド デフォルト デフォルトで設定されているサーバはありません。

コマンド モード コンフィギュレーション (config) #

コマンド履歴	リリース	変更内容
	2.0.0.306	このコマンドが導入されました。

使用上のガイドライン この **ntp server** コマンドは、システムを指定したサーバと同期させる場合に、信頼できるキーを指定して使用します。

キーはオプションですが、NTP 認証には必要です。まず、このキーを **ntp authentication-key** コマンドで定義し、**ntp trusted-key** コマンドに追加した後、**ntp server** コマンドに追加します。

show ntp コマンドは同期の状態を表示します。設定されたいずれの NTP サーバも到達可能ではなく、認証されていない場合 (NTP 認証が設定されている場合)、このコマンドによって最小のストラタムを持つローカルへの同期が表示されます。

NTP サーバが到達可能ではないか、適切に認証されていない場合、このコマンド統計についての到達度はゼロになります。

Cisco ISE 管理者ポータルから NTP サーバ コンフィギュレーションと認証キーを定義するには、『*Cisco Identity Services Engine Administration Guide*』の「System Time and NTP Server Settings」の項を参照してください。コンフィギュレーションモードで Cisco ISE CLI から NTP サーバのみに **Autokey** を設定できます。NTP サーバに **Autokey** を設定した後、NTP サーバから生成された公開キーをインポートする必要があります。詳細については、**crypto** コマンドを参照してください。



- (注) NTP サーバに対して公開キー認証を使用する場合は、次の条件が必要です。
- ネットワークで使用可能な NTP サーバが **Autokey** で設定されていることを確認します。NTP サーバは DNS または ホスト名 アドレス 経由で到達可能である必要があります。NTP サーバに対して **Autokey** を設定する方法については、『[NTP Support Web](#)』を参照してください。
 - **ntp-keygen-T** コマンドを使用して、NTP サーバでキーペアを生成し、NTP サーバの信頼できる公開キーを取得します。**crypto** コマンドを使用して、公開キーを Cisco ISE にインポートします。



- (注) このコマンドは、同期プロセス時に矛盾した情報を表示します。同期プロセスは、完了までに最大 20 分かかることがあります。

例

```
ise/admin# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ise/admin(config)# ntp server 209.165.200.225 autokey

ise/admin# show running-config
interface GigabitEthernet 0
 ip address 209.165.200.225 255.255.255.0
 ipv6 address autoconfig
 ipv6 enable
!
 ip name-server 209.165.200.226
!
 ip default-gateway 209.165.200.227
!
 ip route 2.2.2.0 255.255.255.0 gateway 127.0.0.1
!
!
 clock timezone Asia/Kolkata
!
 ntp authentication-key nn md5 hash xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
 ntp trusted-key nn
 ntp server 209.165.200.228 key nn
 ntp server 209.165.200.229
 ntp server 209.165.200.225 autokey
!
```

NTP サーバ認証の信頼キーの設定

NTP サーバによるシステムのソフトウェアクロックの同期を許可するには、コンフィギュレーション モードで **ntp server** コマンドを使用します。

```
ise/admin(config)# ntp server ntp.esl.cisco.com key 1
% WARNING: Key 1 needs to be defined as a ntp trusted-key.
```



```

ise/admin(config)#
ise/admin(config)# ntp trusted-key 1
% WARNING: Key 1 needs to be defined as a ntp authentication-key.
ise/admin(config)#
ise/admin(config)# ntp authentication-key 1 md5 plain SharedWithServe
ise/admin(config)#

ise/admin(config)# ntp server ntp.esl.cisco.com 1
ise/admin(config)# ntp server 171.68.10.80 2
ise/admin(config)# ntp server 171.68.10.150 3
ise/admin(config)#
ise/admin(config)# do show running-config
Generating configuration...
!
hostname ise
!
ip domain-name cisco.com
!
interface GigabitEthernet 0
 ip address 10.105.171.218 255.255.255.0
 ipv6 address 2001:420:54ff:4::420:101/112
 ipv6 address autoconfig
 ipv6 enable
!ip name-server 10.105.171.200 2001:420:54ff:4::420:200
!
ip default-gateway 172.21.79.1
ipv6 route ::/0 gateway 2001:420:54ff:4::420:10
!
clock timezone UTC

!
ntp authentication-key 1 md5 hash ee18afc7608ac7ecdbeefc5351ad118bc9ce1ef3
ntp authentication-key 2 md5 hash f1ef7b05c0d1cd4c18c8b70e8c76f37f33c33b59
ntp authentication-key 3 md5 hash ee18afc7608ac7ec2d7ac6d09226111dce07da37
ntp trusted-key 1
ntp trusted-key 2
ntp trusted-key 3
ntp authenticate
ntp server 10.105.171.10 key 1
ntp server 2001:420:54ff:4::420:111 key 2
ntp server clock.cisco.com key 3
!
--More--

```

同期化のステータスの確認

同期のステータスを確認するには、**show ntp** コマンドを使用します。

例 1

```

ise/admin# show ntp
Primary NTP   : ntp.esl.cisco.com
Secondary NTP : 171.68.10.80
Tertiary NTP  : 171.68.10.150
synchronised to local net at stratum 11
  time correct to within 448 ms
  polling server every 64 s

```

remote	refid	st	t	when	poll	reach	delay	offset	jitter
*127.127.1.0	.LOCL.	10	l	46	64	37	0.000	0.000	0.001
171.68.10.80	.RMOT.	16	u	46	64	0	0.000	0.000	0.000

```
171.68.10.150 .INIT.          16 u  47  64   0   0.000   0.000   0.000
Warning: Output results may conflict during periods of changing synchronization.
ise/admin#
```

例 2

```
ise/admin# show ntp
Primary NTP   : ntp.esl.cisco.com
Secondary NTP : 171.68.10.150
Tertiary NTP  : 171.68.10.80
synchronised to NTP server (171.68.10.150) at stratum 3
  time correct to within 16 ms
  polling server every 64 s
    remote          refid          st t when poll reach  delay  offset  jitter
=====
  127.127.1.0      .LOCL.           10 l  35   64  377   0.000   0.000   0.001
+171.68.10.80     144.254.15.122  2 u  36   64  377   1.474   7.381   2.095
*171.68.10.150   144.254.15.122  2 u  33   64  377   0.922  10.485   2.198
Warning: Output results may conflict during periods of changing synchronization.
ise/admin#
```

ntp trusted-key

時刻源を信頼できるリストに追加するには、一意の識別子を指定して **ntp trusted-key** コマンドを使用します。

ntp trusted-key key

この機能を無効にするには、このコマンドの **no** 形式を使用します。

no ntp trusted-key

構文の説明	trusted-key	このキーに割り当てる ID。
	<i>key</i>	信頼できる時刻源にキー番号を指定します。これは、NTP 認証キーとして定義する必要があります。最大 65535 桁までサポートします。
コマンドデフォルト	なし	
コマンドモード	コンフィギュレーション (config) #	
コマンド履歴	リリース	変更内容
	2.0.0.306	このコマンドが導入されました。

使用上のガイドライン このキーを NTP サーバに追加する前に、このキーを NTP 認証キーとして定義し、信頼リストにこのキーを追加します。信頼リストに追加されたキーは、システムで NTP サーバによって同期できるもののみ使用できます。

例 1

```
ise/admin# configure
ise/admin(config)#
ise/admin(config)# ntp trusted-key 1
ise/admin(config)# ntp trusted-key 2
ise/admin(config)# ntp trusted-key 3
ise/admin(config)# no ntp trusted-key 2
(Removes key 2 from the trusted list).
```

例 2

```
ise/admin(config)# no ntp trusted-key
(Removes all keys from the trusted list).
```

rate-limit

送信元IPアドレスからのTCP、UDP、またはICMPパケットの制限を設定するには、コンフィギュレーションモードで **rate-limit** コマンドを使用します。この機能を削除するには、このコマンドの **no** 形式を使用します。

rate-limit 250 ip-address net-mask port

構文の説明	<1-10000>	1秒あたりの平均TCP/UDP/ICMPパケット数。
	ip-address	パケットレート制限を適用する送信元IPアドレス。
	net-mask	パケットレート制限を適用する送信元IPマスク。
	port	パケットレート制限を適用する宛先ポート番号。
コマンド デフォルト	デフォルトの動作や値はありません。	
コマンド モード	コンフィギュレーション (config) #	
コマンド履歴	リリース	変更内容
	2.0.0.306	このコマンドが導入されました。
使用上のガイドライン	なし	

例

```
ise49/admin(config)# rate-limit 4000 ip 20.20.20.20 port 443
% Notice : Actual rate limit rounded up by iptables to 5000 per second
ise49/admin(config)# do show running-config | incl rate
rate-limit 5000 ip 20.20.20.20 port 443
ise49/admin(config)#
ise49/admin(config)# rate-limit 6000 ip 10.10.10.10 port 443
% Notice : Actual rate limit rounded up by iptables to 10000 per second
ise49/admin(config)# do show running-config | incl rate
rate-limit 10000 ip 10.10.10.10 port 443
rate-limit 5000 ip 20.20.20.20 port 443
ise49/admin(config)#
```

password-policy

システムに対するパスワードをイネーブル化または設定するには、コンフィギュレーションモードで **password-policy** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

password-policy options



(注) **password-policy** コマンドには、ポリシー オプションが必要です（「構文の説明」を参照）。**password-expiration-enabled** コマンドは、他の **password-expiration** コマンドの前に入力する必要があります。



(注) **password-policy** コマンドを入力すると、**config-password-policy** コンフィギュレーション サブモードに入ります。

構文の説明

<i>digit-required</i>	ユーザパスワードに数字を含むことを必須にします。
<i>disable-cisco-password</i>	パスワードに、「Cisco」や「Cisco」を含む語を使用できないようにします。
<i>disable-repeat-chars</i>	同じ文字が5つ以上含まれているパスワードをディセーブルにします。
<i>do</i>	EXEC コマンド。
<i>end</i>	コンフィギュレーションモードを終了します。
<i>exit</i>	このサブモードを終了します。
<i>lower-case-required</i>	ユーザパスワードに小文字が含まれている必要があります。
<i>min-password-length</i>	有効なパスワードの最小文字数。40文字まで指定します。
<i>No</i>	コマンドを無効にするか、またはデフォルト値を設定します。
<i>no-previous-password</i>	前回のパスワードの一部を再使用できないようにします。

<i>no-username</i>	パスワードにユーザ名を含めることを禁止します。
<i>password-delta</i>	文字数が古いパスワードと異なるようにします。
<i>password-expiration-days</i>	パスワードの有効日数。3650 までの整数をサポートします。
<i>password-expiration-enabled</i>	パスワードの有効期限をイネーブルにします。 (注) password-expiration-enabled コマンドは、他の password-expiration コマンドの前に入力する必要があります。
<i>password-expiration-warning</i>	パスワードの期限が迫っていることを通知する警告を開始するまでの日数。3650 までの整数をサポートします。
<i>password-lock-enabled</i>	指定した回数の試行が失敗したら、パスワードをロックします。
<i>password-lock-retry-count</i>	試行回数を指定します。この回数の試行が失敗するとユーザパスワードがロックされます。20 までの整数をサポートします。
<i>password-lock-timeout</i>	アカウント ロックアウトをクリアするまでの時間を設定します (分単位)。5 分から 1440 分までの時間値をサポートします。
<i>special-required</i>	ユーザ パスワードに特殊文字が含まれている必要があります。
<i>upper-case-required</i>	ユーザ パスワードに大文字が含まれている必要があります。

コマンド デフォルト デフォルトの動作や値はありません。

コマンド モード コンフィギュレーション (config-password-policy) #

コマンド履歴	リリース	変更内容
	2.0.0.306	このコマンドが導入されました。

使用上のガイドライン なし

例

```
ise/admin(config)# password-policy
ise/admin(config-password-policy)# password-expiration-days 30
ise/admin(config-password-policy)# exit
ise/admin(config)#
```




(注) server はサーバ名です。path は /subdir/subsubdir を指します。NFS ネットワーク サーバのサーバ名の後には、コロン (:) が必要です。

表 5: 表 4-5 URL キーワード (続き)

キーワード	コピー元またはコピー先
URL	サーバおよびパス情報を含む、リポジトリの URL を入力します。最大 80 文字の英数字をサポートします。
cdrom:	ローカルの CD-ROM ドライブ (読み取り専用)。
disk:	ローカルストレージ。 ローカルリポジトリ内のすべてのファイルを表示するには、 show repository を実行します。 (注) すべてのローカルリポジトリは、/localdisk パーティションに作成されます。リポジトリの URL で disk:// を指定すると、システムは、/localdisk に対する相対パスでディレクトリを作成します。たとえば、 disk://backup と入力すると、ディレクトリは /localdisk/backup に作成されます。
ftp:	FTP ネットワーク サーバのコピー元またはコピー先の URL。ftp://server/path という URL を使用します
http:	HTTP ネットワーク サーバのコピー元またはコピー先の URL (読み取り専用)。
https:	HTTPS ネットワーク サーバのコピー元またはコピー先の URL (読み取り専用)。
nfs:	NFS ネットワーク サーバのコピー元またはコピー先の URL。nfs://server:/path という URL を使用します
sftp:	SFTP ネットワーク サーバのコピー元またはコピー先の URL。sftp://server/path という URL を使用します

キーワード	コピー元またはコピー先
tftp:	TFTP ネットワーク サーバのコピー元またはコピー先の URL。tftp://server/path という URL を使用します (注) Cisco ISE アップグレードの実行に、TFTP リポジトリは使用できません。

コマンド デフォルト デフォルトの動作や値はありません。

コマンド モード コンフィギュレーション (config-Repository) #

コマンド履歴	リリース	変更内容
	2.0.0.306	このコマンドが導入されました。

使用上のガイドライン サブモードで **url sftp:** を設定する場合は、最初に RSA フィンガープリント (AKA host-key) をターゲット SFTP ホストから ISE にロードする必要があります。これを行うには、CLI で **crypto host_key add** コマンドを使用します。詳細については、[crypto](#) コマンドを参照してください。

この機能を無効にするには、サブモードで **host-key host** コマンドの **no** 形式を使用します。

Cisco ISE 管理者ポータル の [管理 (Administration)] > [システム (System)] > [メンテナンス (Maintenance)] > [リポジトリ (Repository)] > [リポジトリの追加 (Add Repository)] でセキュアな FTP リポジトリを設定すると Cisco ISE は常に次の警告を表示します。

このリポジトリを使用できるようにするには、SFTP サーバのホスト キーをホスト キー オプションを使用して CLI を介して追加する必要があります。

ホスト キーを設定せずに、セキュアな FTP リポジトリにバックアップしようとするすると、対応するエラーが Cisco ADE のログにスローされます。



(注) Cisco ISE は、FIPS モードが ISE で有効になっていない場合でも、FIPS モードで発信 SSH または SFTP 接続を開始します。ISE と通信するリモート SSH または SFTP サーバが FIPS 140-2 承認暗号化アルゴリズムを許可していることを確認します。

Cisco ISE では、組み込みの FIPS 140-2 の検証済み暗号化モジュールが使用されています。FIPS コンプライアンスの要求の詳細については、『[FIPS Compliance Letter](#)』を参照してください。

service

管理するサービスを指定するには、コンフィギュレーションモードで **service** コマンドを使用します。

service sshd

この機能を無効にするには、このコマンドの **no** 形式を使用します。

no service

構文の説明

sshd	Secure Shell Daemon。SSH のデーモンプログラムです。
enable	sshd サービスをイネーブルにします。
encryption-algorithm	SSH暗号化アルゴリズムを設定します。サポートされているアルゴリズムは、a、aes128-cbc、aes128-ctr、aes256-cbc、および aes256-ctr です。
encryption-mode	システムで SSH 暗号化モードを設定します。サポートされているモードは、cbc と ctr です。
key-exchange-algorithm	sshd サービスで許可するキー交換アルゴリズムを指定します。
diffie-hellman-group14-sha1	キー交換アルゴリズムを diffie-hellman-group14-sha1 に制限します
LogLevel	sshd からセキュアシステムログに対するメッセージのログ レベルを指定します。 <ul style="list-style-type: none"> • 1 : 抑止 • 2 : 致命的 • 3 : エラー • 4 : 情報 (デフォルト) • 5 : 冗長 • 6 : デバッグ • 7 : デバッグ 1 • 8 : デバッグ 2 • 9 : デバッグ 3

コマンド デフォルト デフォルトの動作や値はありません。

コマンド モード コンフィギュレーション (config) #

コマンド履歴	リリース	変更内容
	2.0.0.306	このコマンドが導入されました。

使用上のガイドライン なし

例

```
ise/admin(config)# service sshd
ise/admin(config)# service sshd enable
ise/admin(config)# service sshd encryption-algorithm
    Configure aes128-cbc algo
    Configure aes128-ctr algo
    Configure aes256-cbc algo
    Configure aes256-ctr algo
ise/admin(config)# service sshd encryption-mode
    Configure cbc cipher suites
    Configure ctr cipher suites
ise/admin(config)# service sshd key-exchange-algorithm diffie-hellman-group14-sha1
ise/admin(config)# service sshd loglevel 4
ise/admin(config)#
```

shutdown

インターフェイスをシャットダウンするには、インターフェイスコンフィギュレーションモードで **shutdown** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト	デフォルトの動作や値はありません。	
コマンド モード	コンフィギュレーション (config-GigabitEthernet) #	
コマンド履歴	リリース	変更内容
	2.0.0.306	このコマンドが導入されました。

使用上のガイドライン このコマンドを使用してインターフェイスをシャットダウンすると、そのインターフェイスを経由した Cisco ISE アプライアンスへの接続性が失われます。これは、アプライアンスの電源が投入されていても変わりません。

ただし、アプライアンス上に別の IP を使用して 2 番目のインターフェイスを設定し、そのインターフェイスがシャットダウンされていないならば、その 2 番目のインターフェイス経由でアプライアンスに接続できます。

インターフェイスをシャットダウンする別の方法として、ONBOOT パラメータを使用し、`/etc/sysconfig/network-scripts` にある `ifcfg-eth[0,1]` ファイルを変更することもできます。

- インターフェイスをディセーブルにするには、`ONBOOT="no"` と設定します。
- インターフェイスをイネーブルにするには、`ONBOOT="yes"` と設定します。

no shutdown コマンドを使用して、インターフェイスをイネーブルにすることもできます。

例

```
ise/admin(config)# interface GigabitEthernet 0
ise/admin(config-GigabitEthernet)# shutdown
```

snmp-server enable

Cisco ISE で SNMP サーバを有効にするには、グローバル コンフィギュレーション モードで **snmp-server enable** コマンドを使用します。

snmp-server enable

SNMP サーバを無効にするには、このコマンドの **no** 形式を使用します。

コマンド デフォルト SNMP サーバはイネーブルに設定されています。

コマンド モード コンフィギュレーション (config) #

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

例

```
ise/admin(config)# snmp-server enable
ise/admin(config)#
```

snmp-server user

新しいSNMPユーザを設定するには、グローバルコンフィギュレーションモードで **snmp-server user** コマンドを使用します。

snmp-server user *username* **v3** {**hash** | **plain**} *auth-password* *priv-password*



(注) このコマンドは、SNMPバージョン3のみに対して使用する必要があります。

指定したSNMPユーザを削除するには、このコマンドの **no** 形式を使用します。

構文の説明

user	新しいユーザを設定します。
<i>username</i>	SNMP エージェントに属するホスト上のユーザの名前。
v3	<p>トラップの送信に使用する SNMP のバージョン。</p> <p>priv および auth キーワードを有効にするには SNMP バージョン3 セキュリティ モデルを使用する必要があることを指定します。</p>
{ hash plain }	パスワードは、暗号化形式またはプレーン形式です。暗号化されたパスワードは、16 進数の形式である必要があります。

auth-password

認証ユーザパスワードを指定します。パスワードの最小長は 1 文字ですが、セキュリティを確保するために 8 文字以上にすることをお勧めします。

- (注) パスワードを忘れた場合は、回復できないため、ユーザを再設定する必要があります。プレーンテキストのパスワードまたはローカライズされたダイジェストを指定できます。ローカライズされたダイジェストは、ユーザに対して選択した認証アルゴリズム (MD5 または SHA にすることができます) に一致する必要があります。ユーザ設定がコンソールに表示される場合、またはファイル (スタートアップ コンフィギュレーションファイルなど) に書き込まれる場合、ローカライズされた認証ダイジェストとプライバシーダイジェストが常にプレーンテキストのパスワードの代わりに表示されます。

priv-password

暗号ユーザパスワードを指定します。パスワードの最小長は1文字ですが、セキュリティを確保するために8文字以上にすることをお勧めします。

(注) パスワードを忘れた場合は、回復できないため、ユーザを再設定する必要があります。プレーンテキストのパスワードまたはローカライズされたダイジェストを指定できます。ローカライズされたダイジェストは、ユーザに対して選択した認証アルゴリズム (MD5 または SHA にすることができます) に一致する必要があります。ユーザ設定がコンソールに表示される場合、またはファイル (スタートアップ コンフィギュレーションファイルなど) に書き込まれる場合、ローカライズされた認証ダイジェストとプライバシーダイジェストが常にプレーンテキストのパスワードの代わりに表示されません。

コマンド デフォルト デイセーブル。

コマンド モード コンフィギュレーション (config) #

コマンド履歴

リリース

変更内容

2.0.0.306

このコマンドが導入されました。

使用上のガイドライン

ユーザを設定した後、SNMPバージョン3のホストを設定する必要があります。トラップは設定されたユーザだけに送信されるため、ターゲット IP アドレスとともにこのホストを設定するには、ユーザ名を設定する必要があります。

例

```
ise/admin(config)# snmp-server user testuser v3 hash authpassword privpassword
ise/admin(config)#
```

snmp-server host

SNMP トラップを受信者に送信するには、コンフィギュレーション モードで **snmp-server host** コマンドを使用します。デフォルトでは、SNMP トラップはイネーブルになっています。デフォルトでは、UDP ポートは 162 です。

snmp-server host {*ip-address* | *hostname*} **version** {{1 | 2c} *community* | 3 *username engine_ID* {**hash** | **plain**} *auth-password priv-password*}

トラップ転送を削除するには、このコマンドの **no** 形式を使用します。



(注) SNMP バージョン 3 のホストが Cisco ISE で設定されている場合、トラップは設定されたユーザだけに送信されるため、ユーザをそのホストに関連付ける必要があります。 **snmp-server host** コマンドを追加した後、トラップを受信するには、Cisco ISE で設定されているクレデンシアルと同じクレデンシアルを使って、NMS でユーザクレデンシアルを設定する必要があります。

構文の説明

host	SNMP 通知を受信するホストを設定します。
<i>ip-address</i>	SNMP 通知ホストの IP アドレス。最大 32 文字の英数字をサポートします。
<i>hostname</i>	SNMP 通知ホストの名前。最大 32 文字の英数字をサポートします。
version {1 2c 3}	<p>(任意)。トラップの送信に使用する SNMP のバージョン。デフォルトは 1 です。</p> <p>version キーワードを使用する場合は、次のキーワードのいずれかを指定します。</p> <ul style="list-style-type: none"> • 1 : SNMPv1。 • 2c : SNMPv2C。 • 3 : SNMP v3。
<i>community</i>	Cisco ISE と NMS との間での共有秘密キーを指定します。長さが最大 32 文字の大文字と小文字が区別された値。スペースは使用できません。デフォルトコミュニティストリングは「public」です。Cisco ISE はこのキーを使用して、着信 SNMP 要求が有効であるかどうかを判断します。

<i>username</i>	(オプション。SNMP バージョン 3 を選択した場合にのみ必要) Cisco ISE で SNMP バージョン 3 のホストが設定されている場合、ユーザとホストを関連付けます。
<i>engine_ID</i>	(オプション。SNMP バージョン 3 を選択した場合にのみ必要) リモートエンジンの ID。
<i>auth-password</i>	(オプション。SNMP バージョン 3 を選択した場合にのみ必要) 認証ユーザパスワードを指定します。
<i>priv-password</i>	(オプション。SNMP バージョン 3 を選択した場合にのみ必要) 暗号ユーザパスワードを指定します。

コマンド デフォルト

イネーブル。

コマンド モード

コンフィギュレーション (config) #

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

SNMP がすでに設定されている場合、Cisco ISE ではアプライアンスの起動 (リロード) 時に「coldStart(0)」トラップを送信します。Cisco ISE では、最初に起動するときは「coldStart(0)」トラップを送信する Net-SNMP クライアントを使用し、停止するときは企業固有のトラップ「nsNotifyShutdown」を使用します。

snmp-server host コマンドを使用して SNMP を再設定した後は、通常の場合、標準の「coldStart(0)」トラップでも「warmStart(1)」トラップでもなく、企業固有のトラップ「nsNotifyShutdown」を生成します。



- (注) SNMP トラップターゲットがホスト名または FQDN によって指定され、DNS によって IPv4 と IPv6 の両方のアドレスに解決される場合、ISE は ipv6 ではなく IPv4 を介して IPv6 デュアルスタックターゲット受信者に SNMP トラップを送信します。IPv6 を介してトラップが送信されるようにするために、ISE 管理者は、DNS によってホスト名または FQDN のみを IPv6 に対して解決するか、または SNMP トラップを設定するときに IPv6 アドレスを直接指定することができます。

例

```
ise/admin(config)# snmp-server community new ro
ise/admin(config)# snmp-server host 209.165.202.129 version 1 password
ise/admin(config)#
```

```

ise/admin(config)# snmp-server host isel version 2c public
ise/admin(config)# snmp-server community public ro
2012-09-24T18:37:59.263276+00:00 isel snmptrapd[29534]: isel.cisco.com [UDP:
[192.168.118.108]:44474]: Trap ,
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (29) 0:00:00.29, SNMPv2-MIB::snmpTrapOID.0
= OID: SNMPv2-MIB::coldStart,
SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
ise/admin(config)# snmp-server contact admin@cisco.com
2012-09-24T18:43:32.094128+00:00 isel snmptrapd[29534]: isel.cisco.com [UDP:
[192.168.118.108]:53816]: Trap ,
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (33311) 0:05:33.11,
SNMPv2-MIB::snmpTrapOID.0 = OID: NET-SNMP-AGENT-MIB::nsNotifyRestart,
SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpNotificationPrefix

ise/admin(config)# snmp-server host a.b.c.d version 3 testuser 0x12439343 hash authpassword
privpassword
ise/admin(config)#

```

snmp-server community

簡易ネットワーク管理プロトコル (SNMP) へのアクセスを許可するコミュニティアクセスストリングを設定するには、コンフィギュレーションモードで **snmp-server community** コマンドを使用します。

snmp-server community community-string ro

この機能を無効にするには、このコマンドの **no** 形式を使用します。

no snmp-server

構文の説明	community	SNMP コミュニティストリングを設定します。
	<i>community-string</i>	パスワードのように機能するアクセス文字列。これによって SNMP へのアクセスが許可されます。空白は使用できません。最大 255 文字の英数字をサポートします。
	ro	読み取り専用アクセスを指定します。
コマンド デフォルト	デフォルトの動作や値はありません。	
コマンド モード	コンフィギュレーション (config) #	
コマンド履歴	リリース	変更内容
	2.0.0.306	このコマンドが導入されました。

使用上のガイドライン **snmp-server community** コマンドでは、コミュニティストリングと引数 **ro** を指定する必要があります。指定しない場合、エラーが発生します。Cisco ISE の SNMP エージェントは、読み取り専用の SNMP v1 アクセスと SNMP v2c アクセスを次の MIB に提供します。

- SNMPv2-MIB
- RFC1213-MIB
- IF-MIB
- IP-MIB
- IP-FORWARD-MIB
- TCP-MIB
- UDP-MIB
- HOST-RESOURCES-MIB
- ENTITY-MIB : 次の 3 つの MIB 変数のみが ENTITY-MIB でサポートされます。
 - 製品 ID : entPhysicalModelName
 - バージョン ID : entPhysicalHardwareRev
 - シリアル番号 : entPhysicalSerialNumber

- DISMAN-EVENT-MIB
- NOTIFICATION-LOG-MIB
- CISCO-CDP-MIB

例

```
ise/admin(config)# snmp-server community new ro
ise/admin(config)#
```

snmp-server contact

SNMP 接続の管理情報ベース (MIB) 値をシステムに設定するには、コンフィギュレーションモードで **snmp-server contact** コマンドを使用します。システム連絡先情報を削除するには、このコマンドの **no** 形式を使用します。

snmp-server contact *contact-name*

構文の説明	contact	この管理対象ノードの担当者を指定します。 最大 255 文字の英数字をサポートします。
	<i>contact-name</i>	ノードのシステム連絡先情報を表す文字列。 最大 255 文字の英数字をサポートします。
コマンドデフォルト	デフォルトの動作や値はありません。	
コマンドモード	コンフィギュレーション (config) #	
コマンド履歴	リリース	変更内容
	2.0.0.306	このコマンドが導入されました。
使用上のガイドライン	なし	
例	<pre>ise/admin(config)# snmp-server contact Luke ise/admin(config)#</pre>	

snmp-server location

SNMP ロケーションの MIB 値をシステムに設定するには、コンフィギュレーションモードで **snmp-server location** コマンドを使用します。システムロケーション情報を削除するには、このコマンドの **no** 形式を使用します。

snmp-server location *location*

構文の説明	location	この管理対象ノードの物理的な場所を設定します。最大 255 文字の英数字をサポートします。
	<i>location</i>	システムの物理ロケーション情報を表す文字列。最大 255 文字の英数字をサポートします。
コマンドデフォルト	デフォルトの動作や値はありません。	
コマンドモード	コンフィギュレーション (config) #	
コマンド履歴	リリース	変更内容
	2.0.0.306	このコマンドが導入されました。

使用上のガイドライン *word* 文字列では、単語の間にアンダスコア (_) またはハイフン (-) を使用することをお勧めします。 *word* 文字列で単語の間に空白を使用する場合、文字列を二重引用符 (") で囲む必要があります。

例 1

```
ise/admin(config)# snmp-server location Building_3/Room_214
ise/admin(config)#
```

例 2

```
ise/admin(config)# snmp-server location "Building 3/Room 214"
ise/admin(config)#
```


snmp-server trap dskThresholdLimit

Cisco ISE パーティションのいずれかがディスク使用率のしきい値の限界に達した際に、SNMP サーバがトラップを受信するよう設定するには、コンフィギュレーションモードで **snmp-server trap dskThresholdLimit** コマンドを使用します。

snmp-server trap dskThresholdLimit *value*

ディスク使用率がしきい値に達した際にトラップの送信を停止するには、このコマンドの **no** 形式を使用します。

構文の説明	<i>value</i>	使用可能なディスクスペースの比率を表す値。値の範囲は 1 ~ 100 です。
コマンド デフォルト	デフォルトの動作や値はありません。	
コマンド モード	コンフィギュレーション (config) #	
コマンド履歴	リリース	変更内容
	2.1.0.474	このコマンドが導入されました。

使用上のガイドライン Cisco ISE のすべてのパーティションに共通する設定です。しきい値の限界を 40 に設定すると、パーティションのディスク領域が 60% を使用され、残り 40% になった時点でトラップを受信します。つまり、空き領域が設定された値に達したときにトラップが送信されます。

Cisco ISE CLI からこのコマンドを設定すると、kron ジョブが 5 分ごとに実行され、Cisco ISE のパーティションを 1 つずつ監視します。いずれかのパーティションがしきい値の上限に達すると、Cisco ISE は設定されている SNMP サーバにトラップを送信します。ディスクのバスおよびしきい値の上限値も送信します。複数のパーティションがしきい値の上限に達すると、複数のトラップが送信されます。MIB ブラウザのトラップ レシーバを使用して SNMP トラップを表示できます。

例

```
ise/admin(config)# snmp-server trap dskThresholdLimit 40
ise/admin(config)#
```

snmp engineid

既存のエンジン ID を新しい値に変更するには、コンフィギュレーションモードで **snmp engineid command** を使用します。このコマンドは、既存のすべてのユーザを再作成する必要があるという警告を表示します。

snmp engineid *engine_ID_string*

設定したエンジン ID を削除するには、このコマンドの **no** 形式を使用します。

構文の説明	engineid	既存のエンジン ID を指定した新しい値に変更します。
	<i>engine_ID_string</i>	エンジン ID を識別する最大 24 文字の文字列。
コマンド デフォルト	コマンドのデフォルト値はありません。	
コマンド モード	コンフィギュレーション (config) #	
コマンド履歴	リリース	変更内容
	2.0.0.306	このコマンドが導入されました。

例

```
ise/admin(config)# snmp engineid Abcdef129084B
% Warning: As a result of engineID change, all SNMP users will need
to be recreated.
ise/admin(config)#
```

synflood-limit

TCP SYN パケットレート制限を設定します。

synflood-limit ?

構文の説明	synflood-limit	許可される 1 秒あたりの TCP SYN パケットの平均数。
	?	1-2147483647 (TCP SYN パケットの範囲)。
コマンド デフォルト	デフォルトの動作や値はありません。	
コマンド モード	コンフィギュレーション (config) #	
コマンド履歴	リリース	変更内容
	2.0.0.306	このコマンドが導入されました。

使用上のガイドライン TCP SYN パケットレート制限を設定するには、この **synflood-limit** を使用します。

例 1

```
ise-pap-sec/admin(config)# synflood-limit ?
```

username

SSH を使用して Cisco ISE アプライアンスにアクセスできるユーザを追加するには、コンフィギュレーションモードで **username** コマンドを使用します。ユーザがすでに存在する場合は、このコマンドを使用してパスワード、特権レベル、または両方を変更します。システムからユーザを削除するには、このコマンドの **no** 形式を使用します。

username *username* **password** **hash** | **plain** {*password*} **role** **admin** | **user** **email** {*email-address*}

既存のユーザに対しては、次のコマンド オプションを使用します。

username *username* **password** **role** **admin** | **user** {*password*}

構文の説明

<i>username</i>	引数 <i>username</i> には 1 つの単語のみを指定できます。空白や二重引用符 (") は使用できません。最大 31 文字の英数字をサポートします。
password	パスワードを指定します。
<i>password</i>	パスワード。40 文字までの英数字で指定します。パスワードは、すべての新規ユーザに指定する必要があります。
hash plain	パスワードのタイプ。最大 34 文字の英数字をサポートします。
role admin user	ユーザのユーザ ロールと特権レベルを設定します。
disabled	ユーザの電子メールアドレスに従って、ユーザをディセーブルにします。
email	ユーザの電子メールアドレスを設定します。
<i>email-address</i>	ユーザの電子メールアドレスを指定します。たとえば、 <i>user1@mydomain.com</i> のように指定します。

コマンド デフォルト

設定時の初期ユーザです。

コマンド モード

コンフィギュレーション (config) #

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン **username** コマンドでは、**username** および **password** キーワードの後に、**hash / plain and the admin / user** オプションを指定する必要があります。

例 1

```
ise/admin(config)# username admin password hash ##### role admin
ise/admin(config)#
```

例 2

```
ise/admin(config)# username admin password plain Secr3tp@swd role admin
ise/admin(config)#
```

例 3

```
ise/admin(config)# username admin password plain Secr3tp@swd role admin email
admin123@mydomain.com
ise/admin(config)#
```

which

管理者 CLI で使用可能なコマンドの内容を表示するには、コンフィギュレーションモードで **which** コマンドを使用します。

which

構文の説明

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

コンフィギュレーション (config) #

コマンド履歴

リリース	変更内容
2.0.0.306	このコマンドが導入されました。

使用上のガイドライン

which は隠しコマンドです。 **which** は Cisco ISE で使用できますが、コマンドラインで疑問符を入力して表示しようとした場合、CLI インタラクティブヘルプには表示されません。

例

次の例は、 **which** の出力を示しています。

```
ise/admin(config)# which
[ 1]. application configure<STRING>
[ 2]. application install<STRING><STRING>
[ 3]. application remove<STRING>
[ 4]. application reset-config<STRING>
[ 5]. application reset-passwd<STRING><STRING>
[ 6]. application start<STRING>
[ 7]. application start<STRING> safe
[ 8]. application stop<STRING>
[ 9]. application upgrade cleanup
[ 10]. application upgrade prepare<STRING><STRING>
```